JYU DISSERTATIONS 590

Henri Tapani Heinonen

Money Innovations Enabled by Blockchain Technologies

From Cryptocurrency to Cryptomoney

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 590

Henri Tapani Heinonen

Money Innovations Enabled by Blockchain Technologies

From Cryptocurrency to Cryptomoney

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella julkisesti tarkastettavaksi joulukuun 16. päivänä 2022 kello 12.

Academic dissertation to be publicly discussed, by permission of the Faculty of Information Technology of the University of Jyväskylä, on December 16, 2022 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2022

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-951-39-9262-0 (PDF)
URN:ISBN:978-951-39-9262-0
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-9262-0

ABSTRACT

Heinonen, Henri Tapani
Money Innovations Enabled by Blockchain Technologies: From Cryptocurrency to Cryptomoney
Jyväskylä: University of Jyväskylä, 2022, 58 p. (+included articles)
(JYU Dissertations
ISSN 2489-9003; 590)
ISBN 978-951-39-9262-0 (PDF)

This Ph.D. thesis paves the way for turning cryptocurrencies into cryptomonies. The difference between cryptocurrency and cryptomoney is that the latter is reliable, functioning as a Decentralized Payment System, and is also environmentally sustainable. The first research work analyses the price difference behavior of ERC-20 tokens, providing insights into the forthcoming many-money cryptoeconomies. The second research article fixes the problem with Morini's stablecoin scheme by using antimoney to form a many-money economy that allows for trading, even when the Savings wallet's money funds are frozen. The novel method should turn cryptocurrencies into cryptomonies because both unit-of-account and store-of-value are stabilized. As an interesting side-effect, there will be a new way to distribute cryptomoney to the economy by simultaneously giving equal amounts of money and antimoney units. The third research introduces hash recycling as a Justification (value-increasing) technology and reversible bitcoin mining as a Green (energy-decreasing) technology. The fourth research is a survey categorizing many interesting technologies into Green, Justification and 'Mix of Both' technologies. The following categories are proposed in this thesis as two new properties for (sound) cryptomonies: greenness and justness. The fifth research is a perspective article that connects three different computing categories of cryptocurrency mining, grid (volunteer) computing and unconventional computing.

Keywords: Bitcoin, cryptocurrency, cryptomoney, blockchain, distributed ledger technology, unconventional computing, grid computing, cryptocurrency mining, volunteer computing, stablecoin, DeFi, hash recycling, reversible computing

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Heinonen, Henri Tapani
Lohkoketjuteknologioiden mahdollistamat rahainnovaatiot: kryptovaluutoista kryptorahaan
Jyväskylä: University of Jyväskylä, 2022, 58 s. (+artikkelit)
(JYU Dissertations
ISSN 2489-9003; 590)
ISBN 978-951-39-9262-0 (PDF)

Tämä väitöskirja näyttää tietä, miten kryptovaluutat muutetaan kryptorahoiksi. Kryptovaluuttojen ja kryptorahan ero on siinä, että jälkimmäinen on luotettava desentralisoidun maksamisen järjestelmänä, ja on myös ympäristön kannalta kestävä. Ensimmäinen tutkimustyö analysoi ERC-20-rahakkeiden hintaerojen käyttäytymistä ja antaa käsityksen tulevista monen rahan kryptotalouksista. Toinen tutkimus korjaa ongelman Morinin vakaakolikkojärjestelmässä muodostamalla antirahalla monirahatalouden, joka mahdollistaa kaupankäynnin myös silloin, kun talletuslompakon rahavarat ovat jäädytettyinä. Uuden menetelmän pitäisi tehdä kryptovaluutoista kryptorahoja, koska sekä laskentayksikkö että arvonsäilyttäjä ovat vakautuneet. Mielenkiintoisena sivuvaikutuksena syntyy uusi tapa jakaa kryptorahaa talouteen antamalla samanaikaisesti yhtä paljon raha- ja antirahayksiköitä. Kolmas tutkimus esittelee tiivisteiden kierrätyksen (arvoa lisäävänä) Oikeutusteknologiana ja reversiibelin bitcoinin louhinnan Vihreänä (energiaa vähentävänä) teknologiana. Neljäs tutkimus on kartoitus, joka luokittelee monia mielenkiintoisia teknologioita Vihreisiin, Oikeutettuihin ja ‘Molempien Sekoituksiin’. Oheisia luokkia ehdotetaan tässä filosofian tohtorinväitöskirjassa kahtena uutena ominaisuutena (kelvolliselle) kryptorahalle: vihreys ja oikeudenmukaisuus. Viides tutkimus on perspektiiviartikkeli, joka yhdistää kolme erilaista laskentakategoriaa: kryptovaluuttalouhinnan, (vapaaehtoisen) grid-laskennan ja epätavanomaisen laskennan.

Avainsanat: Bitcoin, kryptovaluutta, kryptoraha, lohkoketju, hajautetun tilikirjan teknologia, epätavanomainen laskenta, grid-laskenta, kryptovaluuttalouhiminen, vapaaehtoinen laskenta, vakaakolikko, DeFi, tiivisteiden kierrättäminen, reversiibeli laskenta

Author

Henri Tapani Heinonen
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors

Professor Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

Research Assistant Professor Alexander Semenov
Department of Industrial and Systems Engineering,
Herbert Wertheim College of Engineering
University of Florida
USA

Professor Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland

Adjunct Professor / Docent Veikko Hara
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers

Associate Professor Qipeng Phil Zheng
Department of Industrial Engineering and
Management Systems
College of Engineering and Computer Science
University of Central Florida
USA

Professor Artem Prokhorov
Discipline of Business Analytics
Business School
University of Sydney
Australia

Opponent

Professor Kimmo Kaski
Department of Computer Science
Aalto University
Finland

PREFACE

The 2020s started with grand challenges and violent conflicts, such as the corona pandemic, wars, climate change, fake news, civil unrest, increasing violence, healthcare system problems, mental health problems, energy crises, food crises, high inflation and many others. The old methods alone are not enough to solve all the problems we are facing, even though many problems could be solved if there was enough funding to meet the needs of societies. 'Money does not grow on trees' is something people usually say to justify the absence of money. How about bitcoin and other cryptocurrencies? Are they just worthless bits generated using electricity or are they valuable money growing on trees or something else?

Bitcoin continued the grid computing or volunteer computing efforts introduced in the 1990s with applications such as SETI@home. However, the main difference was that, instead of rewarding the volunteer with credits without any monetary value (such as the BOINC credits), Bitcoin rewards the volunteer (the bitcoin miner who wins the latest round) with a block reward and transaction fees that are paid in the bitcoin cryptocurrency with an actual monetary value. Nothing backs the monetary value of bitcoin: at the beginning, one bitcoin was exactly 0.00 euros, and there were 50 new bitcoins created about every 10 minutes. The value of 50 bitcoins were around one million euros in September 2022, and the value/money created in the early Bitcoin ecosystem per day would be worth 144 million euros, with an exchange rate of about 20,000 EUR/BTC. Of course, it is not entirely obvious how to measure the market capitalization of cryptocurrencies.

Two of the problems facing cryptocurrencies are their volatility (considerable and sudden price changes) and the vast energy consumption of the consensus-forming methods based on Proof-of-Work mining. This Ph.D. research aims to develop tools for turning cryptocurrencies into cryptomonies, which can then be candidates for a Decentralized Payment System. The eventual vision is to add cryptomonies to the contemporary money system, which is based mainly on central bank fiat money and commercial bank credit money.

KIITOKSET

Veikko Haran kanssa käytiin monia mielenkiintoisia keskusteluita jatko-opintojeni alkuvaiheessa. Veikko näki jo tuolloin paljon mahdollisuuksia lohkoketjutekniikoille. Veikkoa ja minua yhdistää lohkoketjujen lisäksi myös fyysikkotaustamme. Häneen tutustuin toisen ohjaajani, Pekka Neittaanmäen, välityksellä. Pekan kanssa on tehty yhteistyössä raportteja ja muistioita liittyen ainakin kvanttilaskentaan ja lohkoketjuihin.

Alexander Semenov motivoi minut julkaisemaan artikkeleita. Monet artikkeleista ovatkin yhteistyössä hänen kanssaan tehtyjä. Ensimmäisessä artikkelissa mukana kirjoittamassa oli myös Vladimir Boginski.

Timo Hämäläinen ja Jari Veijalainen olivat niin ikään kiinnostuneita lohkoketjutekniikoista. Väitöskirjan ylivoimaisesti pisin artikkeli 'A Survey on Technologies Which Make Bitcoin Greener or More Justified' syntyi muutaman viikon aikana. Aihe on mielestäni erittäin ajankohtainen ja tärkeä. On mielenkiintoista nähdä, montako viittausta artikkeliin kertyy vuoden aikana.

Jatko-opintojen alkuvaiheessa rahoitusta tuli Jyväskylän yliopiston informaatioteknologian tiedekunnan tohtorikoululta. Artikkeli PI:n tekemiseen sain apurahaa Ellen ja Artturi Nyyssösen säätiöltä, artikkelien PII ja PIII tekemiseen sain apurahaa Liikesivistysrahastolta ja artikkelit PIV ja PV syntyivät Jyväskylän yliopistolla projektitutkijana ollessa.

Marja-Leena Rantalainen antoi monia arvokkaita ehdotuksia väitöskirjan LaTeX-koodin kohentamiseksi. Qipeng Phil Zheng ja Artem Prokhorov tarkastivat väitöskirjani syksyllä 2022. Vastaväittelijä Kimmo Kasken kanssa on luvassa mielenkiintoisia keskusteluita väitöskirjan aihepiirin tiimoilta.

Jyväskylän yliopiston IT-tiedekunnassa oli vuoden 2018 aikana lohkoketjulaboratorio, jonka kotisivut ovat vielä olemassa [1]. Labrassa työskentelivät minun lisäkseni Veikko Hara, Pekka Neittaanmäki, Alvar Mahlberg, Teemu Hyytiäinen, Kasper Tontti, Ville Yli-Pelkonen, Kai-Markus Lehtimäki, Atte Sarkonen, Aaro Leikari ja Noora Hämäläinen. Lohkoketjulabratiimin ja Santeri Tanin kanssa pidettiin lohkoketjutekniikoita käsitteleviä kurssejakin. Tommi Hakalan kanssa toteutettiin vastaavanlainen kurssipaketti Jyväskylän ammattikorkeakoululle. Ilmari Kortelainen auttoi minua ymmärtämään Salamaverkon toimintaa. Sonja Kärkkäinen, Matti Savonen, Petri Vähäkainu ja Antti Kariluoto olivat monessa vaiheessa mukana kirjoittelemassa raportteja ja muussakin yhteistyössä kanssani. Pekka Abrahamsson, Taija Kolehmainen, Joni Kultanen ja muut StartupLab JYU:n jäsenet tulivat myös vuosien varrella tutuiksi. Vuosina 2010 – 2011 olin mukana Jyväskylän yliopiston tietotekniikan laitoksen FSI-ryhmässä, jonka kotisivut ovat myös edelleen olemassa [2]. Kiitokset Jyväskylän yliopistolle ja Jyväskylän yliopiston informaatioteknologian tiedekunnalle monista mahdollisuuksista. Semman (entinen Sonaatti) henkilökunnan ja Agoran ja Mattilanniemen vahtimestarien (Timo on erityisesti jäänyt mieleen) työ ansaitsevat myös erityismai-

[1] http://blockchain.it.jyu.fi/

[2] https://fsi.it.jyu.fi/

ninnan.

Grammarly ja Scribendi auttoivat englannin kielen oikeinkirjoituksen suhteen erityisesti väitöskirjan loppuvaiheessa.

Teemu Laitinen, Mihail Mateev, nimimerkki Rebirther ja BOINC-yhteisö auttoivat vuosina 2013 – 2017 toteuttamaan BOINC-projektin, joka yhdisti vapaaehtoista grid-laskentaa ja kryptovaluuttalouhintaa.

Juhani Julin perheineen, Suvi Kosonen, Kenneth Partti, Petja Sidoroff, Aku Talikka, Toni Turpeinen, Tuomas Ali-Hokka, Emmi Olin, Mikko Trygg, Maarit Salo, Maaret Suomi, Aminda Suomalainen, Tuomo Littunen, Tuomo-Paavo Salokas, Aulikki Pietinhuhta-Toikka, Andràs Molnàr-Varga, Kirsi Kiviniemi, Tapani Hynynen, Saleem Ullah, Inka Haltiapuu, Merkku Sovijärvi, Elli Backman, Harri Lahti-Luopa, Matleena Käppi, Heidi Elmgren, Jasmin Nevala, Katja Tynkkynen, Marwan Martén, Timo Pitkänen, Emmanuel Okoro, Béla Pavelka, Petri Janhunen, Vilma Talasjärvi, Hensu, Arla, Valo, Lasse Lampén, Jim 'Jukka' Wilce, Mohamed Ahmed Haji Omar, Joel Lehtonen tiimeineen, Jukka Mikkonen, Elmo Koivunen tiimeineen, Ville Salmensuu, Jyrki Parkkinen, Karoliina Salminen, Kate Alhola, Tea Törmänen, Juho P., Antti Peltonen, Antti Tulonen, Markus Mäkelä, Heimo Kotilainen, Pirkko Tuomikoski, Olli Rantanen, Kaija Mattinen, Anssi Kojo, Anitta Rasi ja monet muut ystävät, kaverit ja tuttavat ovat myös osaltaan mahdollistaneet tämän väitöskirjatyön koskien lohkoketjutekniikoita ja rahainnovaatioita.

Lisäksi kiitän isää, äitiä, veljeä ja muita sukulaisia perheineen tuesta vuosien varrella.

Jyväskylä 1.12.2022
Henri Tapani Heinonen

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

PI Henri T. Heinonen and Alexander Semenov and Vladimir Boginski. Collective Behavior of Price Changes of ERC-20 Tokens. *International Conference on Computational Data and Social Networks (CSoNet 2020)*, 2020.

PII Henri T. Heinonen. On Creation of a Stablecoin Based on the Morini's Scheme of Inv&Sav Wallets and Antimoney. *2021 IEEE International Conference on Blockchain (Blockchain), IEEE Workshop on Blockchain Security, Application, and Performance (BSAP-2021)*, 2021.

PIII Henri T. Heinonen and Alexander Semenov. Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators. *International Conference on Blockchain (ICBC 2021)*, 2021.

PIV Henri T. Heinonen and Alexander Semenov and Jari Veijalainen and Timo Hämäläinen. A Survey on Technologies Which Make Bitcoin Greener or More Justified. *IEEE Access*, 2022.

PV Henri T. Heinonen and Alexander Semenov. (unpublished) Bitcoin Mining Could Revolutionize Grid Computing and Unconventional Computing. *Computer (IEEE Computer Society, ISSN 0018-9162)*, 2022.

1 INTRODUCTION

The contemporary money system [Bje16, vas] is a combination of two different kinds of money in three different types: 1a) fiat money in the form of physical cash (banknotes and coins), 1b) fiat money in the form of central bank reserves held in commercial banks' account with the central bank (basically a form of 'electrical cash,' but it is not available to average citizens) and 2c) credit money in the form of deposits in private money users' current accounts with the commercial banks. Even though there are two different kinds of money in three different types, there is only one national currency in most European countries and most of the world. Two notable exceptions are the countries that have made bitcoin (BTC) a second legal tender: El Salvador (United States dollar and bitcoin) and Central African Republic (Central African CFA franc and bitcoin). Belgian economist Bernard Lietaer proposed that communities should create local or complementary currencies that are used along with the national currencies. In Finland, Toholampi (euro and toho) and Sysmä (euro and sysmä) are two municipalities that have trialed the use of local currencies. Local and complementary currencies aim to protect, stimulate and orientate the local economy. For example, a local currency called the Bristol Pound was accepted in 2015 by a renewable energy provider for paying energy bills [the].

The Fourth Industrial Revolution (Industry 4.0) [wor] introduced various new technologies, including blockchain and cryptocurrencies, so there is some motivation to use these techniques to re-invent the monetary system, disrupt existing economic and business models and fight corruption. Indeed, fiat money, credit money, local currencies and complementary currencies can and will work without modern blockchain technologies. Is a new monetary system based on blockchain or other Distributed Ledger Technology (DLT) needed? What is a blockchain? Blockchain is a special case of DLT. Blockchain's database or ledger is distributed on a Peer-to-Peer (P2P) network. Usually, blockchains are not suitable for storing large amounts of data. The usual use case is to append a new block with some metadata and a bunch of transactions to the blockchain. A hash pointer connects the two nearest blocks, forming a chain structure. It is noteworthy that some DLTs (like Corda) are called blockchains, even though they might

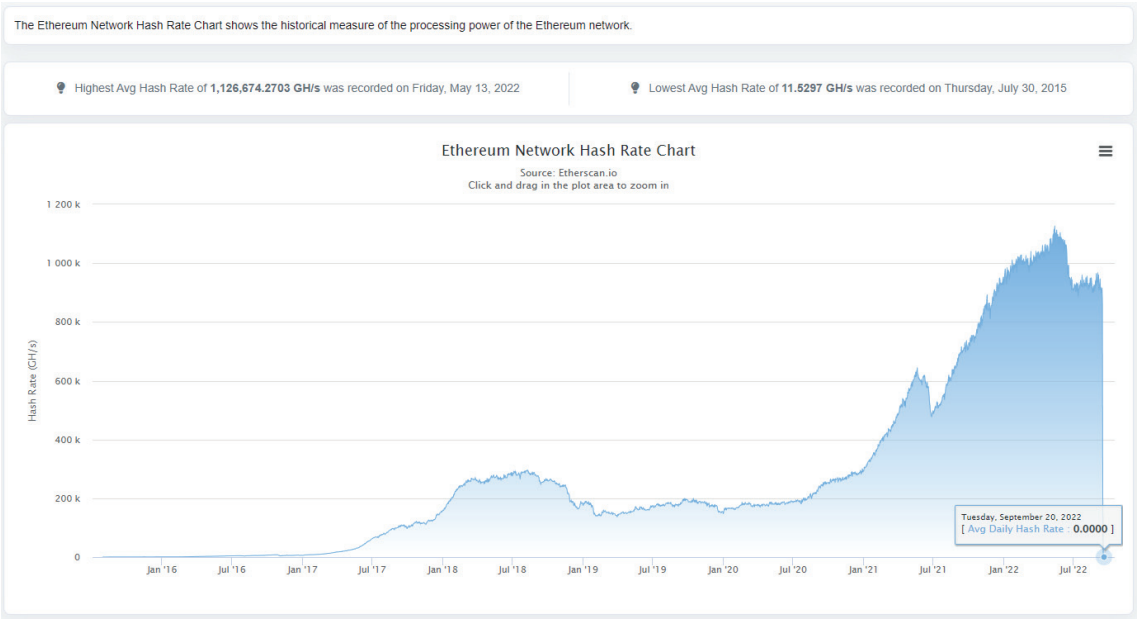


FIGURE 1 The Ethereum network hash rate went to zero after transforming from Proof-of-Work mining to Proof-of-Stake minting. Source: [eth]

not have blocks or a chain structure.

Bitcoin (with an uppercase 'B') is a blockchain, a network and a protocol, and bitcoin (with a lowercase 'b') is the cryptocurrency stored in the Bitcoin blockchain at the protocol level as an entity called a 'coin'. The bitcoin cryptocurrency is the most famous blockchain application, and it has the currency unit BTC, or more officially, XBT. The second most famous cryptocurrency is the Ethereum blockchain's ether (ETH). Ethereum also has application-level entities called 'tokens', which are programmed using smart contracts. The philosophy behind some blockchain projects is that there cannot be a blockchain without the cryptocurrency part. The motivation for securing the Bitcoin blockchain is the bitcoin cryptocurrency that is given as a reward to the miners whose contribution through the Proof-of-Work mining process is securing the blockchain against malicious users. However, the Proof-of-Work model is a competition where the winners tend to have the most mining (computing) power; hence, it incentivizes miners to invest in expensive cryptocurrency mining hardware. On September 15, 2022, the Ethereum Merge stopped the Proof-of-Work mining for Ethereum and started using the Proof-of-Stake consensus method instead, as shown in Figure 1. The new consensus method should reduce Ethereum's energy usage by more than 99% and introduce some optimism for blockchain projects, including Bitcoin, in proving that cryptocurrencies can be environmentally sustainable.

Blockchain technologies could be used for authentication in areas such as financial transactions, supply chains, healthcare, cybersecurity, and personal identity. Using immutable and decentralized blockchain methods for authentication could be useful because the standard centralized methods of using commercial banking services for authentication still have some problems [ilt]. Blockchain is also useful for recording medical data [MBY+20] and cadastre information

[MS19]. VATcoins and digital invoicing [AACT18] have been proposed as a blockchain and cryptocurrency solution to MTIC (Missing Trader Intra Community) frauds, which are the theft of value-added tax (VAT) by organized crime groups that cause 60 billion (10^9) euros of annual tax losses [eur].

1.1 Motivation for the Research

There is much discussion in public domain about the high volatility of cryptocurrencies and the environmental impact of blockchain technologies: even the early Bank of England's report on Bitcoin mentioned the rising cost of mining and increasing total computing power of the Bitcoin network [bana]. The immense volatility of bitcoin price and vast energy usage of the Bitcoin network are the two primary motivators for the present Ph.D. work. The current research aims to develop solutions for 1) making cryptocurrencies more reliable as a Decentralized Payment System (DPS) and 2) making blockchains environmentally sustainable.

One of the motivations behind the present research is to find new use cases for blockchain technologies. Many public discussions about blockchains and cryptocurrencies claim they are useless. This might be true for people who do not use them directly. For public blockchains to survive in the world of climate change and other environmental issues, it is crucial to find new use cases for blockchains - as a way to make them more justified for the general public. If Bitcoin uses as much energy as a small European country, but only several million people worldwide use the bitcoin cryptocurrency, it would be necessary to find more value for that ecosystem without increasing the system's energy usage. In the case of Bitcoin, what new use cases could there be for a system mainly meant to store value transactions in immutable database?

1.2 Research Questions

Based on the motivations mentioned above, the current dissertation addresses the following research questions:

RQ1 What kind of hierarchical structures and groupings do the network graphs show for ERC-20 tokens?

RQ2 How to modify Morini's Scheme of Inv&Sav wallets in a way that makes it a more practical stablecoin for Decentralized Payment Systems?

RQ3 How to change bitcoin mining to use potentially less energy and do something valuable besides securing the Bitcoin blockchain?

RQ4 What technological solutions do we have to make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified?

RQ5 In what ways could bitcoin mining revolutionize grid computing and unconventional computing?

RQ1 has been addressed in Article PI, where networks based on a cross-correlation of ERC-20 token' returns are constructed and analyzed. The resulting graphs' degree distribution do not follow the power law degree distribution. Overall, there are no hierarchical structures or groupings of ERC-20 tokens.

RQ2 has been addressed in Article PII, where an economy of three agents with some sample transactions is demonstrated for two different rebasement equations of the Investment wallet balances. The problem of negative balances can occur in the case of either of the equations. The proposed solution for a negative balance is to freeze the money in the Savings wallet and then use antimoney to enable trading in the economy when the buyer does not have access to money funds.

RQ3 has been addressed in Article PIII, where two different concepts are introduced: hash recycling (justification or value-increasing technology) and reversible bitcoin mining (green or energy-decreasing technology).

RQ4 has been addressed in Article PIV, where technologies are categorized into Justification, Green, and 'Mix of Both' technologies. The categorization came from the two different concepts introduced in Article PIII.

RQ5 has been addressed in Article PV, where cryptocurrency mining, grid computing, and unconventional computing are linked together. It is shown how these three seemingly different forms of computing categories can improve each other.

1.3 Research Methods and Process

The Design Science approach [PTRC07] is followed in the present thesis. It has the following six stages:

1. Problem identification and motivation
2. Definition of the objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

Next, we will review these stages for each article.

Article PI: 'Collective Behavior of Price Changes of ERC-20 Tokens'

Problem identification and motivation. The price fluctuation between cryptocurrencies is not known very well.

Definition of the objectives for a solution. An analysis of price behavior between cryptocurrency tokens is required.

Design and development. The price data of 541 ERC-20 tokens were collected, and a network of ERC-20 token pair price change correlations was constructed and analyzed.

Demonstration. The degree-distribution plots and network graphs of tokens were created.

Evaluation. The degree distributions did not exhibit the power-law behavior usually found in correlation network graphs.

Communication. The publication in Article PI is the primary communication.

Article PII: "On Creation of a Stablecoin Based on the Morini's Scheme of Inv&Sav Wallets and Antimoney"

Problem identification and motivation. A non-collateralized stablecoin would not need fiat monies, cryptocurrencies or commodities to back its value because a 'central bank' coded inside the algorithm controls the stablecoin money supply. The ultimate goal in stablecoin research is to develop a non-collateralized stablecoin, but there are no good examples. One proposed non-collateralized stablecoin is Morini's Scheme, which involves users having two different wallets: the Investment wallet (Inv) and the Savings wallet (Sav). Morini's Scheme has the problem of the possibility of gaming the system when users can predict the upcoming rebasement of the Inv wallets.

Definition of the objectives for a solution. The objective is to design a non-collateralized stablecoin based on Morini's Scheme of Inv and Sav wallets but without problems because of the predictability of the upcoming rebasements.

Design and development. A non-collateralized stablecoin based on Morini's Scheme and antimoney was designed but not developed.

Demonstration. A small economy of three agents using the stablecoin was demonstrated.

Evaluation. The improvement of the novel antimoney-enhanced stablecoin design over the regular Morini's stablecoin was shown using demonstration economy.

Communication. The publication in Article PII is the primary communication.

Article PIII: 'Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators'

Problem identification and motivation. The problem with bitcoin mining is the vast number of hashes generated during the mining process; almost all are thrown away without any usage.

Definition of the objectives for a solution. The objective is to find some usage for the hashes (making bitcoin mining more justified) and to potentially use less energy for the hash generation (making bitcoin mining greener).

Design and development. A proposal for a system that recycles hashes to seed PseudoRandom Number Generators (PRNGs) was made.

Demonstration. The quality of the bitcoin mining hashes was demonstrated by running code that generated the Bitcoin Genesis block and analyzing the hashes with an appropriate application.

Evaluation. The quality of the bitcoin mining hashes as seeds was found to be good enough for PRNGs. It was calculated that recycling all of the hashes generated during bitcoin mining over today's Internet connections would not be practical.

Communication. The publication in Article PIII is the primary communication.

Article PIV: 'A Survey on Technologies Which Make Bitcoin Greener or More Justified'

Problem identification and motivation. Both bitcoin and ether mining use lots of electricity. The mining process provides little value besides securing the Bitcoin and Ethereum blockchains. No surveys categorized technologies into energy-reducing (Green) and value-increasing (Justification) categories.

Definition of the objectives for a solution. The objective is to find a large set of Green and Justification technologies that are mature for production use and also that still need some research and development.

Design and development. A novel technology categorization of Green, Justification and 'Mix of Both' were proposed, and about 20 different technologies were placed into these categories.

Demonstration. Various real-world technologies like Primecoin, SolarCoin, Gridcoin, Curecoin and Foldingcoin are presented.

Evaluation. The technologies are placed into different categories, discussing whether they are plausible for Bitcoin to use.

Communication. The publication in Article PIV is the primary communication.

Article PV: 'Bitcoin Mining Could Revolutionize Grid Computing and Unconventional Computing'

Problem identification and motivation. Cryptocurrency mining uses lots of energy, and new ways to optimize energy usage are needed. There is also a vast source of unused computing cycles in various consumer-grade electronics.

Definition of the objectives for a solution. Three forms of computing – cryptocurrency mining, grid computing and unconventional computing – have a theoretical connection, but the connection has never been used in practice efficiently. This connection should be made more robust.

Design and development. The connection between these three areas of computing is established, and future directions are given.

Demonstration. The connections between three different types of computing are demonstrated:

Cryptocurrency mining: The stories of Bitcoin ASIC machines and the development of graphics cards for cryptocurrency miners are used to demonstrate the industries affected by bitcoin/cryptocurrency mining.

Grid computing: The computing power of the iPhone 6 smartphone is multiplied by an estimated number of smartphones worldwide. Then, the fraction of the phone's recharging hours per day is used to multiply the available computing power. The figure is compared with the world's fastest supercomputer's computing power.

Unconventional computing: The article mentions the oPoW optical computing project for bitcoin mining and proposal of using reversible computing for bitcoin mining to demonstrate the promises of unconventional computing.

Evaluation. The calculation of available computing cycles in a decade-old smartphone multiplied by the estimated number of smartphones worldwide is comparable to the fastest supercomputer in the world, even when only the recharging period of the phone is used for grid computing purposes.

Communication. The publication in Article PV is the primary communication.

Summaries of these data are presented in Tables 1–5.

TABLE 1 Summary of research questions and research methods for Article PI.

Article PI	Explanation
Research Question	RQ1: What kind of hierarchical structures and groupings do the network graphs show for ERC-20 tokens?
Problem	The price fluctuation between cryptocurrencies is not known very well.
Solution Objective	An analysis of price behavior between cryptocurrency tokens is required.
Development	A network-based approach for analyzing price behavior between cryptocurrency tokens.
Demonstration	A network based on Pearson correlation coefficients between the returns of hundreds of ERC-20 tokens.
Evaluation	The degree distributions do not exhibit power-law behavior that is usually found in correlation network graphs.
Communication	Article PI

TABLE 2 Summary of research questions and research methods for Article PII.

Article PII	Explanation
Research Question	RQ2: How to modify Morini's Scheme of Inv&Sav wallets in a way that makes it a more practical stablecoin for Decentralized Payment Systems?
Problem	There are no known non-collateralized stablecoins without major issues.
Solution Objective	Stablecoin design required.
Development	Antimoney-enhanced stablecoin design based on the Morini's scheme.
Demonstration	The stablecoin design was demonstrated on a small economy of three agents.
Evaluation	An improvement of the design was shown using the demonstration economy.
Communication	Article PII

TABLE 3 Summary of research questions and research methods for Article PIII.

Article PIII	Explanation
Research Question	RQ3: How to change bitcoin mining to use potentially less energy and do something valuable besides securing the Bitcoin blockchain?
Problem	Bitcoin mining is irreversible and energy-consuming, and the huge number of hashes generated are being wasted.
Solution Objective	Hash recycling (Justification technology) and reversible bitcoin mining (Green technology) designs are required.
Development	Reversible bitcoin mining proposal and a crude design for hash recycling.
Demonstration	The quality of the hashes was analysed with an appropriate application.
Evaluation	The quality of the hashes was shown to be good enough for seeds.
Communication	Article PIII

TABLE 4 Summary of research questions and research methods for Article PIV.

Article PIV	Explanation
Research Question	RQ4: What technological solutions do we have to make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified?
Problem	There is no survey that lists both energy-reducing and value-increasing blockchain/DLT technologies.
Solution Objective	A new categorization is required.
Development	Proposal for two different technology categories (Green and Justification).
Demonstration	Twenty different technologies were categorized.
Evaluation	The choice of categories and the plausibility of the technologies for Bitcoin were discussed.
Communication	Article PIV

TABLE 5 Summary of research questions and research methods for Article PV.

Article PV	Explanation
Research Question	RQ5: In what ways could bitcoin mining revolutionize grid computing and unconventional computing?
Problem	Cryptocurrency mining is using lots of energy, and new ways to optimize the energy usage are needed.
Solution Objective	The connection among cryptocurrency mining, grid computing and unconventional computing should be made stronger.
Development	The connection between these three areas of computing is established, and future directions are given.
Demonstration	Stories of connections between cryptocurrency mining, grid computing and unconventional computing are presented.
Evaluation	Computing cycles of smartphones in the world are compared with a modern supercomputer.
Communication	Article PV

1.4 Thesis Structure

The present dissertation is structured as follows: Chapter 2 discusses the related work, Chapter 3 describes the results, Chapter 4 summarizes the original articles, and Chapter 5 concludes the dissertation, which is followed by the original articles.

This dissertation includes five original articles. Four of them are published.

2 RELATED WORK

In this chapter, a literature review is given to provide the reader with some background material. Cryptocurrencies and blockchains (and other DLTs) have much to offer to the financial world, but we first examine the history of money.

2.1 History of Money

What is the origin of money? There are usually three theories [Bje16]: commodity, fiat, and credit theory. Let us start with some early history of money.

2.1.1 Barter system

Before money, several thousands of years ago, there were barter systems in which goods and services were exchanged. The problems with barter systems were the (double) coincidence of wants, the non-divisibility of livestock and the non-durability of food. The double coincidence of wants is a rare phenomenon in which two parties can directly exchange items without a monetary medium because they both hold an item the other party wants. Livestock can be considered domesticated animals and, as living animals, they do not have the divisibility property, which is usually needed from (sound) currency/money. Food is usually non-durable because food tends to become moldy and non-edible very fast. Sound currency/money should be durable over long periods.

2.1.2 Commodity money and representative money

Schmitt et al. [SSB14] have noted that a correct definition of money is still being debated and that money is defined by its functions as 'money is what money does' in most economic textbooks. The authors also mention that it is helpful to distinguish between commodity money and representative money.

Adam Smith [Smi76] told the story of the butcher, the brewer and the baker,

who invented a money economy because a simple barter system was not enough anymore. An economy of commodity money, which uses money, with an intrinsic value, as means of exchange, was born. These commodity monies include jewelry, clothes and gold and silver coins. It is sometimes said [Bje16, Ing13] that the commodity theory fails to recognize the role of the state and relations between debt and money.

Money could also have an extrinsic value instead of an intrinsic value. The opposite of commodity money is representative money, such as banknote money. It was created when metal coins and metals stored in a bank were certified to a piece of paper that was accepted as a means-of-payment. Representative money did not have any (practical) intrinsic value, but the creator (usually a government) of the representative money committed to exchange that money for a known amount of a certain commodity: for example, with a banknote, it was possible to get a known amount of gold from a bank.

2.1.3 Fiat money

A state or another sovereign entity can make money through two simultaneous movements: a) it produces objects that are legal money, and b) it demands its citizens to use these objects to pay taxes and other kinds of debt to the state [Bje16]. The fiat theory states that money is created by the process described above.

Fiat money might look quite similar to representative money, but any commodity cannot back fiat money, and it does not have significant intrinsic value. Already during the eleventh century, fiat money banknotes were used in China.

Between 1944 and 1971, many national currencies were pegged to the U.S. dollar, and gold was used as the basis for the U.S. dollar in a system known as the Bretton Woods Agreement, which was negotiated in 1944 by delegates representing 44 countries in Bretton Woods, New Hampshire. One of the agreement's goals was to prevent currencies' devaluation.

During the Vietnam War, expenses were funded by creating more U.S. dollars. However, the gold reserve was not enough to correspond to the newly created U.S. dollars, leading Richard Nixon ending the Gold Standard. The convertibility between the U.S. dollar and gold ended on August 15th, 1971, ending the Bretton Woods system and turning the U.S. dollar into fiat money.

2.1.4 Credit money

Credit theory says that money is debt. As stated in the introduction section, credit money is used in commercial banks. In commercial banks, credit money works as an immediate means-of-payment, and it circulates between customers of commercial banks [Bje16].

The vast majority of publicly held money are in the form of bank deposits [banb]. Fractional reserve banking makes it possible to create new credit money. Contrary to the popular misconception, there will be new money deposits when new loans are made, not the other way round [banb].

2.1.5 Digital money and cryptocurrency

Electrical payments became common after home computers with Internet connections rose in popularity. There were early electrical money experiments in the 1990s, but they failed because of technical limitations and high fees. For example, according to a press release [eu.] from March 13th, 1996, EUnet and DigiCash first launched a system of electronic cash (eCash) in Finland because Finland already had a high number of Internet connections per person. Merita, the largest bank in Finland during the time, allowed users to visit a virtual ATM on the Internet and send money to an eCash purse from their bank account. A report [hel] mentions that the eCash system had considerably higher monthly fees for merchants than the Avant card money. To use the Avant system, the user needed to buy a card reading device for the computer, and loading money to the card also came with some fees.

In 2008, a blockchain-based cryptocurrency called bitcoin was introduced. The currency unit of bitcoin is BTC (or officially XBT). The idea and the original implementation of bitcoin came from an individual using a pseudonym, Satoshi Nakamoto. The Bitcoin blockchain was started in January 2009. Bitcoin solved some problems that made the other electrical currency projects fail: for example, Bitcoin solved the Byzantine Generals Problem [SM15]. In a blockchain, the blocks are chained together, making the data tamper-proof and immutable. Blocks tend to contain information about transactions, which are value transfers to a bitcoin address. It is said that the Bitcoin blockchain is the Internet of Value or Internet of Money. New blocks are being created every 10 minutes on average, and for the first four years, there were 50 new bitcoins in every block given as a block reward to miners securing the blockchain. Every four years, the Bitcoin block reward is halved. As of writing this in 2022, the Bitcoin block reward is 6.25 BTC/block. In addition to the block reward, the winning miner will collect the transaction fees from users whose bitcoin transactions were included in the block.

Do anonymous or pseudonymous cryptocurrencies make it easy to commit crimes? Berentesen et al. [BS18] have noted that both governments and citizens can be bad actors. The authors welcome anonymous cryptocurrencies to protect citizens from bad governments. Do cryptocurrencies make public money obsolete? Brunnermeier et al. [BJL19] claim that a Central Bank Digital Currency (CBDC) ensures that public money will remain a relevant unit-of-account. Brunnermeier et al. [BN19] construct a framework for cryptocurrency and public money swaps, but it assumes a permissioned blockchain, not the typical Proof-of-Work-based permissionless blockchain like Bitcoin. Fernández-Villaverde et al. [FVS19] build a model of competition for privately-issued fiat currencies; they say that most cryptocurrencies are fully fiduciary and that most historical private monies have been commodity-backed currencies. Fernández-Villaverde et al. [FVSSU21] mention CBDC giving consumers the possibility of having a central bank account and potentially eliminating physical cash.

According to Bjerg [Bje16], bitcoin is commodity money without gold, fiat

money without a state and credit money without debt. Jones et al. argue that [JGB22] bitcoin operates from the climate perspective as digital crude oil.

The dynamics of monetary aggregates and cryptocurrencies (and other digital monies) are a potential topic of new research. It is important to understand how current monetary aggregates work with new monetary innovations like bitcoin. The present thesis only mentions the popular monetary aggregates in the following section and does not discuss their relations to cryptocurrencies.

2.2 Properties of Currencies and Monies

What are money and currency? Often, the properties of (sound) money are said to be the following:

- scarcity
- durability
- divisibility
- verifiability (or recognizability)
- storability
- portability (or transportability)
- fungibility
- non-counterfeitability
- useability
- medium-of-exchange (or means-of-payment)
- unit-of-account
- store-of-value
- standard-of-deferred-payment

Often, the properties of (sound) currency are said to be the same as those of (sound) money, excluding store-of-value. Thus, money has one more property than currency: it stores a value (economic energy) over long periods. The following is a summary of the currency/money properties from various sources [ecb, tra, ude, xap, bana, BBL+20]:

Scarcity. Scarcity is a property that means the object used as money should not be easy to find or create. Fiat, gold and bitcoin are scarce [tra]. Fiat is usually scarcely created by a small group of people, but large amounts of fiat during extreme inflation can be created. Gold is scarce but widely available; some metals like copper and platinum are too plentiful or scarce compared with gold. The Bitcoin protocol defines that only 21 million bitcoin coins will ever be created, making bitcoin scarce.

Durability. Durability is a property that means that currency/money should not degrade over time. For example, glass objects are not durable because they

are easily broken. Fiat is neutral in its durability, and gold and bitcoin are durable [tra]. Paper fiat is easily damaged but easily replaced. Gold bars do not need maintenance and can last hundreds of years. Bitcoin is digital and does not wear out, but the wallet files can be corrupted or deleted, so care must be taken.

Divisibility. Divisibility is a property that means that currency/money should be possible to divide into smaller pieces suitable for trading. The livestock example mentioned in the beginning is an excellent example of non-divisibility: a living animal is always traded as a whole. Fiat and bitcoin are divisible, and gold is neutral in this aspect [tra]. Fiat is available in various denominations. Bitcoin is currently divisible up to eight decimal places. Dividing gold is difficult but not impossible.

Verifiability. Verifiability is a property that means that currency/money is easily identified and verified. Fiat is easily verifiable, and gold and bitcoin are neutral in this aspect [tra]. For example, many euro banknotes can be verified using ultraviolet light. Gold can be weighed, and chemical tests can be performed to verify it. Bitcoin verification needs lots of technical knowledge because it is primarily a software-based entity, but there are also physical bitcoin entities like paper wallets and casascius coins.

Storability. Storability means that currency/money is easily stored in large quantities. Fiat is neutral in storability, gold is not easily stored, and bitcoin is easily stored [tra]. Fiat, especially coins, needs some space and infrastructure for storing. Gold usually requires expensive infrastructure for storing (e.g., Fort Knox). Bitcoin is as easily stored in small and large quantities, but many transaction outputs require storage space from the blockchain.

Portability. Portability means that currency/money should be lightweight enough for carrying around. Fiat is neutral in portability, gold is not very portable, and bitcoin has good portability [tra]. Coins are heavy compared with their low monetary value, but banknotes are lightweight. Gold is hefty and not very practical to carry on a daily basis. Bitcoin is usually digital, and the monetary value stored in a bitcoin wallet does not affect the weight of the smartphone.

Fungibility. Fungibility is a property that means that all units of the currency/money must be considered equivalent and replaceable with each other. Fiat and bitcoin are fungible, and gold is neutral [tra]: all equal fiat denominations are equally valuable, and the same goes with bitcoin, but gold has different purity levels. To be precise, commemorative fiat coins can be significantly more valuable than their face value. Also, some bitcoins with a history of being involved in illegal activities could be banned on some crypto exchanges, so they are not precisely fungible.

Non-counterfeitability. Currency or money should not be easily counterfeitable. If a non-authorized person or organization can duplicate currency/money quickly, the currency/money cannot be trusted. Quantum money is a theoretical concept that would make money non-counterfeitable by using the no-cloning theorem from quantum physics. Cryptocurrencies are mostly seen as non-counterfeitable, but there have been cases such as the value overflow incident [dec] when someone was able to create 184 billion bitcoins, even though the limit has always been 21 million bitcoins. There is also a claim about bitcoin double spending [bit], which means that the same bitcoin was used again (possibly multiple times) by the same holder after it was already spent earlier.

Useability. Currency or money should have widespread use so that the user of the money or currency does not have to worry about if the next merchant will accept it [tra]. Fiat is usually accepted everywhere inside the country where it is an official currency, but there are sometimes shops that do not accept too cheap coins or too expensive banknotes. Gold is rarely ever accepted as a means-of-payment in everyday shopping. Bitcoin is still not widely accepted, probably because of the high volatility of the cryptocurrency.

Medium-of-exchange. Medium-of-exchange is a function used to facilitate the sale, purchase or trade of goods between parties. It is an intermediary to avoid the inconveniences typical of barter systems.

Unit-of-account. Unit-of-account is a function for pricing (a measurement of value and cost) for goods, services, assets and liabilities.

Store-of-value. Store-of-value is a function for saving wealth. Sound money saves monetary value over time, making it possible to retrieve that value in the future.

Standard-of-deferred-payment. Standard-of-deferred-payment is a function for valuing a debt. Sound money should have the function of standard-of-deferred-payment for allowing goods and services to be acquired in the present and paid for in the future. William Stanley Jevons, known for the Jevons Paradox, considered standard-of-deferred-payment to be one of the four functions of money.

Of course, there are lots of contradicting definitions for currencies and monies. The current thesis mainly differentiates money from currency by its store-of-value. Money can also be defined by monetary aggregates M0, M1, M2, M3, M4 and so on, here with different degrees of liquidity. The Quarterly Bulletin 2014 Q1 report of the Bank of England [banb] lists the following popular monetary aggregates for the UK.

Notes and coins. Notes and coins in circulation outside the Bank of England.

M0. Notes and coins plus central bank reserves.

Non-interest-bearing M1. Notes and coins plus non-interest-bearing sight deposits held by the non-bank private sector.

MZM. Notes and coins plus all sight deposits held by the non-bank private sector.

M2 or retail M4. Notes and coins plus all retail deposits (including retail time deposits) held by the non-bank private sector.

M3. Notes and coins plus all sight and time deposits held with banks (excluding building societies) by the non-bank private sector.

M4. Notes and coins, deposits, certificates of deposit, repos and securities with a maturity of less than five years held by the non-bank private sector.

M4^{ex}. M4 excluding the deposits of Intermediate Other Financial Corporations (IOFCs).

Divisia. A weighted sum of different types of money.

2.3 Many-Money Economies

There is some evidence that an economy could flourish and be more stable if there is more than one money in the economy. Belgian economist Bernard Lietaer proposes that communities should create local or complementary currencies that are used along with the national currencies. Local and complementary currencies aim to protect, stimulate and orientate the local economy. For example, Toholampi and Sysmä are two Finnish municipalities that have trialed with local currencies (toho and sysmä). The Swiss Wirtschaftsring ('WIR') or the Swiss WIR-Bank, is the world's largest and oldest (founded in 1934) exchange, which uses an alternative or complementary currency: WIR-credits [Sto09]. The WIR credits or WIR francs (CHW) are used together with the Swiss francs (CHF).

What if blockchains could be the proper testing laboratories for multiple currencies/monies? For example, the economy on the Ethereum blockchain has not only the Ether coin (ETH) but thousands of ERC-20 tokens and other tokens using various ERC smart contract standards. Popular Non-Fungible Tokens (NFT) are usually stored in the Ethereum blockchain as smart contracts.

Boginski et al. [BBP06] construct a market graph – a network representation of the stock market data. The cross-correlations were calculated between stock pairs over time using the opening prices data. A node in the market graph

represents each stock, and there is a link between two nodes if the correlation coefficient exceeds a threshold $\theta \in [-1, 1]$. Boginski et al. find power-law degree distribution in the graphs.

A similar approach has been used in Article PI to look for groupings or hierarchies between price changes of ERC-20 tokens. The returns (price changes) $R_i(t)$ of a token over a time scale Δt with a function $Y_i(t)$ as the price of a collection of tokens $i = 1, \ldots, N$ at time t can be calculated using the following:

$$R_i(t) \equiv \frac{Y_i(t + \Delta t) - Y_i(t)}{Y_i(t)} = \frac{Z_i(t)}{Y_i(t)}. \tag{1}$$

The cross-correlation matrix is then

$$C_{ij} \equiv \langle R_i(t) R_j(t) \rangle. \tag{2}$$

A sliced network can be created by keeping only the links (edges) formed by correlations with a value higher than the 95th percentile. Article PI could not find groupings or hierarchies providing evidence that the ERC-20 cryptocurrency market is underdeveloped: there are lots of new cryptocurrencies created every year and the older cryptocurrencies might go on hiatus after a short period of initial interest.

Liang et al. [LLCZ19] compare foreign exchange, stock market, and cryptocurrencies, finding that the cryptocurrency market does not have clear clustering rules and that the clusters change more rapidly than they do in the foreign exchange and stock market. They also note that the cryptocurrency market is fragile.

2.4 Antimoney

Bitcoin was not the only proposed solution for the financial crisis of 2007 – 2008. A potential solution coming from the field of econophysics is the concept of antimoney [SSB14]. Econophysics is a field combining economics and physics, so it tries to solve problems found in the economy with methods mostly from statistical physics and particle physics.

The proposed antimoney is compared with the concept of antimatter, but the difference is that money and antimoney do not annihilate each other. The question is whether money always has to be positive or zero. Antimoney can be considered a form of negative money, but it has a different currency unit than its counterpart, that is, money. There is an exchange rate between antimoney and money, like exchange rates between fiat currencies and cryptocurrencies.

A real monetary wealth in a symmetric monetary system [SSB14] is given by the following:

$$\omega = \frac{a}{p_a} - \frac{l}{p_l}, \tag{3}$$

where a is money, l is antimoney, p_a is the price level for money, and p_l is the price level for antimoney.

Antimoney needs stricter rules than money because it should not be allowed to hoard unlimited amounts of antimoney, destroy antimoney, or send antimoney to someone unsolicited.

2.5 Stablecoins

As mentioned in Section 2.2, money's functions are medium-of-exchange, unit-of-account, store-of-value, and standard-of-deferred-payment. Cryptocurrencies tend to be volatile, so they might undergo sudden and large changes in their exchange rate and purchasing power.

Stablecoins are cryptocurrencies that use some mechanism to lower their volatility or stabilize their exchange rate and purchasing power. Stablecoins are pegged to some asset (usually EUR or USD) and follow the asset's value [hac]. However, the pegged asset does not necessarily collateralize stablecoins. For example, imagine a stablecoin pegged to the US dollar and collateralized by ether (ETH) coins. Collateralization means that there is something that backs the value of the stablecoin. The token/coin supply algorithm stabilizes non-collateralized stablecoins. K. Ito et al. [IMOT20] have categorized stablecoins into four collateralization categories: fiat, commodity, crypto and non-collateralized. The authors also mention non-collateralized stablecoins having the potential to become a part of a DPS.

One of the main problems of stablecoins is that blockchains and smart contracts cannot interact with the 'outside world', so they cannot easily get the current price value of the pegged asset, which is needed to stabilize the stablecoin. The stablecoin report [squ] mentions several ways to implement oracles to input price data into the stablecoin smart contract: a) a centralized trusted server, b) a semi-decentralized solution, where decentralized governance chooses which price feed data providers to use and c) a decentralized solution which uses a Schelling-point public betting contest, where statistically 'incorrect' results are penalized and 'correct' results are incentivized. The report also mentions the Stablecoin Trilemma that states that only two of three goals can be achieved simultaneously with cryptographic stablecoins: a) capital efficiency, b) collateralization and c) decentralization. The stablecoin trilemma is compared with the Impossible Trilemma of traditional economics (Mundell–Fleming Trilemma).

F. M. Ametrano's stablecoin proposal [Ame16] is Hayek Money, which uses dynamical rebasing to change the number of coins in wallets. M. Morini [Mor14] says that Hayek Money only stabilizes unit-of-account but not store-of-value, and Bitcoin only stabilizes store-of-value but not unit-of-account. Morini's stablecoin proposal is having two types of wallets: Investment (Inv) wallets (the software 'central bank' can affect this wallet) and Savings (Sav) wallets (the software 'central bank' does not touch coins in this wallet). R. Sams [Sam15] states that cryp-

tocurrency price stability is not only about stabilizing unit-of-account but also store-of-value. Hayek Money is just as volatile as bitcoin, and Morini's Scheme of Inv and Sav wallet also has a problem: if the price development has predictability, people will transfer all their money to either an Investment wallet if demand goes up or to a Savings wallet if demand goes down. The proposed solution by Sams is the seigniorage shares, that is, two types of coins: money coins and share coins. The seigniorage method also has a problem of speculators not buying shares or bonds [IMOT20].

2.6 Grid Computing, Volunteer Computing

Grid computing or, more specifically, volunteer computing, is computing that uses the spare computing power of, usually, a user's home computer devices to solve some scientific problems such as protein folding (Folding@home), climate modeling simulations (Climateprediction.net) or finding evidence of extraterrestrial intelligence (SETI@home).

Hundreds of scientific publications have been made regarding BOINC (Berkeley Open Infrastructure for Network Computing) projects [boib, boia]. Kondo et al. [KJM+09] compare cloud computing to volunteer computing, finding that clouds offer a homogeneous resource pool (by using Virtual Machines) and volunteer grids offer a heterogeneous resource pool (many kinds of devices and operating systems). Clouds are based on a large-scale centralized server with network-attached storage that is usually located at different geographical locations worldwide. Volunteer grids' resources, such as data access, storage and computation, are located at different geographical locations worldwide, but they are often operated across volatile, low-bandwidth and high-latency Internet connections.

Despite the technical problems with volunteer computing, it has served as a precursor to decentralized cryptocurrency/blockchain networks such as Bitcoin. Cryptocurrencies combine the ideas from volunteer computing and peer-to-peer file sharing software such as BitTorrent. Cryptocurrency mining uses home computing resources to solve mathematical problems (generating random-like hashes), such as volunteer computing projects like Folding@home and SETI@home. The difference is that cryptocurrency mining is generally not carrying out any scientifically useful computations besides securing the blockchain. Cryptocurrencies usually use blockchain technology to distribute the ledger in a peer-to-peer network, such as BitTorrent software, which uses a peer-to-peer network to share files among users.

2.7 Unconventional Computing

Conventional computing is usually classical, electrical, digital, binary and irreversible, and unconventional computing is any computing that is not conventional. Some interesting forms of unconventional computing include analog computing, optical computing, ternary computing, reversible computing and quantum computing.

Quantum computing is probably the most popular topic in unconventional computing. Usually, any computing that is not quantum computing is classical computing, which means that information handling is based on the rules of classical physics, even if the classical computers themselves might have some parts that use quantum physics in one way or another. For example, quantum tunneling effects must be considered when developing modern chips. Quantum computing may pose some security risks in many areas, including cryptocurrencies. For example, Baniata et al. [BK22] have found that thousands of qubits (quantum bits) are required to attack Bitcoin; they also mention that the most advanced quantum computer in May 2022 had 433 qubits.

Ternary computing is based on three digits (trinary digits or trits), and it already has some cryptocurrency applications: the IOTA Beginners Guide [iot] mentions that a ternary system will lead to energy and space savings. Some calculations are more efficient in ternary than binary, because balanced ternary can handle both negative and positive values easily.

Optical computing uses light waves (photon particles) for information processing, storage, and communication. There is a project that aims to change Bitcoin's Proof-of-Work to Optical Proof-of-Work (oPoW) [DBKP20]. The change could decouple Bitcoin mining from energy, shifting the operating expenses (OPEX) to capital expenses (CAPEX).

Reversible computing. Reversible computing is a form of unconventional computing that does not erase information. According to

$$E = k_{\mathrm{B}} T \ln(2)\,, \tag{4}$$

erasing one bit of information at room temperature of 293.15 kelvins generates about $2.805 \cdot 10^{-21}$ joules of heat. There are predictions that, by the 2050s, reversible computing could be at least a thousand times as cost-effective as irreversible computing.

One of the problems of reversible computer architectures is the usage of 'scratch memory', which is used to store the intermediate results. The amount of data tends to be huge, so simple forms of reversible computers need a large amount of scratch memory. More complicated forms of reversible computers might have solutions to this huge memory usage issue. The second problem of reversible computing is that the charging and discharging of circuit elements probably need to be adiabatic as well. The rules [Lew17] are as follows:

1. A switch should not be turned on when a significant voltage difference exists between the channel terminals.

2. A switch should not be turned off when a significant electrical current flows through the switch's channel.

A common misconception is that reversible computing could reverse any output of the SHA256 hashing function. Without all the outputs of R-SHA256 (the reversible version of the SHA256 function), it is generally not possible to reverse the output of SHA256 alone.

3 KEY CONTRIBUTIONS

This chapter discusses the key contributions of all the articles.

3.1 Article PI: 'Collective Behavior of Price Changes of ERC-20 Tokens'

Network of Price Fluctuations. The price data of 541 ERC-20 tokens were collected and analyzed for the period 2016 to 2019. The Pearson correlation coefficient between those tokens' returns was calculated using Equations (1) and (2). A sliced network was created by keeping only the links (edges) formed by those correlations with a value higher than the 95th percentile. The three formed networks are described in Table 6.

TABLE 6 Characteristics of the ERC-20 token networks for the three studied years. The years 2015 and 2016 are omitted because of insufficient data.

year	# nodes	# edges
2017	8	2
2018	111	306
2019	333	2781

Table 7 shows the top five nodes with the highest degrees for the years 2018 and 2019, providing some evidence that many ERC-20 tokens have numerous links to other tokens, meaning that the degree distributions do not follow the power-law that is found in many real-world graphs, including the stock market.

He et al. [HI22] use econometrically robust tests to study the predictability of cryptocurrency returns and prices. The authors state that the properties of heterogeneity, volatility clustering, nonlinear dependence, and heavy tailedness are more evident in non-developed markets like the cryptocurrency market; article PI does not find groupings or hierarchies, possibly providing further evidence that the ERC-20 cryptocurrency market is not developed.

TABLE 7 The top five nodes by degree for the years 2018 and 2019.

year 2018		year 2019	
token	degree	token	degree
BNT	41	OMG	125
CVC	31	SNT	111
POWR	30	GNT	107
OMG	29	MKR	107
LEND	28	AE	106

3.2 Article PII: 'On Creation of a Stablecoin Based on the Morini's Scheme of Inv&Sav Wallets and Antimoney'

3.2.1 Money and antimoney

Initially, the motivation for antimoney came from the need to stabilize the economy against the effects of credit money creation [SSB14]. Antimoney is, therefore, based initially on the credit money of commercial banks (see Section 2.1.4). Antimoney in the present Ph.D. thesis is meant to be a blockchain-based entity. For example, Article PII proposes the antimoney version of bitcoin (BTC) to be called 'antibitcoin' ('aBTC'). The proposed improvement on Morini's stablecoin scheme also takes advantage of antimoney to enable trading in situations where money funds are frozen.

3.2.2 Improving Morini's stablecoin

Rebasement of the Investment wallet means changing the size of the money supply (increasing or decreasing the amount of money in the economy). The problem with Morini's stablecoin scheme is that people can game the system when there is a chance of predicting price changes before the Investment wallet rebasement. The proposed solution is to freeze the balance in the Savings wallet and then use antimoney to continue trading in the economy.

Because it is not clear from Morini's paper [Mor14], the two rebasement equations (5) and (6) for calculating the balance in Investment wallets were formed and compared with each other:

$$\Delta I_i(t) = \frac{I_i(t-1)}{\sum_{j=1}^{n} I_j(t-1)} \cdot \Delta M(t) \tag{5}$$

and

$$\Delta I_i(t) = \frac{M_i(t-1)}{\sum_{j=1}^{n} M_j(t-1)} \cdot \Delta M(t) \tag{6}$$

with the following definitions

$$\Delta I_i(t), I_i(t-1), \Delta M(t), M_i(t-1) : T \longrightarrow \mathbb{R}.$$

Please, refer to Article PII for a detailed explanation of the equations. Equation (6) was fairer to the agents, because it distributed the change of money supply among all the agents. The problem of negative balances was present when using either of the two equations. Freezing some of the balance in the Savings wallet and using antimoney to do trading if there are not enough useable (non-frozen) money funds available was proposed to solve the problem.

3.2.3 Decentralized credit cards

It is said that bitcoin is not popular because it does not replace credit cards. With a credit card, a person can buy something without actually having enough money funds on hand. The money comes from a credit card company or bank, and the person needs to pay them back later with a (usually) modest interest.

With antimoney, the person can buy goods and services and take antimoney from the seller. The difference when compared with credit cards is that the person does not pay antimoney back to the seller; instead, the person needs to give it forward in the economy. The decentralization of credit cards fits the decentralization philosophy behind bitcoin and other cryptocurrencies. Article PII might be the first paper to bring decentralized credit to the blockchain world.

3.2.4 New method to distribute cryptocurrencies

The usual methods to distribute cryptocurrency include the following:

- buying cryptocurrency with fiat money
- receiving free cryptocurrency from airdrops
- getting cryptocurrency from mining

Buying cryptocurrency with fiat money is usually the easiest way to get into the cryptocurrency world. The problem with this method is the centralization and dependency on the fiat world. Getting cryptocurrencies with this method would be challenging if laws ban cryptocurrency exchanges.

Receiving free cryptocurrency from airdrops is a popular method to get new cryptocurrencies. In the early years of bitcoin, there were bitcoin faucets on the Internet where people could send their bitcoin address and then receive free bitcoins with (then) a small monetary value. Of course, bitcoins' value has drastically increased over the years and could be worth hundreds of euros, if not thousands of euros, at today's exchange rates. With other cryptocurrencies, the usual method to distribute them is the airdrop method, which is possible at the early stages of a new cryptocurrency when the monetary value is near zero. The problem with this method is that it works more efficiently only when the value of the cryptocurrency is near zero. Otherwise, the creators of the airdrop would have to make a considerable investment.

Another problem is that the airdrop method could lead to pump-and-dump schemes where the cryptocurrency creators will artificially raise (pump) the value of the cryptocurrency to make their cryptocurrency holdings more valuable in

relation to fiat money. Then, they will sell (dump) their holdings to get lots of fiat money. After a while, the value of the cryptocurrency might go to zero again because there might be no project leaders left to further develop or manage the cryptocurrency.

Getting cryptocurrency from mining can be considered a very industrialized process nowadays. In the early days, bitcoin mining was possible for anyone owning a computer with an Internet connection. The CPU of the computer was used to run the bitcoin mining algorithm. Nowadays, bitcoin mining can be profitable for customers of data centers with hundreds of expensive and noisy ASIC bitcoin mining devices and who have an access to cheap electricity.

Article PII has suggestd a fourth method to distribute cryptocurrencies / cryptomonies: agents can give massive amounts of cryptocurrencies away without changing their monetary wealth. For example, if 1 bitcoin (BTC) is worth 40,000 euros and 1 antibitcoin (aBTC) is worth $|-20{,}000|$ euros, then by giving away 1 BTC and 2 aBTC at the same time, the monetary wealth of the giver has changed by 0 euros. The monetary wealth of the receiver has also changed by 0 euros, which can be calculated from Equation (3) as follows:

$$\begin{aligned} 0\,\mathrm{EUR} &= 40{,}000\,\mathrm{EUR} - 2 \cdot 20{,}000\,\mathrm{EUR} = 1\,\mathrm{BTC} - 2 \cdot \frac{1}{2}\,\mathrm{BTC} = 1\,\mathrm{BTC} - 2 \cdot \frac{\mathrm{BTC}}{2} \\ &= 1\,\mathrm{BTC} - 2\,\mathrm{aBTC} = \omega. \end{aligned} \tag{7}$$

3.3 Article PIII: 'Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators'

3.3.1 Deflationary bitcoin (BTCd) and inflationary bitcoin (BTCi)

Sometimes, bitcoin (BTC) is considered to be a deflationary currency. These claims are usually based on the fact that there is a cap of 21 million bitcoin coins in total. The limit of 21 million BTC coins will be reached around the year 2140. There is also the effect of people losing access to their private keys, so some coins will be lost forever. Based on these facts, the value of bitcoin should go up eventually. There are many other reasons why the value of bitcoin might not increase.

Article PIII has termed the regular bitcoin (BTC) a deflationary bitcoin (BTCd). Deflationary bitcoin is probably good for savings, at least when the value of bitcoin is steadily increasing, but it might not be suitable for spending on everyday goods and services. People like to hold bitcoins because their value might increase significantly in the near future.

Bitcoin was originally meant to be a payment system [nak]. One potential solution to make the Bitcoin economy more open for everyday payments could be through introducing a second coin type with different features, a different exchange rate and a different currency unit to separate it from the original bitcoin cryptocurrency. Article PIII has termed the second coin type inflationary bitcoin,

giving it the currency unit of BTCi. Inflationary bitcoin does not necessarily have any upper limit cap of coin supply. For comparison, deflationary bitcoin has a limit of 21 million coins. There are already cryptocurrencies with unlimited supplies: dogecoin (DOGE) is one example.

The second coin would most likely increase the number of transactions in the Bitcoin network, so miners using the new – and still BTCd-profitable – mining devices would also take advantage because they would collect more transaction fees.

3.3.2 Reducing e-waste

The problem of e-waste in bitcoin mining means that the lifetime of an ASIC miner is around one and a half years [dV19]. Because ASIC Bitcoin miners can only calculate SHA256d hashes, they cannot be repurposed to do any general computations. For comparison, old graphics cards that are too slow for modern video games can be repurposed to do scientific calculations using their Graphics Processing Units (GPU). The proposed solution to the e-waste problem in Article PIII was to introduce inflationary bitcoin (BTCi) to motivate the old mining hardware users to keep their devices online, even though they are not profitable in mining deflationary bitcoin (BTCd) cryptocurrency. The old hardware could still seed PRNGs and make the network more valuable to Internet users. The reward for this work would be given as the BTCi cryptocurrency. This solution should reduce the amount of e-waste by keeping the old hardware online for many years.

3.3.3 Recycling hashes

Article PIII estimated that, in late 2021, about 10^{28} hashes had been generated during bitcoin mining since the beginning of the Bitcoin blockchain. Because one SHA256d hash equals 256 bits, the storage space for storing all those hashes would need to be more than 10^{30} bits. According to estimates, the whole Internet traffic in 2016 was less than 10^{22} bits. Comparing the number of hashes generated (10^{28}) to the Bitcoin block height (about 700,000), which means the number of hashes that are currently accepted as valid tickets for adding a new block to the blockchain, shows that almost all the hashes generated are basically wasted or thrown away. With the current hash rate of 190 EH/s ($190 \cdot 10^{18}$ H/s), there will be about $6 \cdot 10^{27}$ hashes generated annually. Could at least some of these otherwise wasted hashes be used in some way before they are thrown away?

LavaRand is a method to seed Pseudorandom Number Generators (PRNG) by binary numbers coming from digital pictures of lava lamps [NMS98]. The process of bubbles moving inside the lava lamp is random, so the images of the bubbles are also random. LavaRand is an exciting method to seed PRNGs. The method can produce good enough random numbers for the usage of public servers [mcn].

Article PIII on simulated bitcoin mining found that the hashes generated and then turned into binary numbers have almost an equal number of ones and

zeros, so they are considered good seeds for PRNGs. This idea of recycling hashes and seeding pseudorandom number generators came from the LavaRand method, but instead of taking pictures of lava lamps, the research proposed using the hashes from bitcoin mining that seem to be random.

3.3.4 Reversible bitcoin mining

Article PIII might be one of the first research papers proposing the usage of reversible computing for bitcoin mining. The first motivation is the prediction that reversible computing could be thousands of times as cost-effective as irreversible computing in the future. The second motivation is the resemblance between the concept of hash recycling and need for scratch memory in reversible computers.

The paper then estimated the bandwidth needed for such activities, concluding that recycling every hash generated during bitcoin mining over Internet connections is impossible. It is probably not convenient to use cloud-based scratch memories for reversible computers.

3.4 Article PIV: 'A Survey on Technologies Which Make Bitcoin Greener or More Justified'

3.4.1 New categories for sustainable cryptocurrencies

Article PIV categorized sustainable cryptocurrency technologies as Green, Justification and 'Mix of Both'.

Conventional monies usually have one property more than conventional currencies: the store-of-value. The categorization done for this survey suggests that there should be two more properties for sound cryptomonies:

- greenness
- justness

Greenness means that the energy usage of the cryptomoney's whole infrastructure needs to be optimized. Justness means that the consensus-forming process of the cryptomoney's ledger (usually implemented as a blockchain) needs to do something scientifically valuable.

3.4.2 Different forms of computing

One contribution of Article PIV is Table 8, which describes most of the major forms of conventional and unconventional computing. Conventional computing is usually classical, digital, electrical, binary and irreversible. There are many different forms of unconventional computing, and most overlap in one way or another.

It is noteworthy that the world of cryptocurrencies is already using some forms of unconventional computing. OPoW might soon replace Bitcoin's SHA256

TABLE 8 Different forms of computing. Source: Article PIV.

Different forms of computing	
Category	Explanation
digital	Conventional computing, which uses discrete or discontinuous values to represent information.
analog	Unconventional computing, which uses continuous ranges of values to represent information.
binary	Conventional digital computing, which uses two-valued logic.
ternary	Unconventional digital computing, which uses three-valued logic.
decimal	Unconventional digital computing, which uses 10-valued logic.
irreversible	Conventional computing, which erases information and where going back to the previous state of the calculation is generally not possible.
reversible	Unconventional computing, which does not erase information and where going back to the previous state of the calculation is possible.
electrical	Conventional computing, which is controlled by electrical circuits.
mechanical	Unconventional computing, which is controlled mechanically.
DNA	Unconventional computing, where the huge parallelization of the deoxyribonucleic acid is being used.
optical	Unconventional computing, where computations, data transfer and storage are done using optical methods.
classical	Conventional computing, where classical physics is used to process information.
quantum	Unconventional computing, where quantum physics phenomena are being used to process quantum information.

Proof-of-Work, and the ternary system has been used for IOTA cryptocurrency since the beginning of IOTA.

3.4.3 Distributed Computing Grid Cryptocurrencies

One contribution of Article PIV is the finding that the market capitalizations of Distributed Computing Grid Coins, this is, gridcoin (GRC), curecoin (CURE) and foldingcoin (FLDC), are significantly lower than the market capitalizations of bitcoin (BTC) and ether (ETH). This finding hints at the fact that the coins associated with scientific computing are not used or mined on a large scale.

Ethereum has very advanced smart contracts that could be used to implement customizable PoW for token mining. Perhaps this is one possibility of introducing Distributed Computing Grid Tokens for a larger audience.

3.5 Article PV: 'Bitcoin Mining Could Revolutionize Grid Computing and Unconventional Computing'

Cryptocurrency Mining, Grid Computing, and Unconventional Computing. Article PV has shown an intense but usually unseen connection among cryptocurrency mining, grid computing, and unconventional computing.

The connection between cryptocurrency mining and grid computing are the cryptocurrencies gridcoin, curecoin and foldingcoin, which use either BOINC or Folding@home software during the mining process.

The connection between cryptocurrency mining and unconventional computing is optical and reversible computing. There is an optical computing project of oPoW that tries to replace the SHA256d hashing algorithm with a more suitable hashing algorithm designed to be used in an optical computing chip. This change could lower the energy usage of Bitcoin mining and make mining profitable in locations where electricity is expensive. A proposal for using reversible computing in Bitcoin mining was made in Article PIII. The proposal was justified because the Bitcoin ASIC mining industry was jump-started with small companies with meager budgets.

4 SUMMARY OF ARTICLES

This chapter summarizes the included articles in the present dissertation. The aim, results and the author's contributions are explained.

4.1 Summary of Article PI

HEINONEN, Henri T.; SEMENOV, Alexander; BOGINSKI, Vladimir. Collective behavior of price changes of ERC-20 tokens. In: International Conference on Computational Data and Social Networks. Springer, Cham, 2020. p. 487-498. JuFo 1.

Aim

The article addresses the problem of the collective behavior of price changes of tokens on the Ethereum blockchain.

Results

For the price change behavior of tokens in the same blockchain, networks based on cross-correlation of ERC-20 tokens' returns are constructed and analyzed using Equation (1). Please, refer to Article PI for a detailed explanation of the equation.

The degree distributions of the resulting graphs do not follow the power law degree distribution. Also, these methods do not find any groupings or hierarchical structures of ERC-20 tokens. For comparison, Boginski et al. [BBP03, BBP06] have found a stable power-law structure of a market graph representation of the stock market. Boginski et al. [BBP03] also mention that the stock market could be considered a self-organized system.

The limitation is the small number of nodes: 111 for 2018 and 333 for 2019. Also, the period of 12 months might be too long for good analysis, so it suggested

to use periods of 3 months in future research. Shirokikh et al. [SPS+22] also mention shorter periods for stock market studies.

Author's Contribution

The author searched for various ERC-20 tokens for the analysis, did most of the literature analysis and wrote parts of the article.

4.2 Summary of Article PII

HEINONEN, Henri T. On Creation of a Stablecoin Based on the Morini's Scheme of Inv&Sav Wallets and Antimoney. In: 2021 IEEE International Conference on Blockchain (Blockchain). IEEE, 2021. p. 409-416. JuFo 1.

Aim

The article addresses the problem of creating non-collateralized stablecoins.

Results

For the problem of creating a non-collateralized stablecoin, Morini's stablecoin scheme is taken into consideration. The scheme involves two different wallets: an Investment wallet and Savings wallet. A rebasement is sometimes needed to change the money supply (adding or removing money in the Investment wallets). The concept of antimoney from econophysics was added to the mix to enable trading, even when the Savings wallet balances are frozen. The proposed solution is novel because antimoney (a form of negative money) has probably never been proposed or used in blockchain applications.

Author's Contribution

The author designed the new version of Morini's stablecoin scheme with the concepts of freezing the Savings wallet balance and enabling antimoney. The author also performed the calculations, plotted the figures and wrote the article.

4.3 Summary of Article PIII

HEINONEN, Henri T.; SEMENOV, Alexander. Recycling hashes from reversible bitcoin mining to seed pseudorandom number generators. In: International Conference on Blockchain. Springer, Cham, 2021. p. 103-117. JuFo 1.

Aim

The article addresses the problem of the wasteful generation of SHA256 hashes during bitcoin mining.

Results

For the problem of the wasteful generation of SHA256 hashes, the paper proposes two different solutions. The more realistic (as of today's technology) solution is to recycle hashes to seed pseudorandom number generators (PRNGs) over an Internet connection. The more difficult solution is to develop bitcoin mining chips based on the principles of reversible computing, which is a form of unconventional computing. It was calculated that the number of hashes generated on a regular ASIC Bitcoin miner is so huge that it is entirely impractical to recycle all of them over today's Internet connections. It is also impractical to have cloud-based scratch memory for reversible bitcoin mining. By analyzing the bitcoin Genesis block mining, it is found that the SHA256 hashes generated have an almost equal number of ones and zeros in a binary format. Based on this analysis, bitcoin mining could be suitable for seeding PRNGs.

Author's Contribution

The author proposed the idea of hash recycling and the idea of using reversible computing for bitcoin mining. The author also analyzed the hashes of Bitcoin's Genesis block and wrote most of the article.

4.4 Summary of Article PIV

HEINONEN, Henri T., et al. A Survey on Technologies Which Make Bitcoin Greener or More Justified. IEEE Access, 2022, 10: 74792-74814. JuFo 2.

Aim

The article addresses the problem of bitcoin and many other cryptocurrencies not being green nor doing practical activities (besides securing the blockchain) during the Proof-of-Work mining process.

Results

For the problem mentioned above, the paper introduced two categories of 'Green' and 'Justification' for blockchain/cryptocurrency technologies. There was also a third category of 'Mix of Both' because some technologies did not fit either the 'Green' or 'Justification' category. It was also estimated if the technology in question was helpful for the bitcoin cryptocurrency shortly. The paper also lists

the technologies used for unconventional computing; this list is given in Table 8.

Author's Contribution

The author invented the categorizations of 'Green', 'Justification', and 'Mix of Both' and searched for the appropriate technologies for categorization. The author designed the paper's scope and wrote most of the paper.

4.5 Summary of Article PV

It has not yet been published in Computer (IEEE Computer Society, ISSN 0018-9162). JuFo 2.

Aim

The article addresses the problem of unused computing cycles available in home computer gadgets accessible through an Internet connection.

The second problem is the lack of motivation to research and develop unconventional computing chips like optical and reversible computing.

Results

For the problem of unused computing cycles of home computing devices, an estimation is given for the amount of computing power available in smartphones during the recharging period of about one hour per day. It is calculated that the daily computing power available in the world's smartphones during a one-hour recharging period alone is so enormous (0.73 exaFLOPS) that it is comparable to the fastest supercomputers (1.1 exaFLOPS).

For the problem of the lack of motivation for R&D in unconventional computing, it is mentioned that the Bitcoin ASIC industry was jump-started by small companies motivated to carry out Bitcoin mining. During the article's writing, customized GPU cards did already exist for cryptocurrency miners. Also, large chip makers, like Intel, were going into Bitcoin ASIC industry during this time.

Author's Contribution

The author proposed linking cryptocurrency mining, grid computing and unconventional computing. The author wrote more than half of the entire article.

5 CONCLUSION

Based on the research done for the present Ph.D. thesis, a sound cryptomoney has the following 15 properties: scarcity, durability, divisibility, verifiability (or recognisability), storability, portability (or transportability), fungibility, non-counterfeitability, useability, medium-of-exchange (or means-of-payment), unit-of-account, store-of-value, standard-of-deferred-payment, greenness, and justness.

Bitcoin is still the most popular cryptocurrency, but the challenges (climate and environment) of the world mean that Bitcoin needs to change. Therefore, it is suggested to make the following modifications to Bitcoin (after more research, development, and testing):

(1) Introduce an inflationary bitcoin coin (BTCi) for motivating bitcoin spending and increasing the lifetime of ASIC mining devices (reducing e-waste).

(2) Introduce an antimoney bitcoin coin (aBTC) to enable decentralized credit and decentralized finance and make the bitcoin distribution model safe against attacks on crypto exchanges.

(3) Recycle hashes from bitcoin mining devices to seed pseudorandom number generators to increase the societal value of Bitcoin.

(4) Develop unconventional computing methods (such as optical and reversible) for bitcoin mining.

(5) Introduce a Hybrid PoW & "PoX" consensus model, where Bitcoin ASIC mining is still possible, but some of the blocks are generated by a novel Proof-of-X method ("PoX" could be Proof-of-Stake or something else, e.g., a system that does protein folding simulations).

(6) Introduce a non-collateralized stablecoin for the Bitcoin blockchain to enable a Decentralized Payment System and peg it to the basket of reserve currencies.

Earlier, it was mentioned that bitcoin is

(a) commodity money without gold,

(b) fiat money without a state,

(c) credit money without debt, and

(d) digital crude oil.

As a counterargument for (a), it is probably safe to say that bitcoin's commodity is the technical infrastructure built around it. At the moment, that infrastructure is mostly the Bitcoin ASIC mining industry. In the future, it could be a network of optical and reversible computers securing the blockchain, or it could be a new "Proof-of-X" system that does scientifically useful calculations, or it could also be a Proof-of-Stake system, or it could be something entirely different. The recent upgrade of Ethereum (the Ethereum Merge that enabled Proof-of-Stake) proves that big changes are possible even for cryptocurrencies with huge market capitalizations. Bitcoin could also see such significant changes shortly. As a counterargument for (b), Internet communities could be seen as state-like entities. For example, there is a clear organizational structure for open source projects like the Bitcoin Core, the most popular software to connect to the original Bitcoin (BTC) network. As a counterargument for (c), the research for this Ph.D. thesis introduced the concept of antimoney to the blockchain world. The antimoney itself is the debt that is given forward in the economy instead of paying it back to the original lender. A software upgrade to Bitcoin could introduce the antimoney counterpart of bitcoin. As a counterargument for (d), the research for this Ph.D. thesis introduced many Green and Justification technologies for turning the bitcoin cryptocurrency into a sustainable cryptomoney.

YHTEENVETO (SUMMARY IN FINNISH)

Tähän väitöskirjaan tehdyn tutkimuksen pohjalta voidaan todeta, että kelvollisella kryptorahalla on peräti viisitoista ominaisuutta. Erona kelvollisella kryptorahalla tyypillisiin kryptovaluuttoihin ovat arvonsäilyttäjäfunktio ja laskentayksikköfunktio, jotka vakaakolikkotekniikoilla vakauttavat kryptorahan arvon. Pari uutta ehdotettua ominaisuutta ovat vihreys ja oikeudenmukaisuus, jotka tekevät kryptorahoista ekologisesti kestäviä. Nämä ominaisuudet saavutetaan uusilla laskennan menetelmillä kuten grid-laskennalla ja epätavanomaisella laskennalla.

Artikkeli PI käsittelee ERC-20-rahakkeiden hintaerotusten käyttäytymistä, koska on tarpeellista ymmärtää tulevia monen rahan kryptoekonomioita.

Artikkeli PII pyrkii ratkaisemaan Morinin vakaakolikkojärjestelmää vaivaavan ongelman, jossa rahavarannon uudelleenperustamisen (eli rahan luonti kiertoon tai rahan poisto kierrosta) ennustettavuus saa käyttäjät pelaamaan järjestelmää vastaan siirtämällä omaisuuteensa joko investointilompakkoon (johon "keskuspankkialgoritmi" vaikuttaa) tai talletuslompakkoon (johon "keskuspankkialgoritmi" ei voi vaikuttaa). Ongelma pyritään ratkaisemaan siten, että talletuslompakon saldo voidaan tarvittaessa jäädyttää, ja kaupankäynti mahdollistuu antirahan avulla. Samalla antiraha mahdollistaa aivan uuden tavan jakaa kryptorahaa ekonomiaan.

Artikkeli PIII esittelee tiivisteiden kierrättämisen oikeutusteknologiana (eli arvoa kasvattavana teknologiana) ja reversiibelin bitcoin-louhinnan vihreänä teknologiana (eli energiankäyttöä vähentävänä teknologiana).

Artikkeli PIV esittelee suuren joukon kryptovaluuttateknologioita ja jakaa ne kolmannessa artikkelissa tutuksi tulleisiin vihreisiin ja oikeuttaviin teknologioihin - lisäksi kolmantena teknologiakategoriana on "sekoitus molempia".

Artikkeli PV nostaa esiin selvän yhteyden kolmen erilaisen laskennan välille: kryptovaluuttalouhinnan, grid-vapaaehtoislaskennan ja epätavanomaisen laskennan. Nämä erilaiset laskennan muodot ovat jo edesauttaneet toistensa kehittymistä ja voivat jatkossa yhä voimakkaammin tukea toisiaan.

Lyhyesti voidaan todeta, että väitöskirjatyöllä yritetään motivoida kryptovaluuttalouhintaorganisaatioita kehittämään epätavanomaisen laskennan muotoja ja grid-laskentaa.

REFERENCES

[AACT18] Richard Thompson Ainsworth, Musaad Alwohaibi, Mike Cheetham, and Camille Tirand. A vatcoin solution to mtic fraud: Past efforts, present technology, and the eu's 2017 proposal. *Boston Univ. School of Law, Law and Economics Research Paper*, (18-08), 2018.

[Ame16] Ferdinando M Ametrano. Hayek money: The cryptocurrency price stability solution. *Available at SSRN 2425270*, 2016.

[bana] The economics of digital currencies | bank of england. https://web.archive.org/web/20220901132336/https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/the-economics-of-digital-currencies.pdf?la=en&hash=E9E56A61A6D71A97DC8535FEF211CC08C0F59B30. Accessed: 2022-09-01.

[banb] Money creation in the modern economy | bank of england. https://web.archive.org/web/20220901044603/https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-creation-in-the-modern-economy.pdf?la=en&hash=9A8788FD44A62D8BB927123544205CE476E01654. Accessed: 2022-09-09.

[BBL+20] Jonathan Beller, Dick Bryan, Benjamin Lee, Jorge Lopez, and Akseli Virtanen. Rethinking money and credit in a cryptoeconomy: Securing liquidity without the need for central control of issuance, 2020.

[BBP03] Vladimir Boginski, Sergiy Butenko, and Panos M Pardalos. On structural properties of the market graph. *Innovations in financial and economic networks*, 48:29–35, 2003.

[BBP06] Vladimir Boginski, Sergiy Butenko, and Panos M Pardalos. Mining market data: A network approach. *Computers & Operations Research*, 33(11):3171–3184, 2006.

[bit] A successful double spend us$10000 against okpay this morning. | bitcoin forum. https://web.archive.org/web/20160322151247/https://bitcointalk.org/index.php?topic=152348. Accessed: 2022-10-02.

[Bje16] Ole Bjerg. How is bitcoin money? *Theory, culture & society*, 33(1):53–72, 2016.

[BJL19] Markus K Brunnermeier, Harold James, and Jean-Pierre Landau. The digitalization of money. Technical report, National Bureau of Economic Research, 2019.

[BK22] Hamza Baniata and Attila Kertesz. Bitcoin revisited: Formalization, benchmarking, and open security issues. 2022.

[BN19] Markus K Brunnermeier and Dirk Niepelt. On the equivalence of private and public money. *Journal of Monetary Economics*, 106:27–41, 2019.

[boia] Boincpapers | boinc. https://web.archive.org/web/20220531082449/https://boinc.berkeley.edu/trac/wiki/BoincPapers. Accessed: 2022-09-19.

[boib] Publications by boinc projects | boinc. https://web.archive.org/web/20220914221508/https://boinc.berkeley.edu/wiki/Publications_by_BOINC_projects. Accessed: 2022-09-19.

[BS18] Aleksander Berentsen and Fabian Schär. The case for central bank electronic money and the non-case for central bank cryptocurrencies. 2018.

[DBKP20] Michael Dubrovsky, M Ball, Lucianna Kiffer, and B Penkovsky. Towards optical proof of work. *Cryptoeconomic Systems*, 11, 2020.

[dec] The day someone created 184 billion bitcoin | decrypt. https://web.archive.org/web/20200903232812/https://decrypt.co/39750/184-billion-bitcoin-anonymous-creator. Accessed: 2022-10-02.

[dV19] Alex de Vries. Renewable energy will not solve bitcoin's sustainability problem. *Joule*, 3(4):893–898, 2019.

[ecb] Overview of virtual currency schemes | european central bank. https://web.archive.org/web/20130626091722/http://globalforumljd.org/docs/events/061413/061413_ppt_ecb.pdf. Accessed: 2022-08-29.

[eth] Ethereum network hash rate chart | etherscan. https://web.archive.org/web/20220921212254/https://etherscan.io/chart/hashrate. Accessed: 2022-09-22.

[eu.] Europeans can now make cash purchases on the information superhighway | eunet. https://web.archive.org/web/19970203224938/http://www.eu.net/press/press960313ecash.html. Accessed: 2022-09-27.

[eur] Mtic (missing trader intra community) fraud | europol. https://web.archive.org/web/20220901042919/https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud. Accessed: 2022-09-19.

[FVS19] Jesús Fernández-Villaverde and Daniel Sanches. Can currency competition work? *Journal of Monetary Economics*, 106:1–15, 2019.

[FVSSU21] Jesús Fernández-Villaverde, Daniel Sanches, Linda Schilling, and Harald Uhlig. Central bank digital currency: Central banking for all? *Review of Economic Dynamics*, 41:225–242, 2021.

[hac] Stablecoins: designing a price-stable cryptocurrency | hackernoon. https://web.archive.org/web/20180504155956/https://hackernoon.com/stablecoins-designing-a-price-stable-cryptocurrency-6bf24e2689e5. Accessed: 2022-10-03.

[hel] Elektra-projektin loppuraportti: 8. elektroniset maksujärjestelmät. https://web.archive.org/web/20210928040451/https://elektra.helsinki.fi/raportti/8.html. Accessed: 2022-09-27.

[HI22] Siyun He and Rustam Ibragimov. Predictability of cryptocurrency returns: evidence from robust tests. *Dependence Modeling*, 10(1):191–206, 2022.

[ilt] Asiantuntija petteri järvinen ihmettelee: S-pankki huomasi tietoturvaongelman myöhään | iltalehti. https://web.archive.org/web/20220914155925/https://www.iltalehti.fi/digiuutiset/a/28886125-7e57-4faa-9241-a79b103e125d. Accessed: 2022-09-14.

[IMOT20] Kensuke Ito, Makiko Mita, Shohei Ohsawa, and Hideyuki Tanaka. What is stablecoin?: A survey on its mechanism and potential as decentralized payment systems. *International Journal of Service and Knowledge Management*, 4(2):71–86, 2020.

[Ing13] Geoffrey Ingham. *The nature of money*. John Wiley & Sons, 2013.

[iot] Ternary systems | iota beginners guide. https://web.archive.org/web/20220513200417/https://iota-beginners-guide.com/future-of-iota/iota-x-0-ternary-vision-abandoned/ternary-systems/. Accessed: 2022-05-13.

[JGB22] Benjamin A Jones, Andrew L Goodkind, and Robert P Berrens. Economic estimation of bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold. *Scientific Reports*, 12(1):14512, 2022.

[KJM+09] Derrick Kondo, Bahman Javadi, Paul Malecot, Franck Cappello, and David P Anderson. Cost-benefit analysis of cloud computing versus desktop grids. In *2009 IEEE International Symposium on Parallel & Distributed Processing*, pages 1–12. IEEE, 2009.

[Lew17] Ted G Lewis. Art scott and michael frank on energy-efficient computing. *Ubiquity*, 2017(September):1–17, 2017.

[LLCZ19] Jiaqi Liang, Linjing Li, Weiyun Chen, and Daniel Zeng. Towards an understanding of cryptocurrency: a comparative analysis of cryptocurrency, foreign exchange, and stock. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 137–139. IEEE, 2019.

[MBY+20] Mohammad Moussa Madine, Ammar Ayman Battah, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, Sasa Pesic, and Samer Ellahham. Blockchain for giving patients control over their medical records. *IEEE Access*, 8:193102–193115, 2020.

[mcn] Totally random | wired. https://web.archive.org/web/20211108233100/https://www.wired.com/2003/08/random/. Accessed: 2022-02-22.

[Mor14] Massimo Morini. Inv/sav wallets and the role of financial intermediaries in a digital currency. *Available at SSRN 2458890*, 2014.

[MS19] Hartmut Müller and Markus Seifert. Blockchain, a feasible technology for land administration. *FIG Working Week: Geospatial information for a smarter life and environmental resilience*, pages 22–26, 2019.

[nak] Bitcoin: A peer-to-peer electronic cash system. https://web.archive.org/web/20211103223918/https://bitcoin.org/bitcoin.pdf. Accessed: 2022-02-22.

[NMS98] Landon Curt Noll, Robert G Mende, and Sanjeev Sisodiya. Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system, March 24 1998. US Patent 5,732,138.

[PTRC07] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[Sam15] Robert Sams. A note on cryptocurrency stabilisation: Seigniorage shares. *Brave New Coin*, pages 1–8, 2015.

[SM15] David Schatsky and Craig Muraskin. Beyond bitcoin. *Blockchain is Coming to Disrupt Your Industry*, 2015.

[Smi76] Adam Smith. *The Wealth of Nations*. 1776.

[SPS+22] Oleg Shirokikh, Grigory Pastukhov, Alexander Semenov, Sergiy Butenko, Alexander Veremyev, Eduardo L Pasiliao, and Vladimir Boginski. Networks of causal relationships in the us stock market. *Dependence Modeling*, 10(1):177–190, 2022.

[squ] The state of stablecoins 2019 - hype vs. reality in the race for stable, global, digital money. https://web.archive.org/web/20220901002130/https://static1.squarespace.com/static/564100e0e4b08c9445a5fc5d/t/5c71e43ef9619ae6c83c30af/1550967911994/The+State+of+Stablecoins+2019_Report+2_20_19.pdf. Accessed: 2022-10-03.

[SSB14] Matthias Schmitt, Andreas Schacker, and Dieter Braun. Statistical mechanics of a time-homogeneous system of money and antimoney. *New Journal of Physics*, 16(3):033024, 2014.

[Sto09] James Stodder. Complementary credit networks and macroeconomic stability: Switzerland's wirtschaftsring. *Journal of Economic Behavior & Organization*, 72(1):79–95, 2009.

[the] Bristol pound gets boost of energy as power company signs up | bristol | the guardian. https://web.archive.org/web/20210419214932/https://www.theguardian.com/uk-news/2015/jun/16/bristol-pound-powered-renewables-good-energy-signs-up. Accessed: 2022-09-13.

[tra] Refuting the ecb - the 9 characteristics that make bitcoin money | tradeblock. https://web.archive.org/web/20160612103556/https://tradeblock.com/blog/refuting-the-ecb-the-9-characteristics-that-make-bitcoin-money. Accessed: 2022-08-29.

[ude] Bitcoin or how i learned to stop worrying and love crypto | udemy. https://web.archive.org/web/20220829125028/https://www.udemy.com/join/login-popup/?next=/course/bitcoin-or-how-i-learned-to-stop-worrying-and-love-crypto/learn/lecture/280010%3Fcomponents%3Dpurchase%252Ccacheable_buy_button%252Cbuy_button%252Crecommendation&__cf_chl_rt_tk=pgPVur9SdYdzfUf_Hs4iOPZ6TcYI55clH8i39lQWhE8-1661777428-0-gaNycGzNCuU. Accessed: 2022-08-29.

[vas] Keskuspankkitili kaikille | vasemmistofoorumi. https://web.archive.org/web/20220121013454/http://vasemmistofoorumi.fi/uusi/wp-content/uploads/2016/08/Aloite-12015-web.pdf. Accessed: 2022-09-19.

[wor] Blockchain: How the fourth industrial revolution can help accelerate progress towards development | the world bank. https://web.archive.org/web/20220412115929/https://www.worldbank.org/en/news/feature/2019/01/24/blockchain-como-asegurarse-que-cada-dolar-llegue-a-quien-lo-necesita. Accessed: 2022-09-27.

[xap] What is bitcoin? the best money in human history | xapo blog. https://web.archive.org/web/20190828063922/https://blog.xapo.com/what-is-bitcoin-the-best-money-in-human-history/. Accessed: 2022-08-29.

ORIGINAL PAPERS

PI

COLLECTIVE BEHAVIOR OF PRICE CHANGES OF ERC-20 TOKENS

by

Henri T. Heinonen and Alexander Semenov and Vladimir Boginski 2020

International Conference on Computational Data and Social Networks (CSoNet 2020)

https://doi.org/10.1007/978-3-030-66046-8_40

Collective behavior of price changes of ERC-20 tokens

Henri T. Heinonen[1][0000−0001−5961−3571], Alexander Semenov[2], and Vladimir Boginski[3]

[1] University of Jyväskylä, Jyväskylä, Finland, henri.t.heinonen@jyu.fi
[2] University of Florida, Gainesville, FL, USA, asemenov@ufl.edu
[3] University of Central Florida, Orlando, FL, USA, vladimir.boginski@ucf.edu

Abstract. We analyze a network constructed from tokens developed on Ethereum platform. We collect a large data set of ERC-20 token prices; the total market capitalization of the token set is 50.2 billion (10^9) US dollars. The token set includes 541 tokens; each one of them has a market capitalization of 1 million US dollars or more. We construct and analyze the networks based on cross-correlation of tokens' returns. We find that the degree distributions of the resulting graphs do not follow the power law degree distribution. We cannot find any hierarchical structures nor groupings of ERC-20 tokens in our analysis.

Keywords: Token · Cryptocurrency · Cross correlation matrix · Degree distribution.

1 Introduction

1.1 History and terminology

Econophysicists have studied complex financial systems using concepts and methods originally developed for studying physical systems [5, 10]. Such methods have also been used to study the collective behavior of price changes of various cryptocurrencies [12].

In 2009, Bitcoin started the revolution of a new form of money and introduced the concept of a blockchain - a special case of a Distributed Ledger Technology (DLT). 'Bitcoin' (with capital 'B') is a protocol and a network. The native currency of the blockchain started by Satoshi Nakamoto is known as 'bitcoin' (with lower case 'b'). The blockchain has split (or forked) into various other blockchains, and their names and currency units differ (BTC for Bitcoin, BCH for Bitcoin Cash, and BSV for Bitcoin SV). The monetary value between these different currencies varies a lot. Their respective blockchain protocols follow different rules. These different splits of the same blockchain all have the same genesis block (the first block of the entire chain) and the same blocks after the genesis block until the block that caused the split event.

There are also completely separate blockchains since the beginning of the chain: for example, Litecoin and Bitcoin do not have the same genesis block.

These completely separate blockchains can be using different rules and/or different hashing algorithms (e.g., Litecoin and Bitcoin) or they can be using the same rules and/or the same hashing algorithms (e.g., Namecoin and Bitcoin).

Ethereum blockchain introduced Turing-complete smart contracts that can be used to create programs that can be run in the supercomputer of the decentralized and distributed network. These smart contracts can be used to create new tokens. Tokens can also have monetary value. The most popular platform for tokens is the Ethereum blockchain and its Ethereum Virtual Machine (EVM) that supports smart contracts. Users are usually creating smart contracts with Solidity language. The ERC-20 standard is for creation of tokens with some basic properties. It is the most used standard for making new tokens. The ERC-20 standard gives three optional (token name, symbol, number of decimals) and six mandatory rules (totalSupply, balanceOf, transfer, transferFrom, approve, allowance) for the tokens [14].

We are using the term 'coin' to describe the native currency of a blockchain; litecoin (LTC) is the coin of Litecoin blockchain. We are using the term 'token' to describe an asset that is constructed by the methods of smart contracts; EOS (EOS) is one of the many ERC-20 tokens of Ethereum blockchain and CryptoKitties is a smart contract with non-fungible tokens following the ERC-721 standard.

Previous studies suggest that prices of some stocks are correlated [1], as are prices of cryptocurrencies [12]. Construction and analysis of networks based on correlations, or causal relationships between the characteristics of the financial instruments may be useful for such kind of applications as portfolio selection. Although there were studies on analysis of cryptocurrency cross-correlations, these studies concentrated on overall cryptocurrency market, and have not dealt with relations between Ethereum tokens. In order to fill this gap, in this paper we construct and study the network between the tokens built on the Ethereum platform.

1.2 Literature review

The econophysics book by Richmond et al. [10] introduces statistical physics, probability theory, and correlation functions. It looks at the behaviour and evolution of financial systems from the perspective of physics - or econophysics. Yet another introduction to econophysics is the book by Mantegna and Stanley [5].

The graph theory book by Bollobás [2] gives an introduction to modern graph theory.

There are lots of methods to analyze financial time series. For example, Podobnik et al. [8] use several methods to analyze the properties of volume changes $|\tilde{R}|$, and their relationship to price changes $|R|$. They analyze 14,981 daily recordings of S&P 500 Index over the period of 1950–2009, and find power-law cross-correlations between R and $|\tilde{R}|$ by using detrended cross-correlation analysis (DCCA) method [9]. This method is suitable for investigating power-law cross correlations between two simultaneously recorded nonstationary time series.

Stosic et al. [12] analyze cross correlations between price changes from data of 119 different cryptocurrencies and 200 simultaneous days in the time period from August 26, 2016 to January 18, 2018. They use methods of random matrix theory and minimum spanning trees. They find that the cross correlation matrix shows non-trivial hierarchical structures and groupings of coin/token pairs. However, they do not find such hierarchy in the partial cross correlations. They discover that most of the eigenvalues in the spectrum of the cross correlation matrix do not agree with the predictions of random matrix theory. The minimum spanning tree of cross correlations reveals distinct community structures that are quite stable. They find that the minimum spanning tree of coins and tokens consists of five communities. The conclusion is that the results represent genuine information about the cryptocurrency market, because similar communities are found for different random measurements or time periods and choices of coins and tokens or set N. It is also indicated that the communities have very different properties than the average properties of the minimum spanning tree. An application could be a lower risk cryptocurrency portfolio where cryptocurrencies are selected from distinct communities.

Boginski et al. [1] study a network representation, the market graph, of the stock market. They conduct the market graph statistical analysis and find out that it follows the power-law model. They detect cliques and independent sets in the market graph.

Plerou et al. [7] use random matrix theory methods to analyze the cross-correlation matrix C of stock price changes of the largest 1000 US companies for the period from 1994 to 1995. Their finding is that the statistics of most of the eigenvalues in the spectrum of C agree with the predictions of random matrix theory. They also find some deviations for the largest eigenvalues.

Plerou et al. [6] analyze cross correlations between price fluctuations of different stocks using methods of random matrix theory (RMT). They use two large databases for calculating cross-correlation matrices C of returns constructed from three different US stock periods. They test the statistics of the eigenvalues λ_i of C against a null hypothesis, which is a random correlation matrix constructed from mutually uncorrelated time series. Their finding is that a majority of the eigenvalues of C fall within the RMT bounds $[\lambda_-, \lambda_+]$ for the eigenvalues of random correlation matrices. They test the eigenvalues of C within the RMT bound for universal properties of random matrices. The result implies a large degree of randomness in the measured cross-correlation coefficients.

Soloviev and Belinskiy [11] construct indicators of critical and crash phenomena for cryptocurrencies. They combine the empirical cross-correlation matrix with the random matrix theory to examine the statistical properties of cross-correlation coefficients, the evolution of the distribution of eigenvalues and corresponding eigenvectors of the global cryptocurrency market. The data is the daily returns of 24 cryptocurrencies price time series from 2013 to 2018. A collective effect of the whole market is reflected by the largest eigenvalue. The proposed economic mass and the largest eigenvalue of the matrix of correlations can act like quantum indicator-predictors of falls in the cryptocurrency market.

Liang et al. [4] do a comparative analysis of cryptocurrency, foreign exchange, and stock. They took the daily close prices for about four years and construct the correlation matrices and asset trees of the markets. They conduct comparisons on volatility, centrality, clustering structure, robustness, and risk. They find that the cryptocurrency market is more fragile than the others based on the robustness and the clustering structure. For example, the clusters in the cryptocurrency market have no evident rules and they change more rapidly. For comparison, the clusters in stock market correspond to geographical regions or business sector, and the clusters in foreign exchange market match nicely with the geographical regions.

Conlon et al. [3] explore the dynamics of the equal-time cross-correlation matrix of multivariate financial time series. They examine the eigenvalue spectrum over sliding time windows and find that the dynamics of the small eigenvalues oppose those of the largest eigenvalues.

It is not known why most of the eigenvalues [12] in the spectrum of the cross correlation matrix in cryptocurrency market do not agree with the universal predictions of random matrix theory. This is in sharp contrast to the predictions for other financial markets. We investigate Ethereum's ERC-20 tokens and their network graphs to learn if similar results hold for such a subset of all the cryptocurrencies. Our research question is thus: What kind of hierarchical structures and groupings do the network graphs show for ERC-20 tokens?

2 Methods

2.1 Returns and cross correlations

To calculate the price change (or return) of a token over a time scale Δt, let us define $Y_i(t)$ as the price of a collection of tokens $i = 1, \ldots, N$ at time t. We analyze returns, defined as

$$R_i(t) \equiv \frac{Y_i(t + \Delta t) - Y_i(t)}{Y_i(t)} = \frac{Z_i(t)}{Y_i(t)}. \tag{1}$$

The problem with equation (1) is that it is sensitive to scale changes when using long time horizons [5].

The equal-time cross correlation matrix is

$$C_{ij} \equiv \langle R_i(t) R_j(t) \rangle. \tag{2}$$

$C_{ij} = 1$ is a perfect positive correlation, $C_{ij} = -1$ is a perfect negative correlation, and $C_{ij} = 0$ means no correlation [12].

2.2 Basic concepts from graph theory

Let us define a graph $G = (V, E)$ with a set of n nodes $V = \{1, ..., n\}$ and a set of m edges $E \subset V \times V$, $|V| = n$ and $|E| = m$. Each edge $e \in E$ of the graph G

has a weight $W(e) \in \mathcal{R}$. Nodes of the graph are formed by tokens for particular calendar year, weight of the edge (i, j) is equal to correlation of returns for tokens i and j. If $(i, j) \in E$, then nodes i, and j are called adjacent. If every two nodes of the graph are adjacent, the graph is called complete. Neighborhood $\mathcal{N}(v)$ of a node v is a set of all nodes v' adjacent to v, i.e. $v' \in \mathcal{N}(v)$ for all $(v, v') \in E$. Then, the degree of v, $\deg(V) = |\mathcal{N}(v)|$. For any subset of nodes $S \subseteq V$, $G[S] = (S, (S \times S) \cap E)$ denotes the *subgraph* induced by S on G. A node that belongs to S is referred to as a group node, and nodes in $V \setminus S$ are considered to be the non-group nodes. Group $G[S]$ is called a *clique* if induced by S *subgraph* is complete.

3 Results

We have collected historical data on price changes for all Ethereum's ERC-20 tokens with market capitalization higher than 1 million US dollars (USD) listed at the website Coingecko.com. Figure 1 displays log-rank plot of its market capitalization. In total, we collected data for 541 tokens, their total market capitalization is 50.2 billion USD. Overall, there were 866 cryptocurrencies with market capitalization higher than 1 million USD. The used data set did not include ether (ETH) coin itself, but it is interesting to observe that total market capitalization of Ethereum tokens exceeds that of ether, which is about 42 billion USD at the time of collection.

In order to compute correlation networks, we took the tokens that have price data for the full calendar year. In this case, it resulted in 4 tokens in 2016, 8 tokens in 2017, 111 tokens in 2018, and 333 tokens in 2019. We have computed the Pearson correlation coefficient between returns of these tokens; distributions of the resulting correlations for the two calendar years are shown in Figures 2 and 3. We created a "sliced" network by keeping only the edges formed by correlations with a value higher than the 95th percentile. As a result, we obtained three networks as described in Table 1.

year	#nodes	#edges	#components	giant component size	density	diameter
2017	8	2	6	3	0.66	2
2018	111	306	56	55	0.2	4
2019	333	2781	143	185	0.16	7

Table 1. Characteristics of the networks for 3 years. We omit the years 2015, and 2016 due to insufficient amount of data. The density and diameter are reported for the giant component.

Figures 4 and 5 show degree distributions for the networks for the years 2018 and 2019. Figures 6 and 7 show the network graphs of the tokens for the years 2018 and 2019. Also, it is interesting to observe, that graph for the year 2019 has a maximum clique size of 33 (tokens OMG, SNT, GNT, AE, BLZ, POLY, MKR,

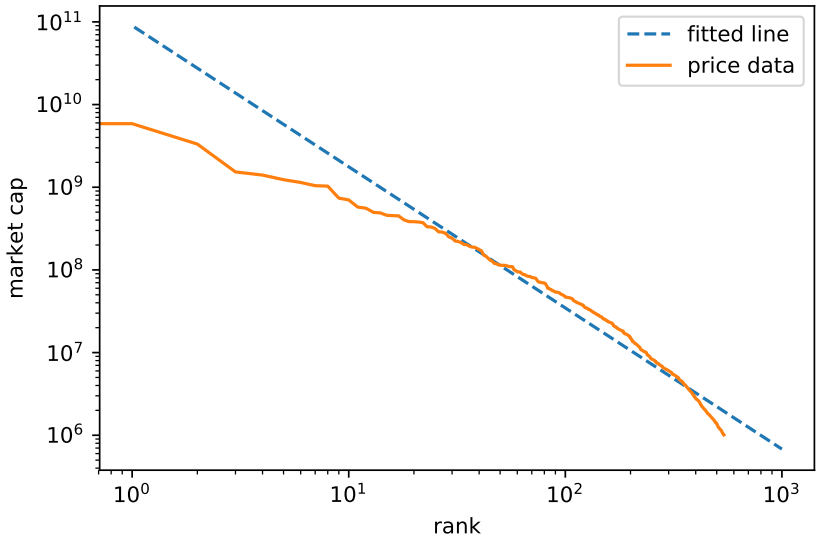


Fig. 1. Log-Rank plot of the market capitalizations of collected tokens. The plot shows the market capitalization of 541 ERC-20 tokens; from these, only 9 have market capitalization more than 1 billion USD. Dashed line shows the line fitted to the log-rank plot ($\gamma = -1.71, R^2 = 0.95$)

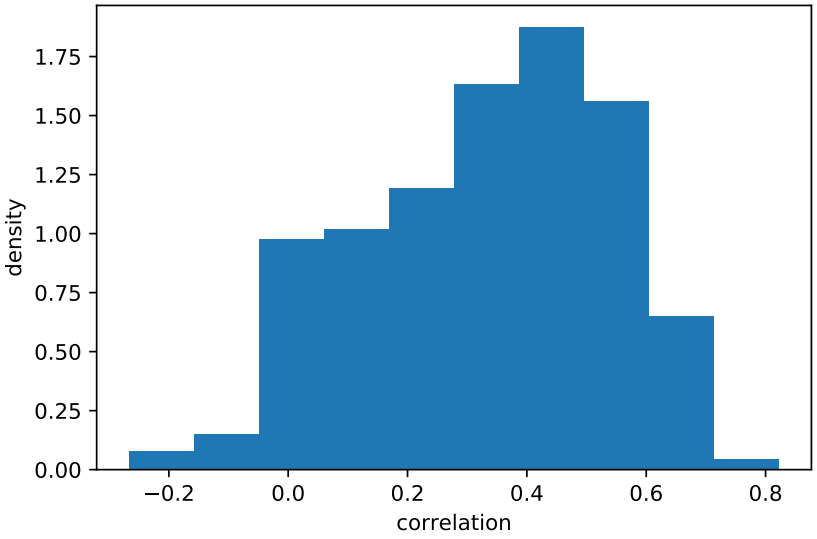


Fig. 2. The distribution of correlations for tokens of the year 2018.

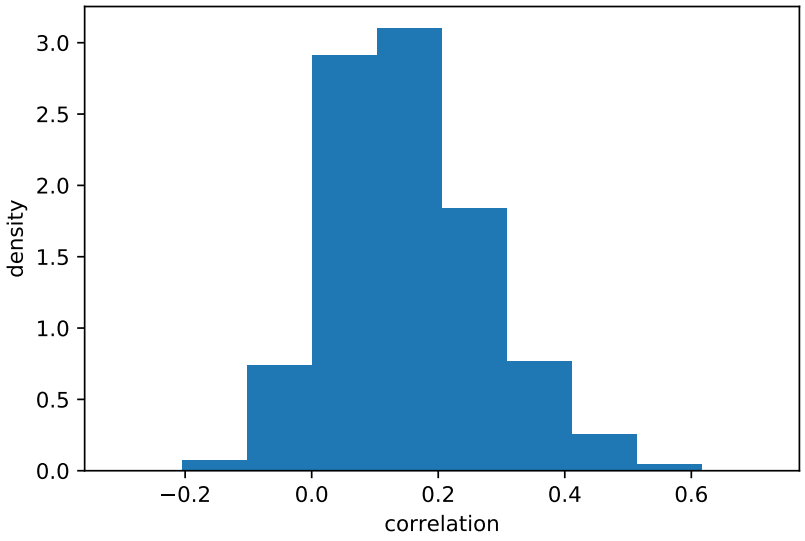


Fig. 3. The distribution of correlations for tokens of the year 2019.

ZRX, POWR, REQ, DNT, ELF, BNT, TNB, SNGLS, CND, GVT, QSP, OCN, WPR, AMB, LOOM, VIBE, MFT, STMX, QKC, VIB, GNO, BCPT, POE, WTC, YOYOW, LRC), and graph for the year 2018 has a maximum clique size of 14 (tokens BNT, CVC, POWR, OMG, LEND, STORJ, SALT, RCN, RDN, KNC, QSP, WINGS, SNM, REQ).

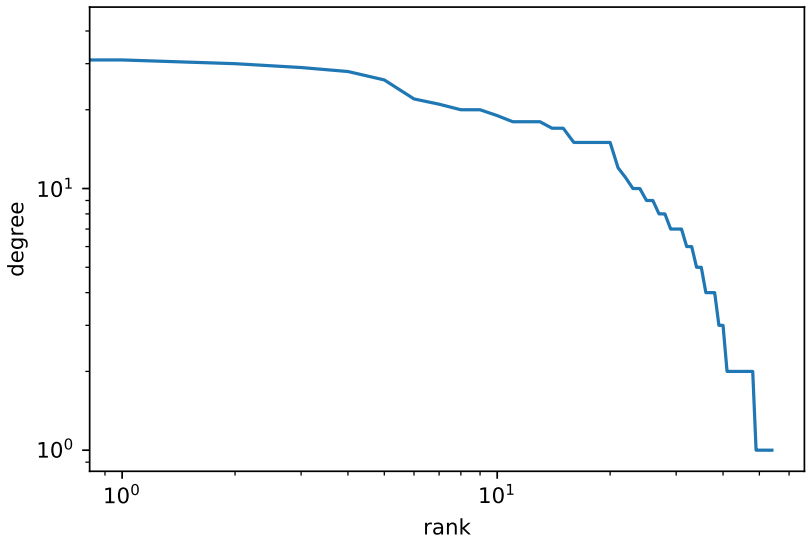


Fig. 4. The Log–Rank plot of degree distribution for the year 2018.

4 Discussion

According to Liang et al. [4] the clusters in the cryptocurrency market have no evident rules and they change more rapidly than clusters in the foreign exchange and stock markets. Do the network graphs show any hierarchical structures and groupings of ERC-20 tokens in our analysis? We can see from Figures 4 and 5 that degree distributions do not exhibit power-law behavior, that is found in many real-world graphs, including correlation networks [1]; however, there are many nodes having equally high degree. Top ten nodes with the highest degree for the years 2018 and 2019 are shown in Table 2. Total market capitalization of the ten tokens with the highest degree for the year 2018 is equal to 2.36 billion USD, and that of 2019 is equal to 2.35 billion USD, however, only two tokens are presented in both data sets: OMG and BNT.

One of the limitations of our study is the limited number of tokens; although, we have collected data on 541 tokens, our largest size graphs (for the years 2018

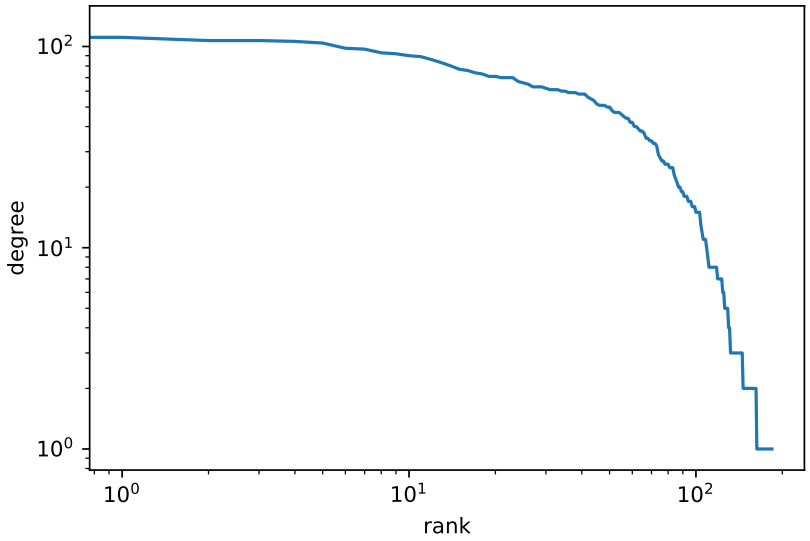


Fig. 5. The Log–Rank plot of degree distribution for the year 2019.

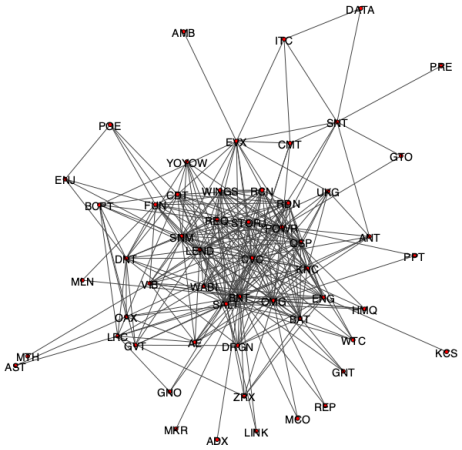


Fig. 6. The network graph of the tokens of the year 2018.

year 2018			year 2019		
name	degree	description	name	degree	description
BNT	41	Continuous liquidity and asynchronous price discovery	OMG	125	Layer-2 scaling solution for transferring value on Ethereum
CVC	31	Identity verification services	SNT	111	Status is an open source messaging platform and mobile interface to interact with DApps; the Status Network Token is a modular utility token that fuels the Status network
POWR	30	Allow access and usage of the Power Ledger Platform	GNT	107	The Golem Network Token is designed to ensure flexibility and control over the future evolution of the project; Golem is the first truly decentralized supercomputer
OMG	29	Layer-2 scaling solution for transferring value on Ethereum	MKR	107	Token for governing the Maker Protocol - the smart contracts that power Dai
LEND	28	Token for global peer-to-peer lending market	AE	106	æternity blockchain is an Erlang-based scalable smart contract platform; the Aeternity Ethereum contract expired on 2019-09-02 rendering all ERC-20 AE tokens non-transferable
SALT	26	Token for a platform for lending and borrowing	BLZ	104	An external token to represent on exchanges for customers to easily obtain to use the Bluzelle service; it is a token that bridges the Bluzelle native token (BNT) with ETH coin
SNM	22	Token on the Sonm computing power marketplace	POLY	98	Token for Polymesh, which is an enterprise-grade blockchain built for security tokens
QSP	21	Token used as the payment method for code security audits	BNT	97	Continuous liquidity and asynchronous price discovery
REQ	20	Token for participating the the Request Network, which is a decentralized network for payment requests	ELF	93	Token for a multi-chain parallel computing blockchain framework
KNC	20	Economic Facilitation, Governance, and Treasury Funds on Kyber Based Networks	ZRX	92	Token for 0x open protocol that enables the peer-to-peer exchange of assets on the Ethereum blockchain

Table 2. The top 10 nodes by degree for the years 2018 and 2019.

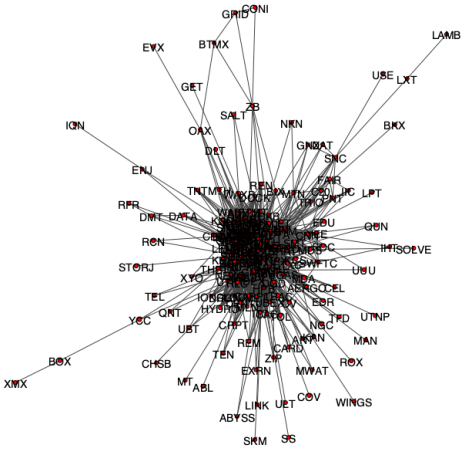


Fig. 7. The network graph of the tokens of the year 2019.

and 2019) have only 111 and 333 nodes, respectively. In future research it would be of interest to construct the networks on shorter-term price data; for example, for each 3 months, instead of one year. The equation (1) we used for calculating the returns is sensitive to scale changes for long time horizons [5].

5 Conclusions

In this paper, we made the first attempt at constructing and analyzing the network of cryptocurrencies based on their price fluctuations. Interestingly, we found that the global connectivity structure of this network does not follow a power law degree distribution that was observed for networks of stocks constructed using a similar approach [1]. Instead, the shape of our network's degree distribution resembles the one found for the Facebook social network graph [13] (although the size of the Facebook network is clearly much larger), which is an interesting observation that might be worth looking into in future work.

Furthermore, our research question was: "What kind of hierarchical structures and groupings do the network graphs show for ERC-20 tokens?" We have constructed the network from the tokens built on the Ethereum platform, but we cannot find such hierarchical structures/groupings in our analysis. Nevertheless, our preliminary results can serve as a starting point for more in-depth analysis of collective behavior of cryptocurrencies price fluctuations via network-based approaches.

References

1. Boginski, V., Butenko, S., Pardalos, P.M.: Statistical analysis of financial networks. Computational Statistics & Data Analysis **48**(2), 431 – 443

(2005). https://doi.org/https://doi.org/10.1016/j.csda.2004.02.004, http://www.sciencedirect.com/science/article/pii/S0167947304000258
2. Bollobás, B.: Modern graph theory, vol. 184. Springer Science & Business Media (2013)
3. Conlon, T., Ruskin, H., Crane, M.: Cross-correlation dynamics in financial time series. Physica A: Statistical Mechanics and its Applications **388**(5), 705 – 714 (2009). https://doi.org/https://doi.org/10.1016/j.physa.2008.10.047, http://www.sciencedirect.com/science/article/pii/S0378437108008960
4. Liang, J., Li, L., Chen, W., Zeng, D.: Towards an understanding of cryptocurrency: A comparative analysis of cryptocurrency, foreign exchange, and stock. In: 2019 IEEE International Conference on Intelligence and Security Informatics (ISI). pp. 137–139 (July 2019). https://doi.org/10.1109/ISI.2019.8823373
5. Mantegna, R.N., Stanley, H.E.: An introduction to econophysics: Correlations and complexity in finance (2000)
6. Plerou, V., Gopikrishnan, P., Rosenow, B., Amaral, L.A.N., Guhr, T., Stanley, H.E.: Random matrix approach to cross correlations in financial data. Phys. Rev. E **65**, 066126 (Jun 2002). https://doi.org/10.1103/PhysRevE.65.066126, https://link.aps.org/doi/10.1103/PhysRevE.65.066126
7. Plerou, V., Gopikrishnan, P., Rosenow, B., Nunes Amaral, L.A., Stanley, H.E.: Universal and nonuniversal properties of cross correlations in financial time series. Phys. Rev. Lett. **83**, 1471–1474 (Aug 1999). https://doi.org/10.1103/PhysRevLett.83.1471, https://link.aps.org/doi/10.1103/PhysRevLett.83.1471
8. Podobnik, B., Horvatic, D., Petersen, A.M., Stanley, H.E.: Cross-correlations between volume change and price change. Proceedings of the National Academy of Sciences **106**(52), 22079–22084 (2009). https://doi.org/10.1073/pnas.0911983106, https://www.pnas.org/content/106/52/22079
9. Podobnik, B., Stanley, H.E.: Detrended cross-correlation analysis: A new method for analyzing two nonstationary time series. Phys. Rev. Lett. **100**, 084102 (Feb 2008). https://doi.org/10.1103/PhysRevLett.100.084102, https://link.aps.org/doi/10.1103/PhysRevLett.100.084102
10. Richmond, P., Mimkes, J., Hutzler, S.: Econophysics and Physical Economics. No. 9780199674701 in OUP Catalogue, Oxford University Press (2013), https://ideas.repec.org/b/oxp/obooks/9780199674701.html
11. Soloviev, V.N., Belinskiy, A.: Complex systems theory and crashes of cryptocurrency market. In: Ermolayev, V., Suárez-Figueroa, M.C., Yakovyna, V., Mayr, H.C., Nikitchenko, M., Spivakovsky, A. (eds.) Information and Communication Technologies in Education, Research, and Industrial Applications. pp. 276–297. Springer International Publishing, Cham (2019)
12. Stosic, D., Stosic, D., Ludermir, T.B., Stosic, T.: Collective behavior of cryptocurrency price changes. Physica A: Statistical Mechanics and its Applications **507**, 499 – 509 (2018). https://doi.org/https://doi.org/10.1016/j.physa.2018.05.050, http://www.sciencedirect.com/science/article/pii/S0378437118305946
13. Ugander, J., Karrer, B., Backstrom, L., Marlow, C.: The anatomy of the facebook social graph. arXiv preprint arXiv:1111.4503 (2011)
14. Vogelsteller, F., Buterin, V.: Eip-20: Erc-20 token standard. https://web.archive.org/web/20200812054202/https://eips.ethereum.org/EIPS/eip-20, accessed: 2020-10-15

PII

ON CREATION OF A STABLECOIN BASED ON THE MORINI'S SCHEME OF INV&SAV WALLETS AND ANTIMONEY

by

Henri T. Heinonen 2021

2021 IEEE International Conference on Blockchain (Blockchain), IEEEWorkshop on Blockchain Security, Application, and Performance (BSAP-2021),

https://doi.org/10.1109/Blockchain53845.2021.00064

On Creation of a Stablecoin Based on the Morini's Scheme of Inv&Sav Wallets and Antimoney

***Abstract*—Decentralized Finance (DeFi) is a popular topic in blockchain and cryptocurrency world in the early 2020s, but cryptocurrencies have not yet become Decentralized Payment Systems (DPS), because of the high volatility of bitcoin and many of the altcoins. We investigated a proposed method to form a non-collateralized stablecoin called the Morini's Scheme of Inv&Sav wallets. We figured out two equations to do the rebasement for the Inv wallet balances and then compared the results. We found the second rebasement method to be more fair to the agents, but we found the issue of negative balances with both of the methods. We proposed novel solutions to overcome these issues. One of the proposed solutions was to freeze some of the money in Sav wallet if there is a negative balance in the Inv wallet. The another proposed solution was to introduce two-money economy of money and antimoney to i) turn the current centralized token distribution model decentralized, ii) make transactions more probable even if agents do not have enough money funds; this could be seen as a decentralized version of credit cards.**

1. Introduction

The three functions of money are medium-of-exchange, store-of-value, and unit-of-account. One of the problems with many cryptocurrencies is the high volatility which makes their exchange rates and purchasing power to change abruptly. Stablecoins (or sometimes stabletokens) are cryptocurrencies that use some mechanism to lower the volatility. Stablecoins are pegged to some asset (e.g. euros or US dollars), so they are following the value of the asset. Stablecoins are not always collateralized to the pegged asset. For example, a stablecoin can be pegged to the US dollar and be collateralized by Ether coins.

Stablecoins can be collateralized by fiat currency, commodity, cryptocurrency or none. Non-collateralized stablecoins are stabilized by the protocol layer or application layer. We are interested in non-collateralized stablecoins because they have lots of potential to become cryptocurrencies for Decentralized Payment Systems (DPSs). [1]

1.1. Literature review

K. Ito et al. [1] classifies existing stablecoins into four collateral categories (fiat, commodity, crypto and non-collateralized) and emphasizes non-collateralized stablecoins as potential DPSs because they have both the decentralization and the simplicity properties. The paper also classifies existing non-collateralized stablecoins into two intervention layer categories (protocol, application). Three concepts in economics are introduced: Quantity Theory of Money (QTM), Tobin tax, and speculative attack. A. Moin et al. [2] introduce a classification framework for stablecoin designs. H. Kołodziejczyk et al. [3] present a taxonomy of stablecoins. D. Bullmann et al. [4] classifies stablecoins on the key dimensions: (i) accountability of issuer, (ii) decentralisation of responsibilities, and (iii) what underpins the value of the asset.

F. M. Ametrano [5] introduces Hayek Money as the price stability solution, which uses dynamical rebasing to change the amount of money in wallets. The adjustment is based on a commodity price index. V. Syropyatov [6] investigates stablecoins as an implementation of Hayek money.

According to M. Morini [7] Hayek Money or Hayekcoins only stabilise unit-of-account, but not store-of-value, and Bitcoin only stabilise store-of-value, but not unit-of-account. Hayekcoins are good for denominating salaries, future financial investments, and loans, but they are unsuitable to store and save the money people receive through salaries or payments. Morini introduces two types of wallets: Investment (Inv) wallets and Savings (Sav) wallets to give users freedom to choose how much they want to be affected by the money supply changes. When money demand increases:

1) Bitcoin
   - Bitcoin wallets are stable
   - House prices (in bitcoin) decrease
   - Purchasing power of bitcoin wallets grows
2) Hayekcoin
   - Hayekcoin wallets are increased to meet demand
   - House prices (in hayekcoin) are stable
   - Purchasing power of hayekcoin wallets grows
3) Inv & Sav
   - Inv wallets are increased with leverage and Sav wallets are stable
   - House prices (in Morini's cryptocurrency) are stable

- Purchasing power of Inv wallets grows and purchasing power of Sav wallets is stable

When money demand decreases:

1) Bitcoin
   - Bitcoin wallets are stable
   - House prices (in bitcoin) increase
   - Purchasing power of bitcoin wallets shrinks
2) Hayekcoin
   - Hayekcoin wallets are shrunken to meet demand
   - House prices (in hayekcoin) are stable
   - Purchasing power of hayekcoin wallets shrinks
3) Inv & Sav
   - Inv wallets are decreased with leverage and Sav wallets are stable
   - House prices (in Morini's cryptocurrency) are stable
   - Purchasing power of Inv wallets shrinks and purchasing power of Sav wallets is stable

R. Sams [8] also notes that the coin/token price stability is not only about stabilising the unit-of-account, but also stabilising the store-of-value. The purchasing power of Hayek Money wallet is just as volatile as a Bitcoin wallet. There is also a problem with the Morini's Inv and Sav wallets: if the price development is predictable, people will either transfer all their money to either Inv wallet (if demand will go up) or Sav wallet (if demand will go down). The offered solution here are the seigniorage shares. There should be two types of coins: coins that act like money and coins that act like shares in the system's seigniorage. According to [1] the Seigniorage Share method has a problem that would probably make speculators to not buy shares nor bonds under such a tautological mechanism. The closure of Basis project in December 2018 is given as a real-world example of the problem.

M. Schmitt et al. [9] have done the first research paper that proposes the concept of antimoney. J. Stein et al. [10] further investigate the concept of antimoney. J. Stein [11] collects the research of antimoney into this PhD thesis. Beller et al. [12] also discuss the roles of money and credit in a cryptoeconomy.

H. Heinonen et al. [13] find that degree distributions of networks based on cross-correlations of ERC-20 tokens' returns do not exhibit power-law behavior.

We know from the literature that methods that work in the stockmarket and the fiat world do not necessarily work at all in the cryptocurrency world. We also know that all the existing stablecoin solutions have some issues that make them impractical as DPSs.

What we do not know yet is how to make impractical stablecoin solutions practical stablecoin solutions for DPSs. This leads to our research question.

1.1.1. Research Question. Our research question is: How to modify Morini's Scheme of Inv&Sav wallets in a way that makes it a more practical Stablecoin for Decentralized Payment Systems?

2. Methods

We came up with the research question after figuring out from the literature review that there are several non-collateralized stablecoin designs, but they are still not practical. Morini's Inv&Sav wallet design was both novel and elegant for our studies.

The data for this research are the results from the two rebasement equations we figured out from the housecoin example in Morini's article [7]. As far as we know, at the moment of writing this article, both housecoin and Hayekcoin are not actual cryptocurrencies.

We created a simple demonstration economy of only three agents and 300 housecoins for the inital timestep $t = 0$. We assumed housecoin is pegged to euro so that $1.0\,\mathrm{HC} = 1.0\,\mathrm{EUR}$. The integer timesteps

$$T_{\text{in}} =]\ldots, 0, 1, 2, 3, \ldots[\subset \mathbb{Z}$$

are the rebasement periods and $\mathbb{Z}$ is the set of integers. The non-integer timesteps

$$T_{\text{ni}} =]\ldots, 2.5, \ldots, 3.1, 3.2, \ldots[\subset \mathbb{Q} \setminus \mathbb{Z}$$

are moments when transactions are done by the agents between the rebasement periods. The set $\mathbb{Q}$ is the set of rational numbers. In the blockchain world we can assume that the set of timesteps

$$T = T_{\text{in}} \cup T_{\text{ni}}$$

can be mapped to the block height numbers.

2.1. Rebasement

Rebasement is needed to increase or decrease the money supply. For example, in Bitcoin there is only the concept of increasing the bitcoin supply with time. At the moment of writing this, there will be 6.25 new bitcoin coins about every 10 minutes. There is no concept of decreasing the bitcoin supply. This could be the reason for the high volatility of Bitcoin.

It was not entirely clear from [7] how to calculate the rebasement for Inv wallets. We figured out the following Rebasement Equations to calculate the new coins/tokens in agent i's Inv wallet at time t

$$\Delta I_i(t) = \frac{I_i(t-1)}{\sum_{j=1}^{n} I_j(t-1)} \cdot \Delta M(t) \tag{1}$$

and

$$\Delta I_i(t) = \frac{M_i(t-1)}{\sum_{j=1}^{n} M_j(t-1)} \cdot \Delta M(t) \tag{2}$$

with the following definitions

$$\Delta I_i(t), I_i(t-1), \Delta M(t), M_i(t-1) : T \longrightarrow \mathbb{R}.$$

Here $\Delta I_i(t)$ is the amount of new coins/tokens in agent i's Inv wallet at time $t \in T$, $I_i(t-1)$ is the amount of coins/tokens in agent i's Inv wallet at time $t-1$, $\sum_{j=1}^{n} I_j(t-1)$ is the total amount of coins/tokens in the whole economy's Inv wallets at time $t-1$, $n \in \mathbb{N}$ is the number of agents in the economy ($\mathbb{N}$ is the set of natural numbers), $\Delta M(t)$ is change in money supply (the amount of new coins/tokens) at time t, $M_i(t-1)$ is the amount of coins/tokens in agent i's Inv and Sav wallets at time $t-1$, and $\sum_{j=1}^{n} M_j(t-1)$ is the amount of coins/tokens in the whole economy's Inv and Sav wallets at time $t-1$, T is the set of timesteps, and $\mathbb{R}$ is the set of real numbers. It must be noted that Equation (1) is not defined when all the Inv wallets are zero.

2.2. Antimoney

Antimoney is not related to stablecoins, but it could be a useful concept when creating a stablecoin economy. Antimoney is a concept from econophysics. It got inspiration from particle physics, where a particle and an antiparticle can be created in pairs from energy. They can also be annihilated (destroyed) in pairs. It is a well-known topic from science fiction that matter and antimatter will destroy each other in a close contact. Money and antimoney do not annihilate each other, but they are created and destroyed in pairs: both money and antimoney supply are always equal. Antimoney is not simply negative money, because there is a constantly changing exchange rate between them. Money and antimoney units also cannot be simply added or subtracted, because they have different currency units like euros (EUR) and US dollars (USD) [9], [10], [11]. We propose a prefix a for the antimoney currency units. For example, the antimoney currency unit of housecoin (HC) would thus be *aHC* and the long name of the unit would be *antihousecoin*. If there ever was an antimoney version of bitcoin (BTC), it could be named *antibitcoin (aBTC)*.

What can be done with antimoney? If a buyer runs out of money, a purchase could still be done if the buyer accepts receiving some antimoney from the seller. In a way, antimoney could be seen as a decentralized version of credit cards.

According to [9] a real monetary wealth in a symmetric monetary system is given by

$$\omega = \frac{a}{p_a} - \frac{l}{p_l} \quad , \tag{3}$$

where a denotes the asset (money) holdings, l denotes the liability (antimoney) holdings, p_a is the price level for money, and p_l is the price level for antimoney. There is also a way to provide liquidity to agents by giving money and antimoney units away at the same time [9]. If both price levels in equation (3) are equal, then an agent X can transfer $\Delta a = \Delta l$ money and antimoney units to a liquidity-seeking agent Y without changing monetary wealth of either of the agents. There is also the option to set a nominal price for the liquidity.

TABLE 1. TIMESTEP $t = 0$. ONE HOUSECOIN (HC) EQUALS ONE EURO (EUR). THERE WERE 300 HOUSECOINS IN THE WHOLE ECONOMY.

agent	Inv	Sav	total
A	40.00 HC	60.00 HC	100.00 HC
B	50.00 HC	50.00 HC	100.00 HC
C	60.00 HC	40.00 HC	100.00 HC
sum	150.00 HC	150.00 HC	300.00 HC

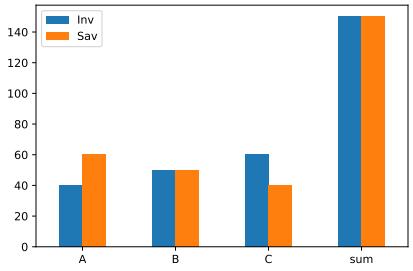


Figure 1. The demonstration economy of housecoins at the initial state $t = 0$.

The usual way to get cryptocurrency is to use fiat money to buy bitcoin or Ether coins. With Ether it is possible to buy ERC-20 tokens. The problem with this is the centralizations of the fiat world and the cryptocurrency exchanges. The second usual way to distribute cryptocurrency is to participate in the Proof-of-Work consensus method called the mining. This method is energy-intensive and bitcoin ASIC mining is famous for its heavy electricity usage [14]. The third usual way to distribute cryptocurrency is the airdrop method. With that method the creators of the cryptocurrency give away some free coins/tokens. The problem with this is that it usually only works when the cryptocurrency is new and when the monetary value of the cryptocurrency is low or zero. Our proposal of passing on money and antimoney coins/tokens at the same time is a novel method to distribute cryptocurrency.

3. Results

The results were calculated for a demonstration economy of three agents and 300 housecoins (HC) that were pegged to euros with an exchange rate of 1 HC = 1 EUR. The initial state is listed on Table 1, which can also be seen on Figure 1.

3.1. Rebasement Option I

The demand for housecoins was going up; 1.0 housecoin was worth 1.2 euros. We used the Rebasement Equation (1) for the state on Table 1 to evolve the economy from timestep $t = 0$ into timestep $t = 1$. The new state after the first rebasement is listed on Table 2.

The demand for housecoins was going down; 1.0 housecoin was worth 0.8 euros. We used the Rebasement Equation

TABLE 2. TIMESTEP $t = 1$. THE DEMAND FOR HOUSECOINS CHANGED SO THAT 1.0 HC = 1.2 EUR. THE ECONOMY OF 300.0 HC BECAME 360.0 HC, WHICH MADE THE EXCHANGE RATE BACK TO 1.0 HC = 1.0 EUR. EQUATION (1) WAS USED TO CALCULATE THE REBASEMENT.

agent	Inv	Sav	total
A	56.00 HC	60.00 HC	116.00 HC
B	70.00 HC	50.00 HC	120.00 HC
C	84.00 HC	40.00 HC	124.00 HC
sum	210.00 HC	150.00 HC	360.00 HC

TABLE 3. TIMESTEP $t = 2$. THE DEMAND FOR HOUSECOINS CHANGED SO THAT 1.0 HC = 0.8 EUR. THE ECONOMY OF 360.0 HC BECAME 288.0 HC, WHICH MADE THE EXCHANGE RATE BACK TO 1.0 HC = 1.0 EUR. EQUATION (1) WAS USED TO CALCULATE THE REBASEMENT.

agent	Inv	Sav	total
A	36.80 HC	60.00 HC	96.80 HC
B	46.00 HC	50.00 HC	96.00 HC
C	55.20 HC	40.00 HC	95.20 HC
sum	138.00 HC	150.00 HC	288.00 HC

TABLE 4. TIMESTEP $t = 2.5$. AGENTS B AND C PREDICTED THAT THE DEMAND OF HOUSECOINS WILL GO DOWN AT $t = 3$, SO THEY EMPTIED THEIR INV WALLETS AND TRANSFERRED THOSE HOUSECOINS TO SAV WALLETS. AGENT A WAS NOT AWARE OF THE SITUATION.

agent	Inv	Sav	total
A	36.80 HC	60.00 HC	96.80 HC
B	0.00 HC	96.00 HC	96.00 HC
C	0.00 HC	95.20 HC	95.20 HC
sum	36.80 HC	251.20 HC	288.00 HC

(1) for the state on Table 2 to evolve the economy from timestep $t = 1$ into timestep $t = 2$. The new state after the second rebasement is listed on Table 3.

At timestep $t = 2.5$ agents B and C predicted that the demand of housecoins will go down at $t = 3$, so they emptied their Inv wallets and transferred those housecoins to Sav wallets. Agent A was not aware of the situation. Table 4 shows the new state of the economy after agents B and C have emptied their Inv wallets.

The demand for housecoins was going down; 1.0 housecoin was worth 0.1 euros. We used the Rebasement Equation (1) for the state on Table 4 to evolve the economy from timestep $t = 2.5$ into timestep $t = 3$. The new state after the third rebasement is listed on Table 5.

3.2. Rebasement Option II

We used the Rebasement Equation (2) for the state on Table 1 to evolve the economy from timestep $t = 0$ into timestep $t = 1$. The new state after the first rebasement is listed on Table 6.

The demand for housecoins was going down; 1.0 housecoin was worth 0.8 euros. We used the Rebasement Equation (2) for the state on Table 6 to evolve the economy from

TABLE 5. TIMESTEP $t = 3$. THE DEMAND FOR HOUSECOINS CHANGED SO THAT 1.0 HC = 0.1 EUR. THE ECONOMY OF 288.00 HC BECAME 28.80 HC, WHICH MADE THE EXCHANGE RATE BACK TO 1.0 HC = 1.0 EUR. EQUATION (1) WAS USED TO CALCULATE THE REBASEMENT.

agent	Inv	Sav	total
A	−222.40 HC	60.00 HC	−162.40 HC
B	0.00 HC	96.00 HC	96.00 HC
C	0.00 HC	95.20 HC	95.20 HC
sum	−222.40 HC	251.20 HC	28.80 HC

TABLE 6. TIMESTEP $t = 1$. THE DEMAND FOR HOUSECOINS CHANGED SO THAT 1.0 HC = 1.2 EUR. THE ECONOMY OF 300.00 HC BECAME 360.00 HC, WHICH MADE THE EXCHANGE RATE BACK TO 1.0 HC = 1.0 EUR. EQUATION (2) WAS USED TO CALCULATE THE REBASEMENT.

agent	Inv	Sav	total
A	60.00 HC	60.00 HC	120.00 HC
B	70.00 HC	50.00 HC	120.00 HC
C	80.00 HC	40.00 HC	120.00 HC
sum	210.00 HC	150.00 HC	360.00 HC

timestep $t = 1$ into timestep $t = 2$. The new state after the second rebasement is listed on Table 7.

At timestep $t = 2.5$ agents B and C predicted that the demand of housecoins will go down at $t = 3$, so they emptied their Inv wallets and transferred those housecoins to Sav wallets. Agent A was not aware of the situation. Table 8 shows the new state of the economy after agents B and C have emptied their Inv wallets.

The demand for housecoins was going down; 1.0 housecoin was worth 0.1 euros. We used the Rebasement Equation (2) for the state on Table 8 to evolve the economy from timestep $t = 2.5$ into timestep $t = 3$. The new state after the third rebasement is listed on Table 9.

Tables 10, 11, and 12 show antimoney enabled transactions constructed on the case of Rebasement Option II. We omit antimoney option for Rebasement Option I, because according to Table 5 there is a negative total money balance in agent A's wallet and that could predict the agent also possibly having equal amount of *negative* antimoney, which we did not want to study in this research article. At timestep $t = 3.1$ on Table 11 agent B buys/receives liquidity (2.00 HC + 2.00 aHC) from agent C. At timestep $t = 3.2$ on Table 12 agent A receives 10.00 aHC from agent B.

4. Discussion

4.1. Third rebasement showed the difference

On Figures 2, 3, and 4 nothing seems to be very different between the two Rebasement Options (subfigures (a) and (b)); agents' Inv and Sav wallet balances seem to be almost the same for both of the Rebasement Options. The difference comes at timestep $t = 3$ (Figure 5), where one can clearly see that Equation (2) gives more fair outcomes between the

TABLE 7. TIMESTEP $t = 2$. THE DEMAND FOR HOUSECOINS CHANGED SO THAT 1.0 HC = 0.8 EUR. THE ECONOMY OF 360.00 HC BECAME 288.00 HC, WHICH MADE THE EXCHANGE RATE BACK TO 1.0 HC = 1.0 EUR. EQUATION (2) WAS USED TO CALCULATE THE REBASEMENT.

agent	Inv	Sav	total
A	36.00 HC	60.00 HC	96.00 HC
B	46.00 HC	50.00 HC	96.00 HC
C	56.00 HC	40.00 HC	96.00 HC
sum	138.00 HC	150.00 HC	288.00 HC

TABLE 8. TIMESTEP $t = 2.5$. AGENTS B AND C PREDICTED THAT THE DEMAND OF HOUSECOINS WILL GO DOWN AT $t = 3$, SO THEY EMPTIED THEIR INV WALLETS AND TRANSFERRED THOSE HOUSECOINS TO SAV WALLETS. AGENT A WAS NOT AWARE OF THE SITUATION.

agent	Inv	Sav	total
A	36.00 HC	60.00 HC	96.00 HC
B	0.00 HC	96.00 HC	96.00 HC
C	0.00 HC	96.00 HC	96.00 HC
sum	36.00 HC	252.00 HC	288.00 HC

TABLE 9. TIMESTEP $t = 3$. THE DEMAND FOR HOUSECOINS CHANGED SO THAT 1.0 HC = 0.1 EUR. THE ECONOMY OF 288.0 HC BECAME 28.80 HC, WHICH MADE THE EXCHANGE RATE BACK TO 1.0 HC = 1.0 EUR. EQUATION (2) WAS USED TO CALCULATE THE REBASEMENT.

agent	Inv	Sav	total
A	−50.40 HC	60.00 HC	9.60 HC
B	−86.40 HC	96.00 HC	9.60 HC
C	−86.40 HC	96.00 HC	9.60 HC
sum	−223.20 HC	252.00 HC	28.80 HC

TABLE 10. TIMESTEP $t = 3.0$. THIS IS EQUIVALENT TO TABLE 9, BUT WE ARE ALSO SHOWING THE ANTIMONEY BALANCES.

agent	Inv	Sav	total	Ant
A	−50.40 HC	60.00 HC	9.60 HC	9.60 aHC
B	−86.40 HC	96.00 HC	9.60 HC	9.60 aHC
C	−86.40 HC	96.00 HC	9.60 HC	9.60 aHC
sum	−223.20 HC	252.00 HC	28.80 HC	28.80 aHC

TABLE 11. TIMESTEP $t = 3.1$. AGENT B BUYS/RECEIVES LIQUIDITY (2.00 HC + 2.00 AHC) FROM AGENT C.

agent	Inv	Sav	total	Ant
A	−50.40 HC	60.00 HC	9.60 HC	9.60 aHC
B	−86.40 HC	98.00 HC	11.60 HC	11.60 aHC
C	−86.40 HC	94.00 HC	7.60 HC	7.60 aHC
sum	−223.20 HC	252.00 HC	28.80 HC	28.80 aHC

agents. According to Table 9, agents B and C both have -86.40 housecoins and agent A have -50.40 housecoins in Inv wallet. This is a strong difference to the rebasement from Equation (1), which gives agents B and C no Inv wallet decreasing at all, but agent A gets a Inv wallet balance of

TABLE 12. TIMESTEP $t = 3.2$. AGENT A RECEIVES 10.00 AHC FROM AGENT B.

agent	Inv	Sav	total	Ant
A	−50.40 HC	60.00 HC	9.60 HC	19.60 aHC
B	−86.40 HC	98.00 HC	11.60 HC	1.60 aHC
C	−86.40 HC	94.00 HC	7.60 HC	7.60 aHC
sum	−223.20 HC	252.00 HC	28.80 HC	28.80 aHC

-222.40 housecoins (Table 5)! Equation (2) is more fair because the equation takes into account the total balance of agent's Inv and Sav wallet, but Equation (1) only takes into account the Inv wallet balance of the agent. The Inv wallet balances of agents B and C are zero after the timestep $t = 2.5$.

4.2. Negative balances of Inv wallets

It is obvious from our results (both rebasement options) that Morini's Scheme of Inv&Sav wallet can eventually lead to negative Inv wallet balances. What does it mean? How can a wallet have negative money? This resembles the concept of antimoney, which can be seen as a form of negative money even though it is not exactly negative money, because money and antimoney have different currency units and a changing exchange rate between them. One solution to handle the issue of negative money in Inv wallets could be locking or freezing some of the money in Sav wallets, preventing money transfers to external wallets, until the agent will transfer positive money from Sav wallet to Inv wallet. Future rebasements might change all the balances to positive numbers again. This might not be enough for rebasements based on equation (1), because agent A does not have enough money in Sav wallet to make Inv wallet balance zero or positive at timestep $t = 3$ (Table 5). We propose that Sav wallets could act as an income generators to refund negative Inv wallets. For example, money in Sav wallets could help to fund routes on the Lightning Network or on other Layer 2 solution. Yet another proposed solution is to use money in Sav wallets to run Proof-of-Stake system; something quite similar was proposed by Morini [7]. Also, antimoney could possibly be used to do business even during when the agent's money funds are low, zero, or negative.

4.3. Antimoney

Let's assume there was antimoney already in the demonstration economy, but the antimoney balances (Ant) were just hidden from the previous steps to make things easier for the reader. On Figure 6a we are using the same wallet balances as in Figure 5b, but we are also showing the antimoney balances. According to Schmitt et al. [9] there should be equal number of antimoney and money units in the economy.

At timestep $t = 3.1$ on Figure 6b agent B buys/receives liquidity (2.00 HC + 2.00 aHC) from agent C.

At timestep $t = 3.2$ agent A wants to buy a book (money price: 9.80 HC, antimoney price: 10.00 aHC) from agent B, but agent A does not have enough money funds. Agent A's unfrozen Sav balance or total wallet balance is less than the book price: $9.60\,\mathrm{HC} < 9.80\,\mathrm{HC}$. Agent A accepts the transaction between agents A and B that sends 10.00 aHC from agent B to agent A as seen on Figure 6c. The purchase of the book was done by using antimoney instead of money. At this step agent A has more antimoney units than total money units. How to handle this to prevent any gaming of the economy? It is not clear, but, again, freezing any unfrozen money funds left on the Sav wallet could be one of the solutions.

4.4. Further research

Further research would include simulating the Inv-Sav-Ant economy for hundreds or thousands of agents and long timescales. cadCAD could be used for simulating dynamical systems like cryptocurrency economies.

Antimoney needs stricter rules than regular money, because the system will fail if people hoard antimoney, get rid off antimoney without contributing to the society, or send antimoney to agents without their permission. These rules must be established before making more complex simulations.

It would be interesting to simulate or test in a real-world setting Universal Basic Income (UBI) that consists of money and antimoney. One of the common arguments against UBI is that it could passivate citizens [15]. Antimoney could motivate UBI receivers to actually contribute to the society; antimoney UBI receivers would pass antimoney (with items or services) on to other agents of the economy which means that they are contributing to the society. Further research could compare different UBI models - some with antimoney and some without antimoney.

5. Conclusion

Our research question was: How to modify Morini's Scheme of Inv&Sav wallets in a way that makes it a more practical Stablecoin for Decentralized Payment Systems? Our answer is to design a system that can handle cases when Inv wallet balances go below zero.

We have proposed a solution that freezes some of the money in Sav wallet, if Inv wallet balance goes below zero. That should prevent the agent from gaming the system.

By introducing two-money economy of money and antimoney, agents could probably still do business even if the money funds are low, zero or even negative.

An economy of money and antimoney could also solve the distribution problem of tokens. With the current token distribution methods in order to get some ERC-20 tokens, one has to use fiat money first to buy some Ether coins and then with Ether coins one can buy ERC-20 tokens. That is a centralized procedure. With cryptocurrency system of money and antimoney, one could directly receive money and antimoney tokens to the wallet. That is a decentralized procedure.

Acknowledgments

References

[1] K. Ito, M. Mita, S. Ohsawa, and H. Tanaka, "What is stablecoin?: A survey on its mechanism and potential as decentralized payment systems," *International Journal of Service and Knowledge Management*, vol. 4, no. 2, pp. 71–86, 2020.

[2] A. Moin, K. Sekniqi, and E. G. Sirer, "Sok: A classification framework for stablecoin designs," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 174–197.

[3] H. Kołodziejczyk and K. Jarno, "Stablecoin–the stable cryptocurrency," 2020.

[4] D. Bullmann, J. Klemm, and A. Pinna, "In search for stability in crypto-assets: are stablecoins the solution?" *ECB Occasional Paper*, no. 230, 2019.

[5] F. M. Ametrano, "Hayek money: The cryptocurrency price stability solution," *Available at SSRN 2425270*, 2016.

[6] V. A. Syropyatov, "Stablecoins as an implementation of hayek's private money theory," *Economics*, vol. 15, no. 2, pp. 318–331, 2021.

[7] M. Morini, "Inv/sav wallets and the role of financial intermediaries in a digital currency," *Available at SSRN 2458890*, 2014.

[8] R. Sams, "A note on cryptocurrency stabilisation: Seigniorage shares," *Brave New Coin*, pp. 1–8, 2015.

[9] M. Schmitt, A. Schacker, and D. Braun, "Statistical mechanics of a time-homogeneous system of money and antimoney," *New Journal of Physics*, vol. 16, no. 3, p. 033024, 2014.

[10] J. A. C. Stein and D. Braun, "Stability of a time-homogeneous system of money and antimoney in an agent-based random economy," *Physica A: Statistical Mechanics and its Applications*, vol. 520, pp. 232–249, 2019.

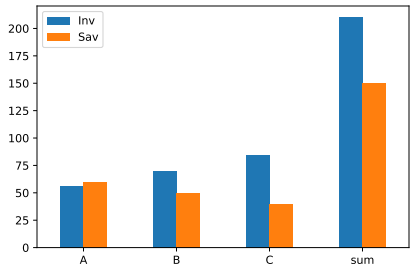
[11] J. Stein, "Stability of a time-homogeneous system of money and antimoney & kinetic microscale thermophoresis," Ph.D. dissertation, lmu, 2021.

[12] J. Beller, D. Bryan, B. Lee, J. Lopez, and A. Virtanen, "Rethinking money and credit in a cryptoeconomy: Securing liquidity without the need for central control of issuance."

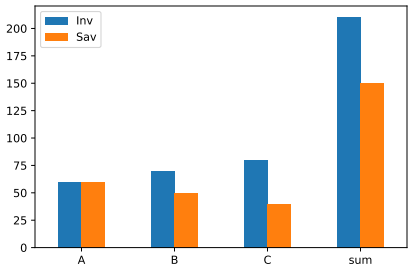
[13] H. T. Heinonen, A. Semenov, and V. Boginski, "Collective behavior of price changes of erc-20 tokens," in *International Conference on Computational Data and Social Networks*. Springer, 2020, pp. 487–498.

[14] Y.-D. Song and T. Aste, "The cost of bitcoin mining has never really increased," *Frontiers in Blockchain*, vol. 3, p. 44, 2020.

[15] U. Gentilini, M. Grosh, J. Rigolini, and R. Yemtsov, *Exploring Universal Basic Income: A Guide to Navigating Concepts, Evidence, and Practices*. World Bank Publications, 2019. [Online]. Available: https://books.google.fi/books?id=00XEDwAAQBAJ

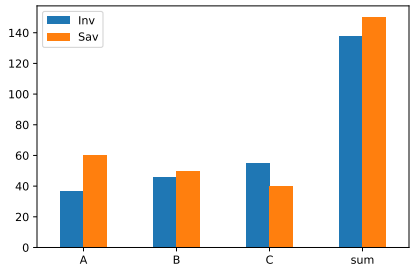


(a) Rebasement Option I

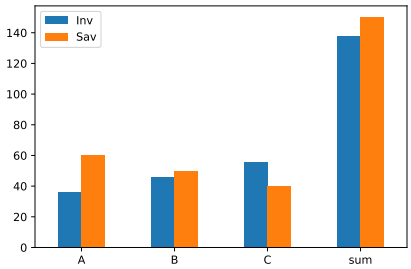


(b) Rebasement Option II

Figure 2. Wallet balances at timestep $t = 1$ after the first rebasement of Inv wallets.

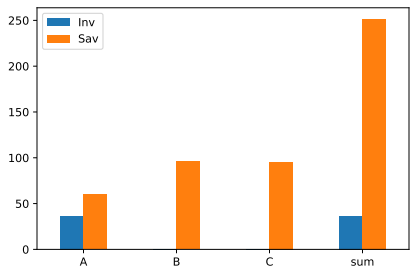


(a) Rebasement Option I

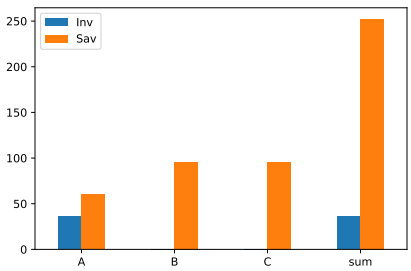


(b) Rebasement Option II

Figure 3. Wallet balances at timestep $t = 2$ after the second rebasement of Inv wallets.

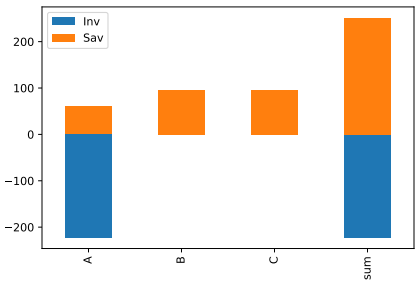


(a) Rebasement Option I

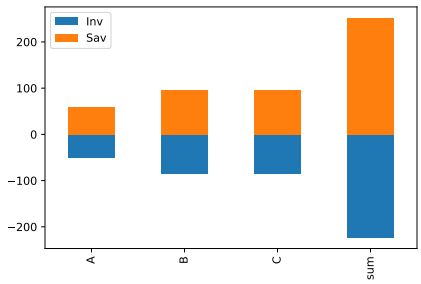


(b) Rebasement Option II

Figure 4. Wallet balances at timestep $t = 2.5$. Agents B and C have emptied their Inv wallets.

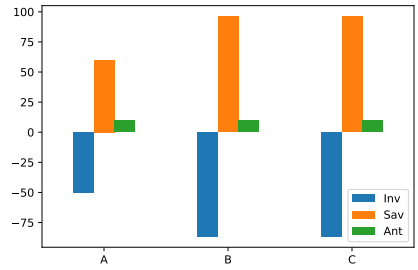


(a) Rebasement Option I

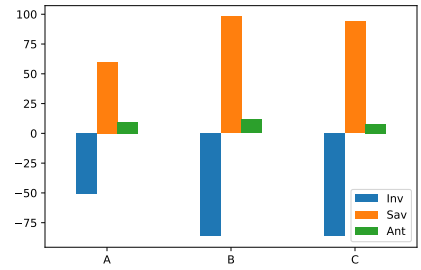


(b) Rebasement Option II

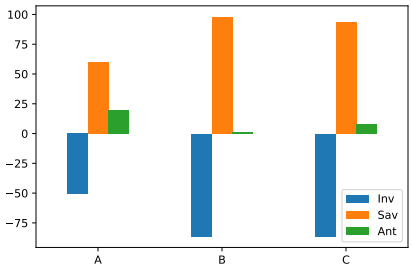
Figure 5. Wallet balances at timestep $t = 3$ after the third rebasement of Inv wallets.



(a) Rebasement Option II with Antimoney, timestep $t = 3.0$



(b) Rebasement Option II with Antimoney, timestep $t = 3.1$



(c) Rebasement Option II with Antimoney, timestep $t = 3.2$

Figure 6. Wallet balances with Antimoney after timestep $t = 3$.

PIII

RECYCLING HASHES FROM REVERSIBLE BITCOIN MINING TO SEED PSEUDORANDOM NUMBER GENERATORS

by

Henri T. Heinonen and Alexander Semenov 2021

International Conference on Blockchain (ICBC 2021)

https://doi.org/10.1007/978-3-030-96527-3_7

Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators*

Henri T. Heinonen[1][0000−0001−5961−3571] and Alexander Semenov[2][0000−0003−2691−4575]

[1] University of Jyväskylä, Jyväskylä, Finland, henri.t.heinonen@student.jyu.fi
[2] University of Florida, Gainesville, FL, USA, asemenov@ufl.edu

Abstract. We analyzed the Bitcoin difficulty data and noticed that the difficulty has been around the level of 10^{13} for three years (H2 2018 - H1 2021). Our calculation showed about 10^{28} hashes have been generated during bitcoin mining around the world for securing the addition of 703,364 blocks to the Bitcoin blockchain. We introduced a concept of Recycling Hashes in the hope to (a) jump-start bespoke silicon (customized silicon) for reversible computing, (b) open up the possibility of Bitcoin's Proof-of-Work to be less energy-consuming in the future, (c) provide scientific value or new services, in the form of entropy pool or random numbers, to Internet users while still achieving the security level of Bitcoin of today, (d) decrease the old mining hardware e-waste by using them to recycle hashes to the entropy pool, and (e) solve the problem of low mining rewards. We found that the bit rates of the current irreversible bitcoin miners are millions of times as high as the existing Internet connections, so it would be difficult to send all the hashes generated in real-time via the Internet. Even if only 0.000000355% of the hashes can be recycled, it would still mean that $355 \cdot 10^{18}$ hashes (355 EH) would have been recycled since the beginning of Bitcoin. Storing all the hashes, so far, would need storage of $2.560 \cdot 10^{30}$ bits, and it is not currently possible to keep all of them. Our simulation of 10,000 bitcoin hashes showed that the occurrences of zeros and ones in bitcoin hashes are almost 50% and 50%, so it is an encouraging finding for seeding the Pseudorandom Number Generators. We also proposed a second coin for the Bitcoin blockchain, an inflationary coin with a different currency unit (BTCi), to motivate the entropy providers to keep the old mining hardware online. The proposed second coin might keep Bitcoin's security model safe in the future when the deflationary bitcoin (BTC or BTCd) block reward is becoming too low.

Keywords: Reversible Computing · Bitcoin Mining · Random Number Generation.

* Supported by Liikesivistysrahasto.

1 Introduction

In this paper, "Bitcoin" (with uppercase B) is the Bitcoin protocol and the Bitcoin network and "bitcoin" (with lowercase b) is the bitcoin money. Bitcoin was introduced in 2008 by Satoshi Nakamoto [3] and the Bitcoin blockchain was started in 2009. Bitcoin mining has been a controversial topic since the mid-2010s. In 2009 and the early 2010s, CPUs (Central Processing Units) were used for bitcoin mining resembling grid computing projects like those utilizing the BOINC (Berkeley Open Infrastructure for Network Computing) platform. In the mid-2010s, bitcoin mining by CPUs was not profitable anymore because there was already bitcoin mining software using the computer graphics card's GPU (Graphics Processing Unit). The next stage in bitcoin mining evolution was the introduction of FPGA (Field-Programmable Gate Array) chips that were even faster at producing SHA256d (double SHA256) (SHA-2 means Secure Hash Algorithm 2) hashes than GPUs. This stage was even shorter than the GPU bitcoin mining stage because some bespoke silicon projects successfully developed and produced ASICs (Application Specific Integrated Circuits) for bitcoin mining.

SHA256d ASICs can only be used to calculate SHA256d hashes; Scrypt ASICs, used for mining litecoin (LTC), can only be used to calculate Scrypt hashes. For comparison, FPGAs can be programmed to do different calculations, and modern GPUs can also be used flexibly. ASICs are not for general computing, but they are swift. The problem with bitcoin ASIC mining is that the chips are still using lots of energy for the calculations. Another problem is that bitcoin ASIC mining devices are "getting old" very fast. It is not profitable to keep old mining hardware online because newer mining hardware will produce hashes at a faster rate and produce more bitcoin income for the hardware owner. Suppose the cost of bitcoin mining is higher than the bitcoin mining revenue. In that case, the only solution is to sell the mining hardware to someone living in an area where electricity is cheaper. Eventually, it is not profitable to use the old hardware for mining anywhere on the planet. The old mining hardware has become "e-waste".

One alternative solution is to use the old hardware to mine some altcoins with the same hash function (SHA256d) Bitcoin is using. One example is namecoin (NMC) that can be mined either alone or merge mined together with bitcoin, but mining altcoins is still not consistently profitable even in the case of merge mining. Merge mining means mining two or more similar kinds of cryptocurrencies simultaneously without sacrificing overall mining performance.

1.1 Bitcoin Mining

Bitcoin mining is a type of lottery game where one competes against other bitcoin miners. The more mining power (the higher the hash rate) one has, the better is the chance to win in this competition. The winner will get permission to add a new block with bitcoin transactions onto the Bitcoin blockchain. The winner will also get a reward that consists of a block reward of several bitcoin (BTC).

The winner will also get the transaction fees (also paid in BTC) added by the users whose transactions were included in the new block.

Difficulty is a measure of how difficult it is to find a hash below a given target. The Bitcoin network has a global block difficulty that is recalculated every 2016 blocks. Because the desired rate of Bitcoin blocks is ten minutes, it would take two weeks to mine 2016 blocks. If it takes less than two weeks for 2016 new blocks, the difficulty will go up; if it takes more than two weeks for 2016 new blocks, the difficulty will go down. [6]

Bitcoin blocks are generally around 1 megabyte in size in 2021. Blocks include transaction data and also headers that contain metadata. There are 80 bytes or 640 bits in the header of a Bitcoin block. The output of the SHA256 (and SHA256d) function is a 256-bit number. This means that the chip to calculate Bitcoin's SHA256d hash function has 640 input wires and 256 output wires.

Mining bitcoin needs lots of electricity. Stoll et al. estimate "the annual electricity consumption of Bitcoin" in November 2018 to be 45.8 TWh and the annual carbon emissions range from 22.0 to 22.9 $MtCO_2$ [36]. For comparison, the use of electricity in Finland totalled 86.1 TWh in 2019 [15], the total energy consumption in Finland in 2019 was 1362 PJ or 378 TWh [9], and the total emissions of carbon dioxide (CO2 eq.) in Finland in 2020 was 48.3 million tonnes [5]. According to the Galaxy Digital Mining report from May 2021 [12], Bitcoin consumed 113.89 TWh of electricity annually, the gold industry used about 240.61 TWh of energy annually, and the banking industry consumed 263.72 TWh of energy annually. They compare Bitcoin's electricity usage to the global annual energy supply (1,458.2 times that of the Bitcoin network), the global annual electricity generation (234.7 times that of the Bitcoin network), the amount of electricity lost in transmission and distribution each year (19.4 times that of the Bitcoin network), and the energy footprint of "always-on" devices in American households (12.1 times that of the Bitcoin network). It is also useful to compare the bitcoin mining electricity usage to the electricity and energy usages of other IT industries' activities. PC gaming used about 75 TWh of electricity in 2012 according to Mills et al. [34] Facebook's global electricity consumption was 5.14 TWh in 2019 according to Alves [8]. The energy consumption of Google (Alphabet) was 12.7 TWh in 2019, according to Jaganmohan [1]. According to Alden [4], Bitcoin's energy usage is not a problem because the mining uses less than 0.1% of global energy and because a sizable portion of the energy used for mining would be otherwise stranded and wasted.

Bitcoin mining is based on a "Proof-of-Work" (PoW) mechanism, the idea that a miner needs to spend a sufficient amount of work to receive the compensation. In Bitcoin, it is implemented based on the principle that it is easy to validate the correctness of a cryptographic SHA256d hash given the input and the resulting hash, but it is very hard (or impossible) to find the input for the hash function from the particular output. Generally, to find an input value for a hash function given its output, one should brute force possible inputs. During the bitcoin mining process, miners compete in finding the *nonce*, a value that is along with details of new transactions and a link to the previous block, a

part of the input to the SHA256d functions. The goal is to find such a nonce that the number of leading zeros in the output would be greater than a certain threshold, set by the difficulty. The more leading zeros should be at the beginning of the output, the harder it is to find a suitable *nonce* value. By finding the nonce, new transactions are added into the blockchain, and modifications of the transactions in this block would require finding another nonce in the current and potential subsequent blocks. Thus, the bitcoin mining process consists of repeated calculations of SHA256d hashes and checking if they suit the difficulty constraint.

1.2 Reversible Computing

Almost all of the computing in the world today (including bitcoin mining) is irreversible. From the chip's output, the final state $f(x)$, it is difficult or impossible to figure out the intermediate states and the initial state x. Reversible computing is a computational model where the computational process can be reversed in time, i.e., its previous states can be reconstructed from its subsequent states. For example, specific inputs of logical exclusive OR (XOR) cannot be obtained from its output, as multiple different inputs may correspond to the output; however, the input of NOT operation can be determined based on its output. According to Frank [14], reversible computing refers to computing in a way that preserves signal energies and reuses them over multiple digital operations. Reversible computing focuses on achieving far greater energy efficiency and practical performance for all digital computing, rather than quantum speedups on relatively few specialized applications.

In 1961 Rolf Landauer [31] noticed that logically irreversible gate will dissipate heat to its environment according to the equation

$$E = k_{\mathrm{B}} T \ln(2). \tag{1}$$

In Equation (1), k_{B} is the Boltzmann constant, T is the temperature of the environment in kelvins, and $\ln(2)$ is the natural logarithm of 2.

With reversible computing, it would be possible to *uncompute* the final state $f(x)$ and go back all the way to the initial state x. By not wasting any information, reversible computing could be highly energy-efficient. Making computing reversible could reduce the excess generation of waste heat. Quantum computing is closely related to reversible computing. Frank et al. [24] note that (a) Landauer's Principle sets a strict lower bound on entropy generation in traditional non-reversible architectures for deterministic computing machines; and (b) reversible computing can potentially circumvent the Landauer limit with the potential of allowing the efficiency of future digital computing to improve indefinitely.

1.3 Generating Pseudorandom Numbers

Random numbers in classical computing systems are generally pseudorandom numbers because it is impossible to get truly random numbers from computers

considered deterministic. The big difference is quantum computing that makes true random number generation possible. For example, Heinonen [25] shows a simple example of how to generate a quantum program that generates true random numbers.

Here we consider classical computing systems, so we concentrate on the PRNGs (Pseudorandom Number Generators). There are PRNGs such as Blum Blum Shub [21], Yarrow [29], and Fortuna [22]. Fortuna is a modern and cryptographically secure PRNG. It is a family of secure PRNGs, and they consist of the following parts: (a) the generator, which once seeded will produce pseudorandom data; (b) the entropy accumulator, which collects random data from various sources and reseeds the generator when possible; (c) the seed file, which stores entropy for the computer to start generating random numbers after rebooting.

1.4 Literature review

We know from Stoll et al. [36] that bitcoin mining uses lots of energy and has a considerable carbon footprint. de Vries et al. [40] found that bitcoin mining generates lots of hardware waste or *e-waste*: 30.7 metric kilotons annually as of May 2021. de Vries [39] estimated mining equipment to become obsolete in roughly 1.5 years.

It is exciting that reversible computing is not a new invention, but it is still not used as of writing this article. Bennett [19] found already in 1973 that every classical computation can be turned into reversible form. Toffoli [38] invented a universal reversible logic gate in 1980. According to Frank [23], reversible computing could be from 1000 to 100,000 as cost-effective as irreversible computing in the 2050s. The IBM Q Experience quantum computing documentation has an excellent introduction to reversible computing [7].

We also know various consensus methods that have the potential to replace the energy-consuming Proof-of-Work consensus methods. For example, Ethereum developers are trying to replace Ethereum's Proof-of-Work with Proof-of-Stake (PoS). We know projects like Gridcoin [10], and Primecoin [30] do valuable science while securing the blockchains with their consensus methods. Bizzaro et al. [20] introduce Proof-of-Evolution (PoE) that keeps the security features of Proof-of-Work, and uses part of the mining computations for the execution of genetic algorithms (GAs). Miller et al. [33] try to repurpose Bitcoin work for data preservation. Manthey et al. [32] try to replace brute force mining algorithm with solving Boolean satisfiability problem (SAT).

Bitcoin's transaction fees are too low to motivate bitcoin miners, according to Kaşkaloğlu [28] and Cussen [17]. According to Alden [4], the Bitcoin network continues to be more energy-efficient each year due to the declining block rewards.

According to Taylor [37], bitcoin ASIC mining is proof that bespoke silicon (customized silicon) can be developed in small volumes. These devices outperform general-purpose SoCs developed by major multi-billion dollar companies.

Ferguson et al. [22] note that backups and virtual machines cause problems when reseeding PRNGs. The problem is that PRNG that loads the seed file from backups will be reseeded from the very same seed file. Until the accumulator has collected enough entropy, the PRNG will produce the same output after two reboots. They claim that there is no direct defense against this kind of attack.

Wang et al. [41] present RandChain, a decentralized random beacon protocol designed to provide continuous randomness at regular intervals.

According to the literature research, we do not have solid answers to the following questions.

1. How to secure the Bitcoin blockchain without a huge carbon footprint and lots of mining hardware e-waste? There are consensus methods like Proof-of-Stake, but they are not ready to replace Proof-of-Work yet.
2. The information in reversible computing needs to be stored somewhere. Where and how will it be stored? Will it be stored locally or globally?
3. There seems to be not enough incentive to build reversible computers. How to stimulate the development of reversible computing hardware and software?
4. When there is not enough entropy available, how to seed PRNGs without using the same seed file during the computer startup process?
5. People who do not use bitcoin tend to state that bitcoin is not valuable. How to make Bitcoin more valuable and justified even for those who do not want to use the bitcoin cryptocurrency itself? One method to provide new value to the system is to solve science problems while securing the blockchain. There are inventions like Proof-of-Evolution, Primecoin, and Permacoin, but Bitcoin is not using their methods.

Research Question Our research question is: How to change bitcoin mining to use potentially less energy and do something valuable besides securing the Bitcoin blockchain?

1.5 Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators

We try to answer our Research Question by introducing Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators. Using reversible computing for bitcoin mining has been discussed on the Bitcoin Forum [13]. Seeding PRNGs with random data is a familiar concept, and methods like LavaRand use digitalized fresh images of lava lamps to seed PRNGs.

What kind of a chip would mine bitcoin using reversible computing? The exact number of input and output wires for the R-SHA256d chip is unknown because reversible computing architectures are still in the early stages. There will probably be more input and, especially, output wires for the reversible SHA256d chip than for the irreversible SHA256d chip.

Is not it impossible to reverse a secure hash function? Reversible computing is not breaking the secure hash functions (including SHA256). It will only echo the input wires x to output wires x, calculate the final state $f(x)$ and generate

some garbage data, intermediate states $g(x)$, from clean scratch memory $000\ldots$ (L zeros). All it does is mapping x, 0^L to x, $g(x)$, and $f(x)$. It is impossible to use the output from SHA256 (or SHA256d) in R-SHA256 (or R-SHA256d) to figure out the input. The output of SHA256 (and SHA256d) is missing the x and $g(x)$ information that would be needed for going back to the initial state x.

The idea of using reversible bitcoin mining to generate random numbers did not come from reversible computing but from the need to find some usage of the billions of hashes generated during the mining process. There is the famous LavaRand method [35] to generate random numbers by taking digital pictures of lava lamps, converting the information to binary numbers, applying a cryptographic hash function, obtaining seed from the hash function, and feeding that seed to the PRNG. Our idea was to take the otherwise wasted hashes of bitcoin mining and feed them to the Bitcoin network users to seed their PRNGs. This idea was getting more justified in reversible computing. Erasing information means generating waste heat. The erasing of information can be avoided if the information is copied to *a clean auxiliary register* before uncomputing the solution $f(x)$ [7].

What if most or at least some of the otherwise wasted hashes of mining could be recycled somehow? Could they be stored onto the blockchain or sent securely to the Bitcoin network users so they can seed their PRNGs? The peer-to-peer network of Bitcoin (or the blockchain itself) could act as the auxiliary register to record the information before it gets uncomputed (and erased). The Fortuna PRNG has a problem with the seed files when using virtual machines or backups because the same seed file will be used. Our solution of using fresh seeds from the blockchain network's entropy pool could solve this problem. It will need an Internet connection to get fresh seeds from the blockchain network.

2 Methods

Bitcoin difficulty is a measure of the mining power available securing the Bitcoin blockchain. The Bitcoin difficulty changes every 2016 blocks (two weeks if there are 10 minutes between each block) to correspond to the changes in total hash rate. We got the Bitcoin difficulty data from Blockchain.com website [11] and a bitcoin miner's technical specs from the producer's website [2].

The Bitcoin network's total hash rate measures the number of hashes the miners worldwide are generating when mining bitcoin in one second. We got the Bitcoin network's total hash rate data from the Blockchain.com website [16].

We simulated mining Bitcoin's Genesis block with Python code to generate 10,000 hashes until the mining ended with finding the correct hash. We stored the hashes as binary numbers into a file sample.bin. The file contained 2,560,000 binary numbers (zeros and ones). We run the Fourmilab's Pseudorandom Number Sequence Test Program, ent, with the following command:

```
ent -c sample.bin > sample.bak
```

Table 1. Table showing the bit rate of the miner divided by the upload speed of the Internet connection. The slower speeds (Gbit/s) are the Internet upload speeds and the faster speeds (Pbit/s) are the bit rates of the miners.

	2.816 Pbit/s	28.160 Pbit/s	281.600 Pbit/s
0.1 Gbit/s	281,600,000	2,816,000,000	28,160,000,000
1.0 Gbit/s	28,160,000	*281,600,000*	2,816,000,000
10 Gbit/s	2,816,000	28,160,000	281,600,000

3 Results

In this section we introduce the results: difficulty and hash rate of Bitcoin over time, the total number of hashes generated in bitcoin mining, and our small pseudorandom number sequence test to check the occurrences of ones and zeros in the set of 10,000 hashes, the entropy of the data set and some other statistics generated by the ent program.

3.1 Difficulty, hash rate, and total number of hashes

We plotted the Bitcoin difficulty in function of time in Figure 1 and the Bitcoin network's total hash rate in function of time in Figure 2. We calculated the integral of the Bitcoin network's total hash rate (hashes per second) data, $H(t)$, over the time period of early 2009 to this date by using Python SciPy's trapezoid function and got the result of

$$\int_{t=T(\text{2009-01-02 23:00:00})}^{T(\text{2021-09-30 00:00:00})} H(t)\,\mathrm{d}t = 1.059466790224828 \cdot 10^{28}\,\text{hashes} \approx 10^{28}\,\text{hashes}. \tag{2}$$

The number of hashes in Equation (2) means that storing all of them would need storage of $2.560 \cdot 10^{30}$ bits.

According to [2] Antminer S19 Pro has a hash rate of 110 TH/s, so it can generate $110 \cdot 10^{12}$ SHA256d hashes per second. One SHA256d hash has 256 bits, so the bit rate of the miner is $28.16 \cdot 10^{15}$ bit/s or 28.160 Pbit/s. We calculated various different upload speeds and bitcoin miner's bit rates in Table 1.

3.2 Pseudorandom number sequence test

We used the program called *ent* to test our sequence of 10,000 hashes stored in a file that contained 2,560,000 zeros and ones. Table 2 shows the fractions of ones and zeros in our file with 10,000 simulated bitcoin hashes. The test results from the ent program were stored in a file sample.bak.

The entropy of the data set was 1.000000 bits per byte according to the ent program. Optimum compression would reduce the size of the 2560000-byte file by 87 percent. Chi-square distribution for 2560000 samples was 325120003.70 and

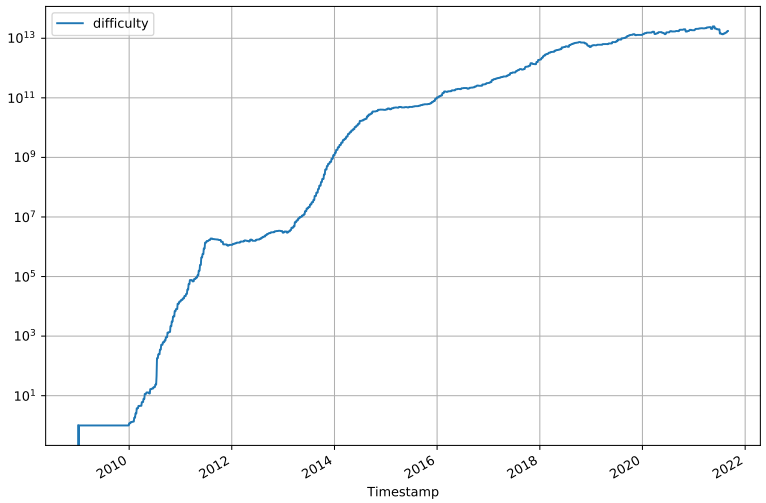


Fig. 1. The difficulty of Bitcoin during the years.

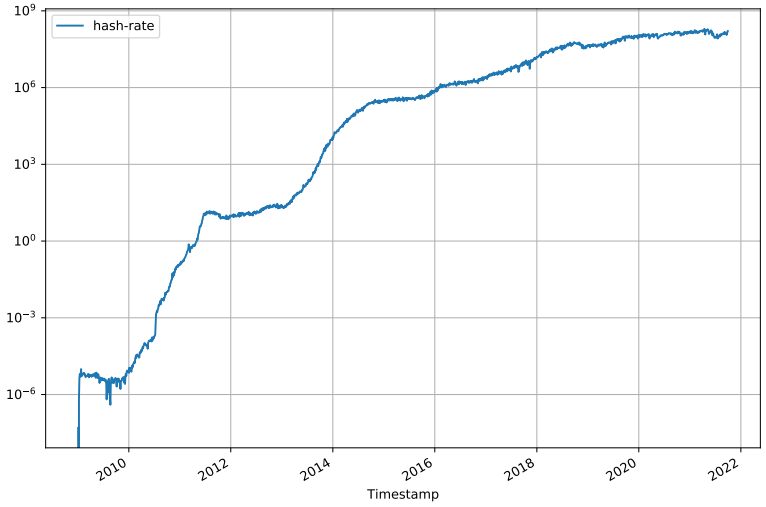


Fig. 2. The total hash rate (H/s) of Bitcoin network during the years.

Table 2. Table showing the ASCII values of the characters, their occurrences and fractions of the whole data set.

ASCII value	Character	Occurrences	Fraction
48	0	1280136	0.500053
49	1	1279864	0.499947
Total		2560000	1.000000

randomly would exceed this value less than 0.01 percent of the time. The arithmetic mean value of the data bytes was 48.4999 (127.5 = random). Monte Carlo value for Pi was 4.000000000 (error 27.32 percent). Serial correlation coefficient was 0.000944 (totally uncorrelated = 0.0).

4 Discussion

In this section, we discuss the huge number of hashes generated by bitcoin mining, the speed of Internet connections, our proposal of a two-coin model to incentivize the usage of bitcoin miners that would not be profitable with the current one-coin model of deflationary bitcoin (BTCd). We also discuss further research.

4.1 The number of hashes and the speed of Internet connections

According to our calculation in Equation (2), the total number of hashes generated by bitcoin mining since the beginning of Bitcoin is 10^{28} hashes. When writing this article, only 703,364 of those hashes have been used to add a new block onto the Bitcoin blockchain.

The Antminer S19 Pro miner will generate $281.6 \cdot 10^6$ as many hashes as it is possible to transfer through the Internet connection as seen in the middle of Table 1. Most of these hashes will probably be erased, so they will contribute to heat generation. What will be the bit rate of a realistic reversible bitcoin miner? We cannot be sure because our understanding of reversible computing principles is minimal.

It was stated in IBM's documentation [7] that one would never use the method described in the documentation for reversible computations since it requires too large a scratch memory. According to the documentation, some proposed optimization methods exist to uncompute partial results and reuse scratch memory bits.

A realistic Internet connection in the consumer market is 100 Mbit/s and small data centers could have a connection of 1 Gbit/s. If a bitcoin mining data center has ten Antminer S19 Pro miners and a 1 Gbit/s Internet connection, then the bit rate of the miners is 2,816,000,000 times the speed of the Internet connection. This would mean that

$$\frac{281,600,000\,\text{Gbit/s} - 1\,\text{Gbit/s}}{281,600,000\,\text{Gbit/s}} \cdot 100\% = 99.9999996448863636\ldots\%$$

of the generated hashes will be destroyed and only $0.0000003551136\ldots\%$ of the generated hashes will be recycled. Even if only 0.000000355% of the hashes can be recycled, it would still mean that $0.0000000355 \cdot 10^{28} = 355 \cdot 10^{18}$ hashes (355 EH) would have been recycled since the beginning of Bitcoin!

Storing all the hashes would mean storing $2.560 \cdot 10^{30}$ bits, but it is not feasible at the moment. According to Barnett [18], in 2016, the whole Internet traffic generated one zettabyte or about $8 \cdot 10^{21}$ bits of information.

Our simulation of 10,000 hashes showed, in Table 2, that the occurrences of zeros and ones in bitcoin hashes are almost 50% and 50%, so it is probably an encouraging finding for seeding the PRNGs.

4.2 Two-coin model

In this work, we proposed a second coin for the Bitcoin blockchain, an inflationary coin with a different currency unit (BTCi), to motivate the entropy providers to keep the old mining hardware online. The second coin might keep Bitcoin's security model safe in the future when the deflationary bitcoin (BTC or XBT or BTCd) block reward is becoming too low. The deflationary bitcoin coin (BTCd) comes with the famous cap of 21 million coins in total, but the inflationary bitcoin coin (BTCi) does not necessarily have any cap at all.

Having inflationary coins in the same blockchain ecosystem could also provide a solution to the problem of coin hoarding, holding, or "hodling". Inflationary coins would motivate (inflationary) bitcoin users to spend their money because inflation would eventually decrease the second coin's monetary value.

There are at least two different reasons why inflationary coin would solve the problem of "low mining rewards": (a) The inflationary bitcoin coin, which is given as a reward to the entropy providers (especially to the old mining hardware users), would probably motivate to keep on mining because the BTCi coin would have a monetary value even if it was not as expensive as the BTCd coin; and (b) the inflationary coin would probably raise the number of transactions in a block because the inflationary nature of BTCi coin would make people to use it more frequently than they use the deflationary BTCd coin. The more transactions are included in a block, the higher are the total transaction fees per block.

4.3 Further research

Further research would include using real bitcoin miners to generate seeds for PRNGs. It would be interesting to know if this could become a practical way to generate good quality random numbers in the future.

There needs to be more research on reversible computing principles. It would be interesting to know if quantum computing groups could also do more research on reversible (classical) computing because reversible computing and quantum computing are closely related.

There must also be more research on many-coin cryptoeconomies. How would the bitcoin economy change if a hard fork introduces a second coin into the

blockchain, for example, the inflationary BTCi coin? In the Ethereum ecosystem, the ether coin (ETH) and thousands of smart contract tokens are mainly running without any significant issues. Heinonen et al. [27] found some differences in behaviour between the ERC-20 (ERC means Ethereum Request for Comments) tokens and stockmarket. Heinonen [26] introduced the two-money cryptoeconomy of money and antimoney.

5 Conclusion

Our research question was: How to change bitcoin mining to use potentially less energy and do something valuable besides securing the Bitcoin blockchain?

Assuming the difficulty of Bitcoin will stay around 10^{13}, we found out that even with a reversible bitcoin miner, lots of heat will probably be generated because most of the generated hashes (information) will be erased in a way or another. The good side is that recycling hashes from bitcoin mining to PRNGs provides new value to the Bitcoin network. This entropy pool service could be available even for those who do not do bitcoin mining nor use bitcoin cryptocurrency nor the Bitcoin blockchain at all.

There may be breakthroughs in Internet connection speeds, mass storage, and reversible computing principles to overcome these issues. Still, it is challenging not to waste any energy during blockchain operations. Even if there are no breakthroughs in these technologies, our finding that

$$\begin{aligned}\text{hashes accepted (current block height)} &\lll \text{hashes potentially recycled} \\ &\ll \text{hashes generated}\end{aligned}$$

still motivates to pursue hash recycling.

Our proposal could be a solution for the problem of bitcoin mining hardware e-waste. One could use one's old (reversible/irreversible) ASIC bitcoin miner to generate hashes for the Bitcoin entropy pool even though the miner device is too old to create profitable deflationary bitcoin coins (BTCd) anymore. The incentive for mining with old hardware could come from the inflationary bitcoin coins (BTCi).

We hope that our concept of Recycling Hashes from Reversible Bitcoin Mining to Seed Pseudorandom Number Generators could:

1. Jump-start bespoke silicon for reversible computing.
2. Open up the possibility of Bitcoin's Proof-of-Work to be less energy-consuming in the future.
3. Provide scientific value or new services, in the form of entropy pool or random numbers, to Internet users while still achieving the security level of Bitcoin of today.
4. Decrease the old mining hardware e-waste by using them to recycle hashes to the entropy pool.
5. Solve the problem of low mining rewards.

Acknowledgements

We thank Professor Pekka Neittaanmäki and Professor Timo Hämäläinen for discussions and feedback. Henri thanks Liikesivistysrahasto (200092) for support.

References

1. Alphabet (google): energy consumption 2019 — statista. https://web.archive.org/web/20211029095928/https://www.statista.com/statistics/788540/energy-consumption-of-google/, accessed: 2021-11-08
2. Antminer s19 pro - the future of mining. https://web.archive.org/web/20210906102302/https://shop.bitmain.com/release/AntminerS19Pro/overview, accessed: 2021-09-06
3. Bitcoin: A peer-to-peer electronic cash system. https://web.archive.org/web/20211103223918/https://bitcoin.org/bitcoin.pdf, accessed: 2021-11-04
4. Bitcoin's energy usage isn't a problem. here's why. https://web.archive.org/web/20211103232331/https://www.lynalden.com/bitcoin-energy/, accessed: 2021-11-08
5. Carbon dioxide emissions - motiva. https://web.archive.org/web/20201030003703/https://www.motiva.fi/en/solutions/energy_use_in_finland/carbon_dioxide_emissions, accessed: 2021-10-26
6. Difficulty - bitcoin wiki. https://web.archive.org/web/20210813113701/https://en.bitcoin.it/wiki/Difficulty, accessed: 2021-09-29
7. Docs and resources - ibm quantum experience - shor's algorithm. https://web.archive.org/web/20201101072900/https://quantum-computing.ibm.com/docs/iqx/guide/shors-algorithm, accessed: 2021-09-06
8. Facebook electricity usage globally 2019 — statista. https://web.archive.org/web/20210818230043/https://www.statista.com/statistics/580087/energy-use-of-facebook/, accessed: 2021-11-08
9. Final consumption of energy - motiva. https://web.archive.org/web/20211026171442/https://www.motiva.fi/en/solutions/energy_use_in_finland/final_consumption_of_energy, accessed: 2021-10-26
10. Gridcoin white paper - the computation power of a blockchain driving science and data analysis. https://web.archive.org/web/20210815003224/https://gridcoin.us/assets/docs/whitepaper.pdf, accessed: 2021-11-04
11. Network difficulty - a relative measure of how difficult it is to mine a new block for the blockchain. https://www.blockchain.com/charts/difficulty, accessed: 2021-09-03
12. On bitcoin's energy consumption: A quantitative approach to a subjective question. https://web.archive.org/web/20211108150128/https://docsend.com/view/adwmdeeyfvqwecj2, accessed: 2021-11-08
13. Re: Theoretical minimum of logic operations to perform double iterated sha256? https://web.archive.org/web/20210906102310/https://bitcointalk.org/index.php?topic=1029536.msg11145144, accessed: 2021-09-06
14. Reversible computing: The only future for general digital computing. https://web.archive.org/web/20210401031527/https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/LPS21-talk-v5.pdf, accessed: 2021-10-01

15. Statistics finland - energy supply and consumption. https://web.archive.org/web/20210414035155/https://www.stat.fi/til/ehk/2019/ehk_2019_2020-12-21_tie_001_en.html, accessed: 2021-11-08
16. Total hash rate (th/s) - the estimated number of terahashes per second the bitcoin network is performing in the last 24 hours. https://www.blockchain.com/charts/hash-rate, accessed: 2021-10-03
17. Turning off bitcoin's inflation funded security model - wishful thinking? https://web.archive.org/web/20211012055718/https://www.onionfutures.com/turning-off-bitcoins-inflation, accessed: 2021-10-26
18. The zettabyte era officially begins (how much is that?). https://web.archive.org/web/20210813122554/https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that, accessed: 2021-10-04
19. Bennett, C.H.: Logical reversibility of computation. IBM Journal of Research and Development **17**(6), 525–532 (Nov 1973). https://doi.org/10.1147/rd.176.0525
20. Bizzaro, F., Conti, M., Pini, M.S.: Proof of evolution: leveraging blockchain mining for a cooperative execution of genetic algorithms. In: 2020 IEEE International Conference on Blockchain (Blockchain). pp. 450–455. IEEE (2020)
21. Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo-random number generator. SIAM Journal on computing **15**(2), 364–383 (1986)
22. Ferguson, N., Schneier, B., Kohno, T.: Cryptography engineering: design principles and practical applications. John Wiley & Sons (2011)
23. Frank, M.P.: Nanocomputer systems engineering. CRC Press (2006)
24. Frank, M.P., Shukla, K.: Quantum foundations of classical reversible computing. Entropy **23**(6), 701 (2021)
25. Heinonen, H.: Katsaus kvanttilaskentateknologiaan ja sen sovelluksiin. Informaatioteknologian tiedekunnan julkaisuja (88) (2021)
26. Heinonen, H.T.: On creation of a stablecoin based on the morini's scheme of inv&sav wallets and antimoney (2021), accepted to IEEE Workshop on Blockchain Security, Application, and Performance (BSAP-2021)
27. Heinonen, H.T., Semenov, A., Boginski, V.: Collective behavior of price changes of erc-20 tokens. In: International Conference on Computational Data and Social Networks. pp. 487–498. Springer (2020)
28. Kaskaloglu, K.: Near zero bitcoin transaction fees cannot last forever (2014)
29. Kelsey, J., Schneier, B., Ferguson, N.: Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator. In: International Workshop on Selected Areas in Cryptography. pp. 13–33. Springer (1999)
30. King, S.: Primecoin: Cryptocurrency with prime number proof-of-work. July 7th **1**(6) (2013)
31. Landauer, R.: Irreversibility and heat generation in the computing process. IBM journal of research and development **5**(3), 183–191 (1961)
32. Manthey, N., Heusser, J.: Satcoin–bitcoin mining via sat. SAT COMPETITION 2018 p. 67 (2018)
33. Miller, A., Juels, A., Shi, E., Parno, B., Katz, J.: Permacoin: Repurposing bitcoin work for data preservation. In: 2014 IEEE Symposium on Security and Privacy. pp. 475–490. IEEE (2014)
34. Mills, N., Mills, E.: Taming the energy use of gaming computers. Energy Efficiency **9**(2), 321–338 (2016)
35. Noll, L.C., Mende, R.G., Sisodiya, S.: Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system (Mar 24 1998), uS Patent 5,732,138

36. Stoll, C., Klaaßen, L., Gallersdörfer, U.: The carbon footprint of bitcoin. Joule **3**(7), 1647–1661 (2019)
37. Taylor, M.B.: Bitcoin and the age of bespoke silicon. In: 2013 international conference on compilers, architecture and synthesis for embedded systems (CASES). pp. 1–10. IEEE (2013)
38. Toffoli, T.: Reversible computing. In: International Colloquium on Automata, Languages, and Programming. pp. 632–644. Springer (1980)
39. de Vries, A.: Renewable energy will not solve bitcoin's sustainability problem. Joule **3**(4), 893–898 (2019)
40. de Vries, A., Stoll, C.: Bitcoin's growing e-waste problem. Resources, Conservation and Recycling **175**, 105901 (2021)
41. Wang, G., Nixon, M.: Randchain: Practical scalable decentralized randomness attested by blockchain. In: 2020 IEEE International Conference on Blockchain (Blockchain). pp. 442–449. IEEE (2020)

PIV

A SURVEY ON TECHNOLOGIES WHICH MAKE BITCOIN GREENER OR MORE JUSTIFIED

by

Henri T. Heinonen and Alexander Semenov and Jari Veijalainen and Timo Hämäläinen 2022

IEEE Access

https://doi.org/10.1109/ACCESS.2022.3190891

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 7 June 2022, accepted 11 July 2022, date of publication 14 July 2022, date of current version 20 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3190891

SURVEY

A Survey on Technologies Which Make Bitcoin Greener or More Justified

HENRI T. HEINONEN[1], ALEXANDER SEMENOV[2], JARI VEIJALAINEN[1], AND TIMO HÄMÄLÄINEN[1], (Senior Member, IEEE)

[1]Faculty of Information Technology, University of Jyväskylä, FI-40014 Jyväskylä, Finland
[2]Department of Industrial and Systems Engineering, Herbert Wertheim College of Engineering, University of Florida, Shalimar, FL 32579, USA

Corresponding author: Henri T. Heinonen (henri.t.heinonen@student.jyu.fi)

ABSTRACT According to recent estimates, one bitcoin transaction consumes as much energy as 1.5 million Visa transactions. Why is bitcoin using so much energy? Most of the energy is used during the bitcoin mining process, which serves at least two significant purposes: a) distributing new cryptocurrency coins to the cryptoeconomy and b) securing the Bitcoin blockchain ledger. In reality, the comparison of bitcoin transactions to Visa transactions is not that simple. The amount of transactions in the Bitcoin network is not directly connected to the amount of bitcoin mining power nor the energy consumption of those mining devices; for example, it is possible to multiply the number of bitcoin transactions per second without increasing the mining power and the energy consumption. Bitcoin is not only ''digital money for hackers''. It has very promising future potential as a global reserve currency and a method to make the World Wide Web (WWW) immune to cyberattacks such as the Distributed Denial-of-Service attacks. This survey approached cryptocurrencies' various technological and environmental issues from many different perspectives. To make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified, what technological solutions do we have? We found that cryptocurrency mining might be cleaner than is generally expected. There is also a plan to make a vast renewable energy source available by combining Ocean Thermal Energy Conversion and Bitcoin mining. There are plans to use unconventional computing methods (quantum computing, reversible computing, ternary computing, optical computing, analog computing) to solve some of the issues regarding the vast energy consumption of conventional computing (including cryptocurrency mining). We think using spare computing cycles for grid computing efforts is justified. For example, there are billions of smartphones in the world. Many smartphones are being recharged every day. If this daily recharging period of twenty to sixty minutes would be used for grid computing, for example, finding new cures to cancer, it would probably be a significant breakthrough for medical research simulations. We call on the cryptocurrency communities to research and develop grid computing and unconventional computing methods for the most significant cryptocurrencies: bitcoin (BTC) and ether (ETH).

INDEX TERMS Blockchain, DLT, cryptocurrency, bitcoin, green technology, sustainability, unconventional computing, climate change.

I. INTRODUCTION

Blockchain is a distributed database that maintains a continuously growing list of records (blocks) linked to each other. Blockchain is a special case of the more general Distributed Ledger Technology (DLT). For example, IOTA (tangle), Hedera (hashgraph), and Corda are not blockchains but distributed ledgers. A blockchain database is secure by design, and once the block is recorded there, it cannot be modified retroactively in a way that other nodes would accept

The associate editor coordinating the review of this manuscript and approving it for publication was Thanh Ngoc Dinh.

the modification. Blockchain relies on a peer-to-peer (P2P) network without any central coordinating node; each node of the network may access the entire blockchain database. Decentralization and resistance to data modification sparked much interest in blockchain technology. The most popular applications are the cryptocurrencies such as Bitcoin or Monero; there, blockchain is used for storing currency transactions. Due to the decentralization of blockchain, there is no need for the intermediaries such as banks or other currency transaction regulating bodies. Transactions propagate through the P2P network, and all the nodes participating in the network may validate them. Blockchain is also suitable for recording medical data [1] or cadastre information [2]. Senator Rand Paul has said bitcoin could become the world's reserve currency [3]. Bitcoin and other blockchain technologies could make the World Wide Web resistant to Distributed Denial-of-Service attacks [4].

In the early years, Central Processing Units (CPUs) were used to secure blockchains. The downsides of the blockchain (and other DLT) technology include a heavy electricity usage and the short lifetime of the mining devices that secure the ledgers; there are now specialized devices to mine cryptocurrencies that have a short lifetime of just about 1.5 years (in the case of Bitcoin ASIC miners). After that, the devices become e-waste with no useful purpose.

There are many efforts to stop climate change and fix the environment. For example, Doughnut Economics explores the ways to achieve thriving humanity in the 21st century [5]. Many people raise many concerns over the environmental impacts of cryptocurrencies, and our survey is one of the first to summarize many helpful technologies to make cryptocurrencies sustainable. Our survey comprehensively summarizes green and justification technologies for the blockchain space.

In this survey, we approach the issues of cryptocurrencies from many different perspectives. We will give a short introduction to why bitcoin and other cryptocurrencies are using so much energy. In later sections, we will list many exciting technologies that could help make bitcoin and other cryptocurrencies greener and more justified.

Blockchain energy consumption is a primary concern preventing its widespread application; many authors proposed to make blockchain more green, that is, by reducing its energy consumption, such as Dubrovsky *et al.* [6] presenting a prototype of Photonic Miner, which is an application of modern analog and optical computing; or alternatively, to make energy consumption to serve more practical purposes, such as training deep learning models during mining [7], or ASIC-resistant puzzles [8], useful puzzles, non-outsourceable puzzles, and Proof-of-Stake and virtual mining. Because of our expertise in volunteer computing (mostly SETI@home and BOINC), we wanted to emphasize potential grid computing methods that could revolutionize cryptocurrency mining.

Yet another motivation are the recent letters [9], [10] to the Environmental Protection Agency (EPA). The letter from Congress of the United States to the EPA [9] claimed that people living near crypto mining facilities are suffering from the air, water, and noise pollution. They refer to the research [11], [12] by de Vries *et al.* They requested the EPA to evaluate the compatibility of cryptocurrency mining facilities with the Clean Air Act and the Clean Water Act.

The EPA also got a response letter from bitcoin miners [10] with some of the misperceptions (in the letter from Congress to the EPA) debunked. For example, bitcoin miners refer to the Bitcoin Mining Council's latest Q1 survey of miners. The miners surveyed use 64.6% sustainable energy (wind, solar, hydro, or nuclear), and according to conservative estimates about the energy mix, bitcoin mining globally might be using about 58.4% sustainable energy. They compare this figure to the default US energy mix at 21% sustainable [13]. These figures mean that bitcoin mining might be cleaner than usually expected.

II. MAKING BITCOIN GREEN AND JUSTIFIED

In this section, we compare our survey to other surveys, describe the basics of Proof-of-Work mining, introduce our categories of Green and Justified technologies, and give a short introduction to Grid computing.

A. COMPARISON TO OTHER SURVEYS

Unconventional computing is often overlooked, so we wanted to emphasize optical, ternary, and reversible computing methods. We think that no other survey on green blockchain technologies at the moment is focusing on these unconventional methods. Bada *et al.* [14] mention a comprehensive list of ''Proof-of-X'' consensus methods. Their paper discusses these methods mostly from the point of view of Green technologies. Tschorsch *et al.* [15] also present a long list of ''Proof-of-X'' methods. Their paper discusses many key ideas regarding blockchain technologies.

Our survey divides technologies into two categories: those that lower the blockchain infrastructure's energy consumption and those that add blockchain infrastructure's usefulness without lowering the energy consumption per se. Our survey has a novel way of categorizing technologies. We also discuss if it is plausible or not to use the technology in question to make the biggest cryptocurrency - bitcoin (BTC) - greener or more justified.

We also like to mention the concept from futures studies called the Kardashev scale [16]. This exciting method for categorizing technological civilizations based on their ability to access power and energy will be discussed in the subsection ''Renewable and Nuclear Energy''.

This survey does not cover all possible technologies related to blockchains and DLTs. Delegated Proof-of-Stake (DPoS), Proof-of-Luck (PoL), Proof-of-Activity (PoAC), Proof-of-Capacity (PoC), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA), Delegated Byzantine Fault Tolerance (DBFT), Proof-of-Authority (PoA), Proof-of-Importance (PoI), Proof-of-Burn (PoB), Proof-of-Believability (PoBLV), Proof-of-Devotion (PoD), Proof-of-Reputation (PoR),

Proof-of-Weight (PoWe), Proof-of-Publication, Proof-of-Bandwidth, Proof-of-Download [17], Proof-of-Learning [18], Proof-of-Excellence, Proof-of-Vote [19] and possibly many other Proof-of-X schemes were left out from the current survey. Many of those listed technologies were covered by [14] and [15].

B. PROOF-OF-WORK MINING NEEDS LOTS OF ENERGY

Bitcoin was described in a white paper in 2008 [20], and the blockchain was started in early 2009. It was possible to run the whole Bitcoin infrastructure on a small set of home computers. The first block of the Bitcoin blockchain is called the Genesis Block, and it contains the following message ''The Times 03/Jan/2009 Chancellor on brink of second bailout for banks''. The message was one of the headlines from The Times magazine released on 3 Jan 2009, so the message proves that the first Bitcoin block was generated during or after 3 Jan 2009.

What are blocks? The Bitcoin blockchain's blocks have two parts:

- header with metadata including a hash pointer reference to the previous block, the Merkle tree root of transactions, and block creation time;
- list of new bitcoin transactions.

The Bitcoin blocks are like pages in a diary; the diary is blank at the beginning, and one usually appends new information to the diary, and erasing or modifying information from the diary written with a ballpoint pen is very difficult. It is also difficult or impossible to erase or modify information from the Bitcoin blockchain's blocks. Adding new information to the Bitcoin blockchain is appending new entries (blocks) to the ledger in a process called mining, which needs lots of energy.

Why is bitcoin using so much energy? Most of the energy is used during the bitcoin mining process (called the Proof-of-Work or PoW), which serves at least two different major purposes:

- it distributes new cryptocurrency coins to cryptoeconomy; and
- it secures the Bitcoin blockchain ledger.

The bitcoin PoW mining algorithm is actually very simple in pseudo-code [21], [22]:

```
nonce=MIN
while(nonce<MAX):
  if sha256(sha256(block+nonce))<target:
    return nonce
  nonce+=1
```

The problem is that `target` tends to be a small number, so the SHA256d hash of `block+nonce` also needs to be a tiny number. One needs to try a considerable number of nonces to find a hash that is small enough eventually. This process of trying very many nonces is what consumes electrical energy.

In the late 2010s, bitcoin's colossal energy consumption became a major news topic. There was even a prediction in 2017 that bitcoin would consume all of the world's energy in 2020 [23]. This prediction was nowhere near becoming a reality because of the limitations of electricity grids, strict electricity regulations, the profitability of bitcoin mining, the lack of bitcoin mining devices, and many other reasons. In 2018, Mora *et al.* [24] claimed that bitcoin emissions could push global warming above two centigrades. The analysis and results of the paper by Mora *et al.* have been debunked at least by Houy [25], Masanet *et al.* [26], and Dittmar *et al.* [27]. According to Houy, rational mining limits Bitcoin emissions, and the average of a list of 62 ASIC miners used by Mora *et al.* in their analysis is not realistic; a rational miner would have turned off 14 of those 62 miners for most of the time. Masanet *et al.* remind us that poorly constructed future IT energy usage scenarios can spread misinformation and lead to ill-informed decisions. They give the five most important issues regarding the critical flaws in the design and execution of the research by Mora *et al.* Also, Dittmar *et al.* note that the electricity demand scenarios by Mora *et al.* seem unlikely.

De Vries [28] estimated in 2018 that the Bitmain company, with a claimed market share of 70%, could produce up to 6.5 million bitcoin mining machines (Antminer S9) in 2018. The machines would have a combined electrical power need of 8.92 GW. Table 1 shows the annual electricity consumption of Bitcoin in 2018 and 2021 and the annual electricity consumption of Ethereum in 2022. In 2019, the average power need of the whole world was 18.44 TW or 0.73 on Carl Sagan's interpolated Kardashev scale [29]. Table 1 shows the annual total energy consumption of the world in 2019 and 2020. In 2020, possibly due to the lockdowns caused by COVID-19, the annual total energy consumption of the world was lower than in 2019.

Bitcoin (BTC) and ether (ETH) are the most popular cryptocurrencies in 2022. Table 1 shows bitcoin, ether, and Visa ''transaction'' energy consumptions in kilowatt-hours in April 2022. We use the quotation marks with the transaction word (''transaction'') to inform the reader of the fact that it is somewhat misleading [30] to compute the transaction energy consumptions by taking the whole network's energy consumption in a period and dividing it by the number of transactions in a said period. In reality, bitcoin and ether transactions are not directly connected to the power needs of mining machines. According to Cambridge Centre for Alternative Finance [31], adding (or removing[1]) mining devices and thus increasing (or decreasing) electricity consumption does not have an impact on the number of processed transactions (transaction throughput). They note that a single transaction can contain hidden semantics like hundreds of payments or settlements (opening and closing transactions of micropayment channels) of Layer 2 payment solutions like

[1]Note by the corresponding author of this survey.

TABLE 1. Various energy consumptions in kilowatt-hours.

ID #	Characteristic	Energy consumption in kWh	Reference(s)
0	One Visa "transaction" (around April 27, 2022)	∼0.0014863	[32], [33]
1	*One ETH "transaction" (around April 27, 2022)*	∼238.22	[33]
2	*One BTC "transaction" (around April 27, 2022)*	∼2,188.59	[32]
3	The annual total energy consumption of a Type 0 civilization	8,760,000.00	[29]
4	The annual global electricity consumption of Facebook (2019)	∼5,140,000,000.00	[34]
5	The annual electricity consumption of Google (Alphabet) (2019)	∼12,700,000,000.00	[35]
6	*The annual electricity consumption of Bitcoin (November 2018)*	∼45,800,000,000.00	[36]
7	Tsar Bomba's yield (58 Mt TNT or 242.672 PJ)	∼67,410,000,000.00	[37], [38]
8	The annual electricity consumption of PC gaming (2012)	∼75,000,000,000.00	[39]
9	The annual electricity consumption of Finland (2019)	∼86,100,000,000.00	[40]
10	*The annual electricity consumption of Ethereum (21 April 2022)*	∼105,630,000,000.00	[41]
11	*The annual electricity consumption of Bitcoin (May 2021)*	∼113,890,000,000.00	[42]
12	The annual total energy consumption of the gold industry (May 2021)	∼240,610,000,000.00	[42]
13	The annual total energy consumption of the banking industry (May 2021)	∼263,720,000,000.00	[42]
14	The annual total energy consumption of Finland (2019)	∼378,000,000,000.00	[43]
15	An unmanned probe to reach Alpha Centauri in 71 years (with deceleration at the destination)	∼2,778,000,000,000.00	[44], [45]
16	The annual total energy consumption of the world (2020)	∼154,750,000,000,000.00	[46]
17	The annual total energy consumption of the world (2019)	∼161,530,000,000,000.00	[29], [46]
18	The annual total energy consumption of a Type I civilization	87,600,000,000,000,000.00	[29]

the Lightning Network or represent timestamped data points (for example, https://opentimestamps.org/).

If we continue using the misleading metric of energy per transaction, we can see that ten ether ''transactions'' is equal to about one bitcoin ''transaction'', but still, about 160,000 Visa ''transactions'' can be done with the same energy as only one ether ''transaction''. Figure 1 shows energy consumptions of the activities listed in Table 1.

Alden [47] says that Bitcoin's energy usage is not a problem because the energy used for mining is less than 0.1% of the world's energy consumption and because a sizable portion of the energy used for mining would be otherwise stranded and wasted.

The annual electricity consumption of Bitcoin in November 2018 was 45.8 TWh and the annual carbon emissions were between 22.0 and 22.9 $MtCO_2$ [36]. For comparison, the total electricity usage in Finland was 86.1 TWh in 2019 [40], the total energy consumption in Finland was 1362 PJ or 378 TWh [43] in 2019, and the total emissions of carbon dioxide (CO2 eq.) in Finland was 48.3 million tonnes in 2020 [48].

However, another problem with Bitcoin is the low throughput of the network on Layer 1: only about seven bitcoin transactions per second were possible globally before the SegWit and the Lightning Network updates. Only about 1 megabyte of information can be recorded on a Bitcoin block, and there are only about six blocks per hour. There are Layer 1 solutions to this; one of the solutions is used in the blockchain called Bitcoin Satoshi's Vision (BSV), a hard fork of Bitcoin Cash (BCH). Bitcoin Cash is a hard fork of Bitcoin (BTC). They all have a shared history - thousands of blocks since the Bitcoin Genesis block is identical to these three blockchains! After the hard fork, the chains separated into different branches. Hard forks can happen when there is a significant change in consensus rules that are incompatible with the old clients. For example, decreasing the block size is compatible with the old clients, so it can be considered a soft fork; increasing the block size is not compatible with the old clients, so it can be considered a hard fork. Bitcoin Cash is a hard fork caused by increasing the maximum block size. Bitcoin SV is a hard fork of Bitcoin Cash caused by implementing even a bigger block cap size. Bitcoin SV is reported to have a throughput of 9,000 transactions per second [49]. The hash rate of Bitcoin SV is still considerably lower than that of Bitcoin's, which means that high throughputs and low energy consumptions are possible with Bitcoin-like technology.

There are also Layer 2 solutions to the low throughput problem of Bitcoin. The Lightning Network is a Layer 2 solution, and it will be discussed later in this survey paper.

C. TWO DIFFERENT TECHNOLOGY CATEGORIES: GREEN AND JUSTIFIED

Usually, the arguments [50] on cleaning cryptocurrencies suggest banning the bitcoin cryptocurrency, cleaning Bitcoin's energy supply, or changing Bitcoin's consensus method from Proof-of-Work (PoW) to Proof-of-Stake (PoS). One does not usually differentiate what is meant by ''banning the bitcoin''. There are several forms of banning the bitcoin, including:

- one does not allow bitcoin to be used at all in the economy, and mining is prohibited in a certain jurisdiction;
- bitcoin is allowed to be used in an economy, i.e., financial transactions are allowed, but mining is prohibited in a jurisdiction;
- bitcoin mining is allowed in the jurisdiction, but its use to convey financial transactions is prohibited.

For example, the European Securities and Markets Authority vice-chair proposed the EU ban the PoW mining, but the proposal did not go through the EU committee [51].

We think that there are two main ways to make cryptocurrencies survive in the world of climate change and green politics. The securing process of the blockchain could

1) use less energy, so the blockchain's contribution to the climate change would be reduced;

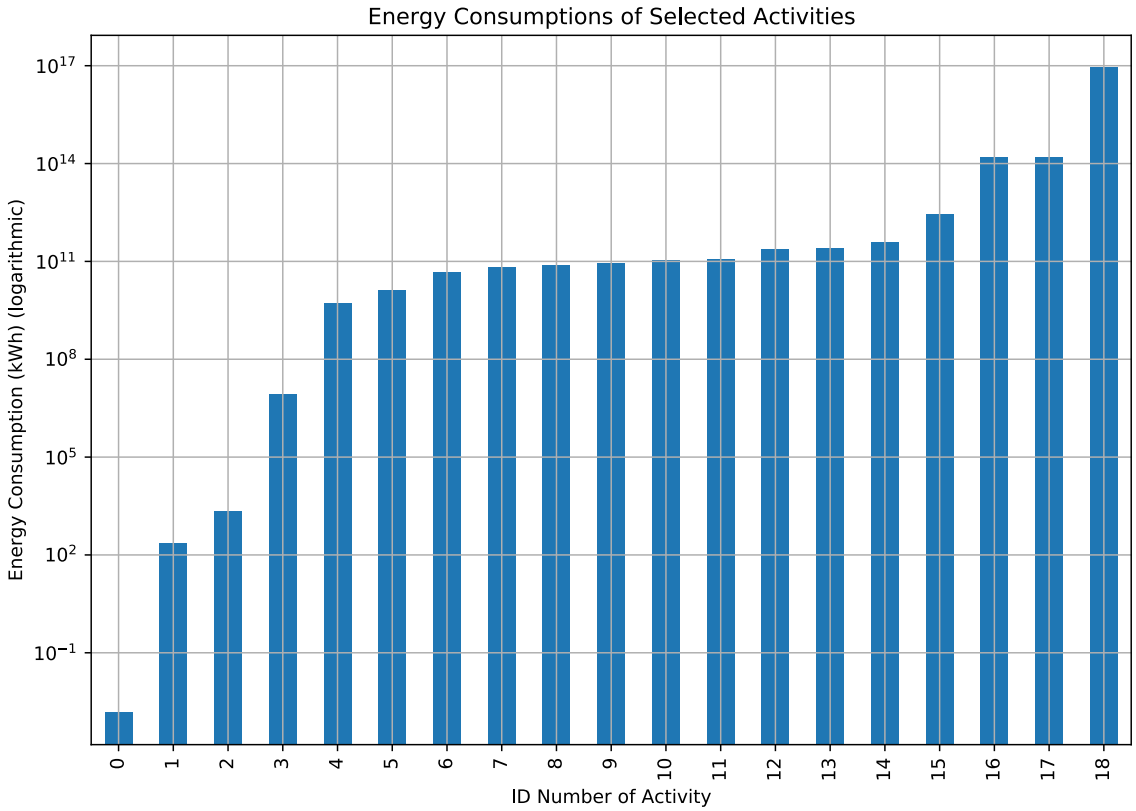


FIGURE 1. Energy consumptions of selected activities in kWh. See Table 1 for explanations to the ID numbers of selected activities.

TABLE 2. Global average virtual water content of selected products, per unit of product [52] and per gram of product.

Product	Virtual water content (litres)	Virtual water content (litres per gram)
1 tomato (70 g)	13	0.186
1 microchip (2 g)	32	16
1 slice of bread (30 g)	40	1.333
1 cotton T-shirt (250 g)	2000	8
1 hamburger (150 g)	2400	16

2) do something valuable (besides securing the blockchain) to make that process more justified.

We call the technologies fitting the description of the first list item the Green Technologies, and the technologies fitting the description of the second list item the Justification Technologies. In short, an example of a Green Technology would be a consensus process that secures the blockchain but does not use massive amounts of energy, even for a blockchain like Bitcoin. What if there is an optical computing method or a reversible computing method to calculate hashes? An example of a Justification Technology would be something that adds additional value to the consensus process without reducing energy consumption. What if the hashes generated in bitcoin mining could be recycled to seed PseudoRandom Number Generators? What if bitcoin mining could simulate new drug molecules for curing cancer?

D. GRID COMPUTING

The Justification Technology is related to volunteering computing [53] or grid computing platforms like GIMPS, distributed.net, SETI@home, Berkeley Open Infrastructure for Network Computing (BOINC), and Folding@home. In 1996, Great Internet Mersenne Prime Search (GIMPS) popularized volunteer computing, followed by distributed.net in 1997. There was a screensaver for volunteer computing called SETI@home in 1999 and the early 2000s before switching to the BOINC platform. SETI@home was invented to use the otherwise wasted spare CPU cycles of home computers when they were left idle with power on. Folding@home was introduced in 2000 and it eventually became one of the most powerful computing systems in the world; it reached 2.43 exaFLOPS (2.43 Eflops/s) in April 12, 2020 [54].

The CPU load of the computer running the grid software like SETI@home was usually around 100% depending on the software settings making the energy consumption also higher than in computers that were left to idle with power on. What is usually not considered is that developing and manufacturing a computer with a processor, mass storage, a Random Access Memory (RAM), a motherboard, a graphics card, and other electronics connected to the computer is also very resource-consuming. What if the computer is never used for anything (scientifically) useful? What if the computer is never even turned on? That computer is never wasting any electrical

energy from the wall socket, but still, vast amounts of energy and other resources were wasted during the manufacturing of the computer's microchips. Hoekstra *et al.* [52] claim that a 2-gram microchip has a virtual water content of 32 liters. For comparison, a 70-gram tomato has a virtual water content of 13 liters, and a 250-gram cotton T-shirt has a virtual water content of 2000 liters. Table 2 shows the virtual water content of selected products per unit of product and gram of product. According to Williams [55], secondary inputs of fossil fuels for manufacturing a microchip are 600 times the weight of the chip. This factor is around 1 or 2 for a car or refrigerator for comparison. We use the term ''manufacturing debt'' to describe the burden of manufacturing chips.

To counterbalance the wasteful manufacturing processes of electronics and wasteful idling of CPUs, one can donate spare computing cycles to scientific grid platforms like BOINC and Folding@home. These platforms then send workunits (analyzable data) to the computer to find new medicines for diseases like COVID-19, Alzheimer's, cancer, Huntington's, and Parkinson's. They can also send workunits to analyze radio telescope data to find evidence of extra-terrestrial intelligence or to simulate molecular interactions for material science research.

III. REVIEW OF GREEN TECHNOLOGIES

In this section we review the following technologies: Proof-of-Stake, The Lightning Network, Optical Computing, Reversible Computing, Ternary Computing, SolarCoin, Proof-of-Elapsed-Time, Renewable and Nuclear Energy, and Application-Specific Integrated Circuits.

A. PROOF-OF-STAKE

The second-largest cryptocurrency at the moment is ether (ETH), using the Ethereum blockchain [56] and a PoW consensus method. The mining of Ethereum's PoW is mostly done using Graphics Processing Units (GPUs) because it is challenging to develop Application-Specific Integrated Circuits (ASICs). The situation is not identical to Bitcoin's PoW because it was relatively easy to develop ASICs for Bitcoin mining [57]. As of April 21, 2022, Ethereum is using 105.63 TWh of electrical energy annually (comparable to the power consumption of Kazakhstan), and the carbon footprint is 58.91 Mt CO2 annually (comparable to the carbon footprint of Libya) [41]. The ASIC mining devices of Bitcoin have a service life of only about 1.5 years [58], and after that, they serve no practical purpose anymore because they can only calculate SHA256d hashes. Bitcoin mining generates 30.7 metric kilotons of e-waste annually, per May 2021 [11]. The numbers above give a strong incentive to develop environmentally friendly methods to achieve consensus in cryptoeconomies like Ethereum and Bitcoin. In 2022, Ethereum is switching from PoW to PoS. The first blockchain network to use PoS was probably Peercoin (or sometimes called ''PPCoin'') described in a whitepaper [59] in 2012. The native cryptocurrency, or coin, of the Peercoin blockchain, is peercoin (PPC).

BitFury Group has examined, in 2015, the pros and cons of PoW and PoS [60]. They use the term ''block mining'' to call the process of solving a computational challenge by a PoW protocol and the term ''block minting'' to call the process of solving a computational challenge by a PoS protocol. They list three important cryptocurrencies using the Hybrid PoW / PoS consensus method: Peercoin (PPCoin), Blackcoin, and Novacoin. They mention that the Nxt cryptocurrency uses the PoS consensus method alone, that BitShares uses Delegated Proof-of-Stake, and that Ethereum will use Delegated Proof-of-Stake in the future. The ''Nothing at Stake Problem'' is mentioned as a potential problem, which allows minting blocks on different branches after forking of the blockchain has happened.

How does a PoS system work? Tschorsch *et al.* [15] mention the concept of ''coin-age'', which is defined as the amount of currency multiplied by the holding period. If Alice sends ten coins to Bob, and Bob holds these coins for two weeks, the coin-age is 140 coin-days. Bob will destroy the accumulated coin-age by spending the ten coins. The coin-age is used to calculate the block reward in PoS. Minting a PoS block needs a hash value below or equal to a target value (similar to PoW mining). PoS (in contrast to PoW) has individual difficulty, which is inversely proportional to the coin-age. The PoS minters cannot use computational power to solve the puzzle faster than others because there is no nonce to modify. Every time the timestamp changes, the minters have a new chance to find the correct solution. After finding the correct solution, the minter broadcasts the block, including the coinstake transaction, rewarding the block minter.

For becoming a PoS validator (similar to being a PoW miner) in Ethereum, one needs to stake 32 ethers [61], which are worth almost 90,000 euros as of April 22, 2022. Because many people do not have such funds available, staking services (similar to PoW mining pools) allow users to serve as validators jointly. The more ethers one stakes (similar to having more mining power in PoW consensus), the greater the chance to win the lottery game of consensus forming.

The change from PoW to PoS should reduce Ethereum's energy consumption by 99% and allow 100,000 transactions per second [61]. From Table 1 we can assume that PoS version of Ethereum ''transaction'' (1% of PoW energy consumption after the 99% reduction) would consume about 2 kilowatt-hours. One PoS Ethereum ''transaction'' would consume as much as about 1600 Visa ''transactions''.

B. THE LIGHTNING NETWORK

The regular bitcoin payments operate on Layer 1. They were limited to around seven transactions per second globally before the SegWit update because the Bitcoin blocks are limited to about one megabyte of size, and mathematics guarantees that about 10 minutes pass between two blocks in general. On average, there are about six new Bitcoin blocks per hour. A common misconception links the Bitcoin network's throughput (transactions/s, or tx/s for short) and the Bitcoin network's energy consumption together. In reality, the

throughput is not directly connected to the amount of bitcoin mining power nor the energy consumption of those mining devices. It is possible to increase the number of bitcoin transactions per second without increasing the mining power and energy consumption.

The Lightning Network (a Layer 2 solution) is one possible method to have a considerable number (thousands) of bitcoin transactions per second. Litecoin was the first blockchain to test the Lightning Network. There is also a similar network for fast, cheap, scalable, and privacy-preserving payments (ERC-20-compliant token transfers) for Ethereum - the Raiden Network. The main idea is to open a micropayments channel, have almost unlimited transactions off-chain, and then close the micropayments channel. Only the transactions involved with the opening and closing of the micropayments channel will be recorded on-chain. Poon *et al.* [62] claim in the Lightning Network paper that 7 billion people making two transactions a day on Layer 1 would require 24-gigabyte blocks every ten minutes. However, seven billion people making two transactions a year (opening and closing the micropayment channels) on Layer 2 (the Lightning Network) would allow unlimited transactions inside the channel and require only 133-megabyte blocks every ten minutes.

C. OPTICAL COMPUTING

Optical computing means using light waves for processing, storage, and communication. Using conversion from photons to electrons would make the system slower and bulkier thus an efficient optical computing system needs three things:

- optical processor;
- optical data transfer; and
- optical storage.

Optical computing is still not widely used, so it is categorized as a form of unconventional computing in Table 3. Still, optical technologies are used for data transmission applications such as optical digital audio (TOSLINK) and fiber-optic communications (some versions of Ethernet). In everyday applications, optical technologies are used in cameras, displays, remote controls, optical mouses, and optical/magneto-optical discs (Laserdisc, CD, MiniDisc, DVD, HD-DVD, Blu-ray, and Ultra HD Blu-ray).

Sawchuck *et al.* [63] define optical computing as ''the use of optical systems to perform numerical computations on one-dimensional or multidimensional data that are generally not images''. They mention that optical signals can interact on time scales smaller than a picosecond (10^{-12} s) via an intermediary medium making high throughputs possible.

1) OPTICAL PROOF-OF-WORK

The motto for Bitcoin's PoW consensus method was ''one CPU, one vote,'' but today, the Bitcoin blockchain is secured by a small number of corporate organizations using ASIC machines, and the mining energy is coming from places with cheap electricity [64]. The ongoing discussion on climate change has also put some pressure on introducing greener cryptocurrencies. For example, Hal Finney, who was a Bitcoin pioneer, thought about ways to reduce carbon dioxide emissions of Bitcoin already in 2009 [50].

Optical Proof-of-Work (oPoW) is a PoW paradigm to decouple Bitcoin mining from energy. Dubrovsky *et al.* [6] present their oPoW Silicon Photonic Miner Prototype as a new application of modern analog computing and optical computing. It should make it possible to mine bitcoin even in areas with high electricity costs. oPoW should shift the operating expenses (OPEX) of electricity to hardware's capital expenses (CAPEX). The new consensus method is computable with photonic processors, but it should also be hardware-compatible with GPUs, Field-Programmable Gate Arrays (FPGAs), and ASICs, making it possible to use both

TABLE 3. Different forms of computing.

Different forms of computing		
Category	Explanation	Example
digital	Conventional computing, where information is discret.	Almost all of the computers of today.
analog	Unconventional computing, where information is continuous.	TDC Mark III.
binary	Conventional digital computing, which uses 2-valued logic.	Almost all of the computers of today.
ternary	Unconventional digital computing, which uses 3-valued logic.	Setun.
decimal	Unconventional digital computing, which uses 10-valued logic.	ENIAC.
irreversible	Conventional computing, which erases information and where going back to the previous state of the calculation is generally not possible.	Almost all of the computing in the past and nowadays.
reversible	Unconventional computing, which does not erase information and where going back to the previous state of the calculation is possible.	Mostly theoretical at the moment.
electrical	Conventional computing, which is controlled by electrical circuits.	Almost all of the computers of today.
mechanical	Unconventional computing, which is controlled mechanically.	Antikythera mechanism.
DNA	Unconventional computing, where the huge parallelization of the deoxyribonucleic acid is being used.	Mostly theoretical at the moment.
optical	Unconventional computing, where computations, data transfer and storage are done using optical methods.	Mostly theoretical at the moment.
classical	Conventional computing, where classical physics is used to process information.	Almost all of the computing in the past and nowadays.
quantum	Unconventional computing, where quantum physics phenomena are being used to process quantum information.	IBM Q 5 Tenerife.

optical and electrical (non-optical) computing methods for mining. A high-CAPEX PoW should also have the benefit of making the hash rate resilient to price fluctuations because it is not expensive to keep low-OPEX hardware online even during a period of low mining rewards [64].

Sawchuck *et al.* [63] predicted, in 1984, that optical systems might be cheaper than equivalent non-optical systems for specific signal processing applications. Interestingly, the developers of oPoW claimed, in 2021, that the silicon photonics used in oPoW are cheaper to develop because they use the older fabrication nodes (90 nm) than the state-of-the-art non-optical computing systems (5 nm) [64].

D. REVERSIBLE COMPUTING

When one calculates something with a regular computer, one asks the computer a question. For example, one is asking the computer "What is $2 + 2$?", and the computer answers "4". From the answer, it is not so easy to form the original question; the question could have been "What is $-6 + 10$?" or "What is $20 - 1 - 19 + 4$?" The information of the original question has been erased. Nevertheless, the information has not disappeared from the universe because there is the law of conservation of information. Erasing even one bit of information generates waste heat because of the laws of thermodynamics [65].

The conventional computing of today is irreversible, meaning that information is erased and vast amounts of waste heat are generated during computations. The computation process can be reversed in time in reversible computing to reaccess the previous states. Frank [66] states that reversible computing preserves signal energies and reuses them. The more popular method of unconventional computing - quantum computing - might only give some speedups on a few specialized applications, but reversible computing might achieve greater energy efficiency and functional performance for all digital computing applications. Reversible computing could be from 1000 to 100,000 times as cost-effective as irreversible computing in the 2050s [67].

Landauer [68] formulated

$$E = k_{\mathrm{B}} T \ln(2), \tag{1}$$

which states that E is the heat dissipated by a logically irreversible gate to its environment, k_{B} is the Boltzmann constant, T is the temperature of the environment in kelvins, and ln(2) is the natural logarithm of 2. At room temperature (293.15 K), erasing one bit of information generates about $2.805 \cdot 10^{-21}$ joules of heat [69].

Making gates logically reversible is probably not enough to achieve energy savings. The gates must also be physically reversible, which they are not in a traditional CMOS design. The charging and discharging of circuit elements must be adiabatic. The rules [69] to achieve this are

1) Do not turn on a switch if there is a significant voltage difference between the channel terminals.
2) Do not turn off a switch if there is a significant electrical current flowing through the channel of the switch.

Probably one of the earliest attempts to use reversible logic for developing secure cryptosystems was the research by Thapliyal *et al.* [70] in 2006. They present reversible designs of adders and Montgomery multipliers for a prototype of a reversible ALU for a cryptoprocessor. The motivation for this is the Differential Power Analysis (DPA), where attackers could break encryptions by measuring the energy consumed, Equation (1), in an irreversible digital circuit.

Heinonen *et al.* [71] suggested using reversible computing in bitcoin mining, but it is not known how much additional energy efficiency it would give (if any) when compared to the irreversible ASIC bitcoin mining. The paper showed that the number of bits generated by a regular ASIC miner is so high that any cloud-based scratch memory (used in reversible computing) is out of the question with any realistic Internet connection bandwidths of today (for example, 1 Gbit/s). There are also no practical reversible computing architectures when writing this. The suggestion to use reversible computing for bitcoin mining was made to motivate bitcoin ASIC developers to jump-start the development of reversible computing chips. Reversible computing might be the only way to keep increasing the computing power in the future after the conventional computing methods of today have reached their limits.

E. TERNARY COMPUTING

Digital computing is almost always using the binary base of two digits: 0 and 1. The binary base is not the only possible method for digital systems. For example, the ternary (trinary) system is based on three digits. The following list of trinary digit mappings is from Connelly's thesis [72]:

- unbalanced trinary: {0, 1, 2};
- fractional unbalanced trinary: {0, 1/2, 2};
- balanced trinary: {−1, 0, 1};
- unknown state logic: {F, ?, T};
- trinary coded binary: {T, F, T}.

In the previous list, "T" means True, "F" means False, and "?" means unknown (both T and F at the same time).

According to the IOTA Beginners Guide [73], ternary systems used for complex logic circuits within a CPU will lead to energy savings and also to space savings due to the smaller design of the microcontroller. Ternary systems have not been used because there is a lack of mass-market support. What other reasons could there be to change from binary logic to ternary logic? The ternary logic could [72], [74]–[79]

- reduce the required interconnections for logic functions;
- reduce the chip area;
- allow more information transformation over a line;
- reduce the memory requirements for data;
- allow higher speeds for serial operations.

The Ternary Manifesto by Douglas W. Jones [80] says that one ternary digit, a trit, can represent 1.58 bits. A 21-trit ternary computer could handle values as big as 33.18 bits, which is slightly larger than a 32-bit binary computer could handle. Jones also notes that a ternary computer would have

more transistors than a binary computer, but the number of wires would be reduced to 64%. Cambou *et al.* [81] suggest that balanced ternary logic is suitable for IoT security, authentication of connected vehicles, and also for hardware and software assurance. There are also ternary systems for quantum computers! These systems do not use qubits but qutrits. Caraiman *et al.* [82] use ternary quantum computing for image representation and processing.

1) IOTA

The IOTA Token [83] is a cryptocurrency that is designed for machine-to-machine (M2M), human-to-human (H2H), and human-to-machine (H2M) payments and for the Internet of Things (IoT). The ternary logic is there in many things: JINN is a ternary microcontroller, Troika is the hash function, and IOTA seeds only have capital letters from A to Z and the number 9. According to the IOTA Beginners Guide [73], the ternary system is more efficient because it has the highest density of information representation.

F. SolarCoin

SolarCoin is a blockchain-based project that rewards those who have solar installations generating electricity and have the appropriate SolarCoin software installed. If the solarcoin (SLR) price exceeds the production cost of the solar energy associated with the generated solarcoin, the solar power becomes basically free.

SolarCoin started as a new blockchain in 2014 [84], but in around 2021, it migrated to Ethereum. In the early days of SolarCoin, from January 2014 to August 2015, a PoW consensus was used, and later from August 2015 onwards, a Proof-of-Stake-Time was used [84].

Johnson *et al.* [84] noted in 2015 that the Bitcoin blockchain used 4,326,821,400.931 kWh of energy annually, and the SolarCoin blockchain (normalized to Bitcoin user size) would have used 328,725,000.000 kWh of energy annually. They calculated that the minimum energy required for a bitcoin ''transaction'' was 19.587 kWh and the minimum energy required for a solarcoin ''transaction'' was 0.1488 kWh

Johnson *et al.* [84] constructed and tested a SolarCoin node for 11 months. The system with a 250 W solar panel was generating on average 0.040 kWh per day and 0.00004 SLR (solarcoins) per day.

G. PROOF-OF-ELAPSED-TIME

Proof-of-Elapsed-Time (PoET) is a consensus method developed by Intel Corporation for permissioned blockchain networks where participants must identify themselves before they are allowed to operate. Intel developed PoET together with Software Guard Extension (SGX) technologies according to Bada *et al.* [14]. It is used in the Hyperledger Sawtooth platform. The other consensus methods that are available for Sawtooth [85] are Raft [86] and Practical Byzantine Fault Tolerance (PBFT) [87].

PoET does not need as much energy as typical PoW methods because PoET randomly selects a node for the consensus forming instead of requiring the miners to compete against each other. The algorithm generates a random wait time for each node in the network. The nodes must sleep over that time. The node that wakes up first (has the shortest sleep time) will win the lottery game and gets to add a new block to the blockchain. The code is also executed within a secure environment, and the lottery results are verifiable by external agents [88].

H. RENEWABLE AND NUCLEAR ENERGY

A simple solution to make Bitcoin greener is to use renewable and nuclear energy for bitcoin mining. This change would not require any changes to the Bitcoin protocol itself.

De Vries [58] concludes that renewable energy is not the answer to Bitcoin's sustainability problem. Also, the lifetime of ASIC mining devices is considerably short, producing lots of e-waste even if the mining itself is using sustainable energy. The conclusions come from the assumptions that it is challenging to unite bitcoin mining with renewable energy sources and that energy usage is not the only way in which bitcoin mining impacts the environment. Nuclear energy is not mentioned in De Vries' article.

Kardashev scale [16], [29] is a method of measuring a civilization's technological level from the power the civilization can use. The categories are Type 0 (or 0.0 on Carl Sagan's interpolated Kardashev scale), Type I (1.0), Type II (2.0), and Type III (3.0). Type 0 civilization is using 10^6 W of power; Type I civilization is using 10^{16} W of power; Type II civilization is using 10^{26} W of power; and Type III civilization is using 10^{36} W of power. According to common speculation, during the transition from Type 0 to Type I, the civilization has a high risk of self-destruction. After reaching Type I, the civilization might be safe. Currently, human civilization has not reached Type I yet. The human civilization is calculated, as in Equation 2, to be around 0.73 on Sagan's interpolated Kardashev scale.

$$K = \frac{\log_{10}(P) - 6}{10}, \tag{2}$$

where K is the Sagan's interpolated Kardashev rating of the civilization, and P is the power the civilization uses (in watts). Type I civilization can control its home planet's power output, Type II civilization can use its home star's entire radiation output, and Type III civilization has access to the power of its home galaxy.

We want to encourage the reader to think that it is not necessarily always wrong to have a considerable energy consumption. A technically advanced civilization needs lots of energy. Humanity should still try to optimize the energy consumption of their technologies (like bitcoin mining). What is usually overlooked is that we need a safe and environmentally-friendly way to produce vast amounts of cheap and usable energy. Solar power, at least in the form of solar power satellites, nuclear fusion energy, and nuclear

fission energy, are all potential candidates of technologies for the human civilization to become a Type I civilization. An advanced civilization could achieve Type II, perhaps, by building a Dyson sphere (basically a swarm of solar power satellites) that completely encompasses the star. Type III could be achieved by building a Dyson sphere for every star in a galaxy. There has been some interest in finding Dyson spheres in the Milky Way galaxy; for example, Minniti *et al.* [89] ask the question: Can we find candidate Dyson spheres in the Milky Way?

Can humanity reach Type I, and how? Ocean Thermal Energy Conversion (OTEC) is a form of renewable energy invented in 1881. It uses the ocean thermal gradient of deep & cool seawater and warm surface seawater for running a heat engine. Pelc *et al.* [90] mention the article by Thomas H. Daniel [91], which claims that about 10 TW of power could be generated by OTEC without affecting ocean's thermal structure. The cost of electricity, in 2002, from OTEC would have been around 0.08 USD/kWh and 0.24 USD/kWh (∼2002 USD price levels), which was much higher than fossil fuel costs, potentially leading the OTEC to be subsidized. A potential solution to make OTEC feasible is to incorporate Bitcoin mining [92]. The interconnected, medium-scale (5-to-10 MW) OTEC plant would cost something between 200 million USD and 300 million USD, and the cost of the electricity would be around 0.50 USD/kWh and 1.00 USD/kWh (∼2022 USD price levels). There would be tens of millions of US dollars savings by avoiding an offshore cable. The final estimate of the electricity price generated by this medium-scale stranded OTEC plant is around 0.11 USD/kWh (∼2022 USD price levels). The electricity would be sold to Bitcoin miners. Coincidentally, the Bitcoin Magazine article mentions the Kardashev scale.

There are also interesting projects on nuclear fission and nuclear fusion power, so nuclear power is not obsolete. Lockheed Martin's Skunk Works even has a slogan ''Restarting the Atomic Age'' [93]. Olkiluoto-3 nuclear fission power plant is operating and should be generating 1600 MWe of power before the end of 2022. Small Modular Reactors (SMRs) could make building nuclear fission power plants faster and cheaper. Olkiluoto-3 is an example of a big nuclear fission power plant, and facilities using an SMR would be examples of small nuclear fission power plants. There is a similar concept of facility size for nuclear fusion power; the trend was to build as large facilities as possible, for example, ITER, but nowadays, it is more attractive to do research and development on small nuclear fusion reactors [94].

I. APPLICATION-SPECIFIC INTEGRATED CIRCUITS

Hashes from different hashing algorithms are not comparable; for example, a SHA256d hash (used in Bitcoin) is not the same as a Scrypt hash (used in Litecoin). Therefore, the hashing rates (H/s) are different for SHA256d ASIC and Scrypt ASIC miners.

Taylor's paper [57] tells the story of early adopters of bitcoin who created the bitcoin ASIC mining industry. CPUs were used for bitcoin mining in 2009 and the early 2010s. Overclocked 6-core CPUs (Core i7 990x) could reach 33 MH/s. In 2010, bitcoin mining software could use GPUs for bitcoin mining. Nvidia's GPUs (GTX570) could reach 155 MH/s, and AMD's powerful gaming graphics card GPUs (7970) could reach 675 MH/s. The next stage started in 2011 and introduced FPGAs for bitcoin mining. CAPEX of Spartan 150 was higher per MH/s compared to AMD GPUs, but a power need of 60 watts compared to 200 watts of AMD GPUs made OPEX of Spartan 150 lower. The latest stage was the introduction of ASICs for bitcoin mining in 2013. After the ASICs became available, CPU, GPU, and FPGA bitcoin mining profits were negative.

Taylor [57] notes that bespoke (customized) silicon can be developed in small volumes. The first developer of Bitcoin ASICs was Butterfly Labs (BFL), taking pre-orders in June 2012 for three types of ASIC miners rated at 4.5 GH/s (Jalapeno), 60 GH/s (SC Single), and 1,500 GH/s (SC MiniRig). Introduced in May 2020, Bitmain's Antminer S19 Pro [95] was capable of achieving a hash rate of 110 TH/s, having an efficiency of 29.5 J/TH, and taking 3250 watts of electrical power.

IV. REVIEW OF JUSTIFICATION TECHNOLOGIES

It is not enough to make Green (energy-efficient) technologies. Hicks *et al.* [96] found that the usage of LED lighting might lead to the usage of more light, increasing the energy consumption and reducing or even eroding any energy savings from the energy-efficient LED technology. The Jevons paradox occurs when the efficiency of some resource usage increases, but the falling cost of the resource usage increases the demand and negates the gains from the efficiency. Modern economics knows this paradox as a rebound effect. In the 1980s, Daniel Khazzoom and Leonard Brookes independently had ideas that increased energy efficiency leads to increased energy usage. In 1992, this hypothesis was named a Khazzoom–Brookes postulate, similar to the Jevons paradox.

We believe that making more energy-efficient ASICs, building optical bitcoin miners, and reversible bitcoin miners will also lead to a higher demand for the bitcoin mining hardware negating any gains from the Green bitcoin mining technology. There is now a motivation to introduce some Justification Technologies.

In this section we review the following Justification technologies: Proof-of-Deep-Learning, Proof-of-Evolution, Prime Chain Proof-of-Work, Distributed Computing Grids, Merge-mining, Many-money Economy, and Hash Recycling.

A. PROOF-OF-DEEP-LEARNING

Chenli *et al.* [7] propose a consensus method called Proof-of-Deep-Learning (PoDL), which generates a valid proof of a new block after a proper deep learning model is produced. Their benchmark and simulation results prove their concept is plausible for various cryptocurrencies using a hash-based PoW consensus method.

The Deep Learning models used in PoDL had sizes from 100 kilobytes to 10 gigabytes [7]. There are techniques to reduce the sizes without affecting the accuracy very much.

The proposed method is not ASIC-resistant [7], quite the contrary: it is even mentioned that ASIC devices will be designed to do the deep learning training, and it will be favorable for the development of better hardware.

B. PROOF-OF-EVOLUTION

Proof-of-Evolution (PoE) is a consensus method developed by Bizzaro *et al.* [97] that keeps the security features of PoW and uses the mining process to execute genetic algorithms (GAs).

The proposed method also encourages cooperation among miners because it is possible to share the best solution found so far with miners, who can then add it to their population. It is similar to Proof-of-Search (also known as "PoS", not to be confused with Proof-of-Stake or Proof-of-Space) [98], which extends PoW for solving optimization problems.

C. PRIME CHAIN PROOF-OF-WORK

The prime number search is mostly focused on Mersenne prime numbers of the form

$$M_p = 2^p - 1, \tag{3}$$

where p is a prime number. They were named after Marin Mersenne. In 2013, the top 10 largest known prime numbers were all Mersenne prime numbers [99] as in Equation 3. The Primecoin whitepaper also mentions other well-known types of prime number pairs, such as twin primes, where both p and $p+2$ are prime numbers, and Sophie Germain prime numbers, where both p and $2p + 1$ are prime numbers. Cunningham Chain of the First Kind and the Second Kind and Bi-Twin Prime Chains are also explained with simple examples.

According to Primecoin's website [100], Primecoin's Prime Chain Proof-of-Work uses the search for Cunningham Chain of the First Kind, Cunningham Chain of the Second Kind, and Bi-Twin Prime Chain to secure the Primecoin blockchain. They state that Prime Chain PoW is valid and that primecoin (XPM) was the first cryptocurrency to achieve energy multi-use.

D. DISTRIBUTED COMPUTING GRIDS

In grid computing, one often encounters the term FLOPS. In cryptocurrency mining, one often encounters the term H/s. What are these terms? FLOPS means floating-point operations per second (flop/s). H/s means hashes per second.

1) GRIDCOIN

According to the Gridcoin Blue Paper [101], gridcoin (GRC) is a decentralized PoS cryptocurrency that incentivizes participation in the BOINC distributed computing grid platform. According to the Gridcoin White Paper [102], an iPhone 6 has seven gigaFLOPS of computing power. They also calculate that all 2.5 billion smartphones in the world would form a computing network of about 17.5 exaFLOPS, and if they are idling half of the time, this computing power will reduce to about 8.75 exaFLOPS. They predicted that in 2020 there would be over 5 billion smartphones in the world.

2) CURECOIN

Curecoin (CURE) [103] is a cryptocurrency reward for those who create computing power for some selected Distributed Computing Networks (DCNs) - currently, only the Folding@home project as in Figure 2. The automated distribution system is located at cryptobullionpools.com. Curecoin has an efficient PoS-like system. The Curecoin wallet can be seen in Figure 3.

3) FOLDINGCOIN

The foldingcoin (FLDC) token [104] is using the Counterparty protocol [105], which allows tokens on the Bitcoin blockchain. There is a method of Proof-of-Fold to verify the computational power contributed to the Folding@home project.

The Foldingcoin White Paper claims the following

- At the end of 2012, there was 25 TH/s of mining power in the Bitcoin network coming from CPUs and GPUs, because ASICs were not available back then.
- Hashing does not do any floating point operations and it is not possible to directly convert from TH/s to petaFLOPS, but there is a generally-accepted ratio of 1 TH/s = 12.7 Pflop/s.
- Therefore, there was 25 TH/s $= 25 \cdot 12.7$ Pflop/s $\approx$ 318 petaFLOPS of unused CPU and GPU computing power available around the beginning of the ASIC Bitcoin mining era.

Foldingcoin's market capitalization did not get any updates after October 2018 in CoinGecko.

E. MERGE-MINING

New and small blockchains tend to have the problem of not having enough benevolent mining power; it could be relatively easy for malicious parties to take them over [106]. Cryptocurrencies are usually competing against each other for computational resources. The competition does not always have to be the case; merge-mining (or merged mining) [107] means the act of mining two or more cryptocurrencies at once without additional PoW effort. The process is also known as Auxiliary Proof-of-Work (AuxPoW). The merge-miners will get extra profits without having to add any extra mining efforts.

Judmayer *et al.* [108] and Zamyatin [109] state that little was known about the effects and implications of merge-mining even though it had been used for several cryptocurrencies. Judmayer *et al.* found that mining pools with merge-mining cryptocurrencies had operated at the edge of, and even beyond, the security guarantees of the Nakamoto consensus. Merge-mining could centralize mining, which is against the principle of decentralization. Ali *et al.* [106] found

FIGURE 2. **Folding@home currently lets the user to choose from research for COVID-19, Alzheimer's, Cancer, Huntington's, and Parkinson's. There are also options for "Any disease" and "High Priority".**

that the then-largest merged-mined cryptocurrency, namecoin, was vulnerable to the 51% attacks giving a false sense of security.

F. MANY-MONEY ECONOMY

Like most blockchains at the moment, the Bitcoin blockchain is only using one type of coin/cryptocurrency. What if the Bitcoin blockchain had two (or more) different types of cryptocurrencies? It is well known that bitcoin (BTC) is suitable for saving money, but it is not so good for spending money. What if there was a protocol update for Bitcoin that introduces a second coin type - perhaps a good coin for spending?

Heinonen *et al.* [71] introduced the idea of the inflationary bitcoin coin (BTCi) to motivate the old mining device users to keep on mining. That kind of coin should reduce the amount of e-waste from ASIC machines. They call the regular bitcoin coin (BTC) the deflationary bitcoin coin (BTCd), and they say that these two different coin types could have different exchange rates and money supply sizes. The motivation for two different monies in the Bitcoin blockchain is that the regular bitcoin (BTCd) is not used so much for everyday spending, making the regular one-money Bitcoin blockchain, not a good candidate for a Decentralized Payments System (DPS). The two-money Bitcoin blockchain would be a far better candidate for a DPS.

Heinonen [110] introduced the idea of antimoney bitcoin coin (aBTC). The research suggested using antimoney to enable payments when Morini's stablecoin is frozen. The above is also an example of a many-money economy.

Ethereum is an excellent example of a many-money economy in a blockchain. Coins are the native cryptocurrencies of a blockchain; tokens are cryptocurrencies based on smart contract technologies. The ether coin (ETH) is the native cryptocurrency of the Ethereum blockchain, and there are thousands of tokens using the smart contract technology, for example, the ERC-20 tokens. These ERC-20 tokens are all stored in the same Ethereum blockchain as the ether (ETH) transactions. There are also many other token standards than

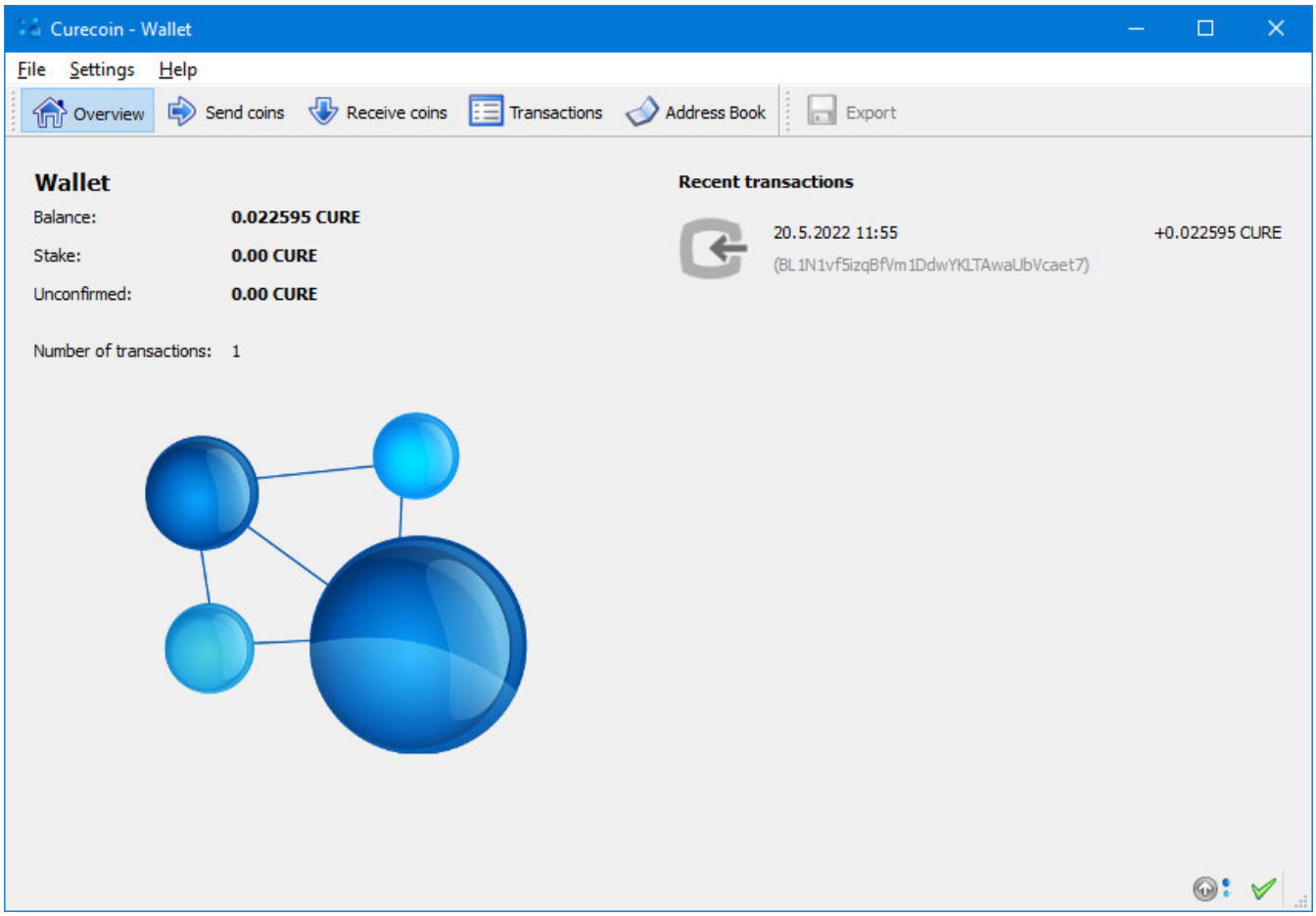


FIGURE 3. Curecoins will be received to the Curecoin wallet after donating spare computing cycles for Folding@home project as a member of the Curecoin team.

the famous ERC-20; Non-Fungible Tokens (NFTs) use other standards. Research on the behavior of price changes of cryptocurrencies is done by Stosic *et al.* [111], and research on the behavior of price changes of ERC-20 tokens is done by Heinonen *et al.* [112].

G. HASH RECYCLING

There are lots of PseudoRandom Number Generators (PRNGs) available such as Blum Blum Shub [113], Yarrow [114], and Fortuna [115]. They can be used to generate numbers that are not true random numbers because computers of classical computing behave in a deterministic way. One could use unconventional computing like quantum computing to produce real random numbers. There are also Quantum Random Number Generators (QRNGs) [116] that generate perfectly unpredictable random numbers from a quantum source.

Still, we are far from using quantum computing in everyday computing, so we should concentrate on classical computing and its deterministic applications like the generation of pseudorandom numbers. How can we make a connection between bitcoin mining and pseudorandom numbers? Heinonen *et al.* [71] introduced the concept of hash recycling. The idea came from the LavaRand method [117] that uses digital images of lava lamps for seeding PRNGs. LavaRand takes a digital picture of a lava lamp, converts the image to binary numbers, applies a cryptographic hash function, obtains a seed from the hash function, and feeds that seed to the PRNG. The idea is to have a public entropy pool on the Internet. A user could use the public entropy pool like the Hardware Random Number Generators (HRNGs) [118], which are usually used to generate the seed for a faster PRNG, which generates pseudorandom numbers at a much higher date rate [119].

It is an interesting observation that according to Heinonen *et al.* [71], there were about 10^{28} hashes and $2.56 \cdot 10^{30}$ bits generated to secure 703,364 blocks to the Bitcoin blockchain between early 2009 and late 2021. The Kardashev scale mentioned earlier is about a civilization's access to power and energy. There is a similar rating concept regarding civilization's access to information. This scale is developed by Carl Sagan [29]. He assigned the letter A to represent 10^6 unique bits of information. Each successive letter (the English alphabet's letters running from A to Z)

represents an order of magnitude increase, which means that a level Z civilization would have access to 10^{31} unique bits. In 1973, humanity was a 0.7H civilization. In 2018, humanity was a 0.73J civilization. Bitcoin mining alone would get humanity easily to level Z, but because humanity does not have access to those wasted hashes anymore, the information rating level of humanity is probably still around level J. Of course, there is nothing extraordinary in bitcoin mining in this regard; any other form of heavy computing (like video gaming and grid computing) will also generate huge amounts of bits. It is not possible at the moment to store $\sim 10^{31}$ bits, and Sagan believed that no civilization has yet reached level Z. In 2012, Baker [120] claimed one gram of DNA could store 455 exabytes ($4.55 \cdot 10^{20}$ bytes) or $3.64 \cdot 10^{21}$ bits of data.

V. "A MIX OF BOTH" TECHNOLOGIES

In this section we review the following technologies: Satcoin, Decentralized Storage Solutions, MultiAlgo, and Blockchain Games.

A. SATCOIN

Boolean Satisfiability (SAT) problem is a problem of finding an assignment of Boolean variables to Boolean formula so that it evaluates to true. SAT problem was proven to be NP-complete. There are many SAT solvers implementing algorithms with exponential complexity that have been used for analyzing cryptographic functions [121]–[124], scheduling, electronic design automation, and for many other things. Manthey *et al.* [22] state that the Bitcoin mining algorithm is based on brute force. They also describe how the mining process could use SAT solving instead. The process of SAT solving for bitcoin mining was already described by Heusser [21] in 2013, where he reformulates hash finding as an SAT with 250,000 variables. The proposed SAT solving method is not based on the brute force search method; instead, it uses algorithms for SAT solving based on back-tracking. The claimed results are significant performance improvement and that the proposed algorithm gets potentially more efficient with increasing difficulty of Bitcoin. However, Heusser does not claim that the proposed SAT solving method would be faster than the brute force method using currently available SAT solvers; it may become more efficient.

B. DECENTRALIZED STORAGE SOLUTIONS

Decentralized Storage Solution (DSS) is a bunch of methods to decentralize cloud storage solutions. Solutions such as Filecoin, Sia, StorJ, MaidSafe, Chia, and Permacoin. For example, Permacoin stores some public data like essential books, and Filecoin can store private data like photos and videos coming from regular users.

1) PROOF-OF-SPACE & PROOF-OF-TIME

Chia (XCH) is enterprise-grade digital money using blockchain technologies. The consensus method of Chia is Proof of Space and Time, which means that Chia farming (similar to Bitcoin mining) uses disk space as the resource for securing its blockchain [125]–[128]. Proof-of-Space means users (or "farmers") allocate unused Hard Disk Drive (HDD) or Solid State Drive (SSD) space for storage by storing cryptographic numbers on disk into large files called "plots". Farmers will scan their plots after a new block is broadcast on the Chia's network. They will check if there is a number close to the new challenge number coming from Proof-of-Time. The second consensus method, Proof-of-Time, is needed to ensure that an actual wall clock time has passed between blocks.

Chia's method is not using vast amounts of electricity for consensus, but there is still the e-waste problem [129] of broken Flash drives on some setups of the Chia environment. For example, Chia farmers have noticed that 256 GB SSD might last only 40 drive-write days, 512 GB SSD might last only 80 drive-write days, and 1 TB SSD might last only 160 drive-write days [130].

Fisch [131] construct a practical Proof-of-Space (also known as "PoS", not to be confused with Proof-of-Stake or Proof-of-Search), which can be used to demonstrate that a prover is using space to store information. His article states that Proof-of-Space is an alternative to PoW for applications like spam prevention, Denial-of-Service (DoS) attacks, and Sybil resistance in blockchain network consensus methods. Proof-of-Space is egalitarian and eco-friendly because it is ASIC-resistant and uses (and reuses) mass storage space instead of energy, which cannot be reused easily.

2) PROOF-OF-RETRIEVABILITY

Miller *et al.* [132] show that Bitcoin's resources could be repurposed for valuable tasks. Permacoin is a cryptocurrency that uses Proof-of-Retrievability (POR) for archiving and accessing some public data like books. Permacoin requires both computational and storage resources. Bitcoin's mining mechanism is called a Scratch-Off Puzzle (SOP), which involves continuous attempts to solve puzzles. They use the POR consensus as an SOP to start a competition among miners to access random local copies of files as a Decentralized Storage Solution (DSS), and then they use a model of rational economic agents and claim that their SOP has the essential properties of the Bitcoin PoW mechanism.

3) FILECOIN

Filecoin is an open-source cloud storage marketplace, protocol, and incentive layer. The project developers have published a paper on Proof-of-Replication (PoRep) [133] and released a paper on Power Fault Tolerance (PFT) [134]. The paper on PoRep claims that PoRep is a new kind of Proof-of-Storage, which can be used to prove that some data has been replicated in physical storage. The system enforces unique physical copies so that the verifier can check that the prover is not gaming the system by deduplicating the same data into the same storage space. The paper on PFT gives a formal definition for PFT, which reframes Byzantine Fault Tolerance (BFT) in terms of users' influence over the

protocol's outcome instead of the number of nodes. Filecoin's native cryptocurrency is filecoin (FIL).

4) SIA

According to Sia's documentation [135], Sia is a platform for decentralized storage. Users can make publicly auditable storage contracts in the blockchain defining what data will be stored and what price. Sia blockchain's native currency is siacoin (SC). There were plans for Sia to become a sidechain as a two-way peg to the Bitcoin blockchain in the future.

5) StorJ

StorJ is a Decentralized Cloud Storage (DCS) that encrypts files and splits them into 80 pieces each. According to the StorJ website [136], retrieving a file only needs 29 of those pieces. StorJ's native cryptocurrency is STORJ.

6) THE SAFE NETWORK BY MaidSafe

The Safe Network is replacing the vulnerable structures of the Web with more decentralized methods [137]. Proof-of-Resource in the Safe Network is a method, similar to a Zero Knowledge Proof, that measures a node's ability to store and retrieve data chunks [138]. The cryptocurrencies associcated with Safe Network are MaidSafeCoin (MAID) and (eMAID) and Safe Network Token [139].

C. MultiAlgo

The MultiAlgo solution is a bit similar to the Hybrid PoW & ''PoX'' solution because they both use multiple different methods to achieve consensus. The difference is that the MultiAlgo is about a PoW mechanism with multiple different (but otherwise quite similar) hashing functions used to form consensus, and the Hybrid PoW & ''PoX'' solution uses PoW and some other form of consensus methods (''PoX''), which can be very different from each other. ''PoX'' can be almost any consensus method, but usually it is PoS.

Many cryptocurrencies are using the MultiAlgo solution. It means securing the blockchain with several different hashing algorithms [140]. One motivation to use multiple algorithms is to make the cryptocurrency more resistant to a single hash function getting cracked [141]. The second motivation is to make the cryptocurrency more resistant to ASIC mining.

X11 [142] is a MultiAlgo solution with 11 different hash functions: Blake, BMW, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, and Echo. There are several cryptocurrencies using X11, one of them is Dash (formerly: Darkcoin, XCoin). There are now ASICs for X11, one of them is Spondoolies SPx36 [143], and more advanced MultiAlgo solutions are now available, such as X12, X13, X14, X15, X16, and X17.

1) DigiByte

DigiByte (DGB) uses five different hashing algorithms: SHA256, Scrypt, Odocrypt, Skein, and Qubit. Odocrypt is said to be ASIC resistant by rewriting and morphing itself every ten days, and it is focused on utilizing FPGA mining [144].

2) QUARKCOIN

Quarkcoin (QRK) [141] uses six different hashing algorithms: BLAKE, Blue Midnight Wish, Groestl, JH, Skein, and Keccak. There are nine rounds of hashing from these six different algorithms. The archived website of Quarkcoin [145] claims that Quarkcoin has 0.5% inflation to keep mining activity going and the Quarkcoin blockchain safe against 51% attacks. They also claim Quarkcoin to be ASIC resistant and CPU mining only.

D. BLOCKCHAIN GAMES

Yuen *et al.* [146] propose a Proof-of-Play (PoP) consensus model for peer-to-peer games. The aim is to create a system that forms a consensus by using the blockchain itself. They compare their model to the conceptual Proof-of-Excellence, but the player does not need to be excellent - the act of playing should be enough for mining.

The idea of Proof-of-Play or Proof-of-Thought might initially come from a blockchain-based videogame called Motocoin.

1) MOTOCOIN

Motocoin [147] was probably the first to use the Proof-of-Thought (or Proof-of-Play) consensus method. The human cognitive workload can be used for mining the motocoins (MOTO) with the method. The name Motocoin comes from the 2D motorbike simulation game, which the player needs to play to form the consensus. When the level is finished, there will be a verifiable chain of commands, proof that a solution has been found. The proof is then attached to blocks [148].

According to Kraft [148], Motocoin's ''PoW''(probably meaning Proof-of-Thought or Proof-of-Play)[2] itself is formulated in terms of a game. The method is compared to the Sudoku puzzle-solving analogy when explaining Bitcoin mining to the general public. Kraft also states that, unlike Huntercoin, Motocoin's blockchain is not associated with a global game state.

According to the homepage of Motocoin [149], the game was dominated by bots, but the developers were also able to introduce a new security model.

2) HunterCoin

HunterCoin is a cryptocurrency blockchain and a multi-player videogame where the player collects coins on a map. As was the case with Motocoin, bots are playing the game. The process of a human player collecting coins inside a game world is called Human mining (or AI mining, if the player is a bot), and the status of the competition, which is getting more difficult over time, is called Human (or AI) Difficulty level [150]. Ujunwa's article on blockchain gaming [151]

[2]Note by the corresponding author of this survey.

uses the term Proof-of-Mining for the method of collecting coins by a human player. HunterCoin is an example of many novel technologies like a) human mining or manual mining, b) MultiAlgo (SHA256d and Scrypt), and c) merge-mining.

Kraft [148] reviews HunterCoin's principles and proposes a protocol that enables trustless off-chain interactions of players. The paper mentions that every node on the Huntercoin network can verify that the gameplay follows the rules.

The huntercoin cryptocurrency (HUC) is mined using PoW, and it can be merge-mined at least with bitcoin, and litecoin (LTC), because the hashing algorithms are SHA256d and Scrypt. The block reward is 10 HUC. Human mining means that a part (9 HUC) of a block reward goes inside the game world, where hunters can collect and bank them to their cryptocurrency address; the other part (1 HUC) of the block reward goes to the PoW miners. There can also be fights over resources in this two-dimensional world so that the hunter might lose all the coins [150].

VI. RESEARCH QUESTION

We form our Research Questions based on the analysis above. The Research Question is: What technological solutions do we have to make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified?

VII. DISCUSSION

This section discusses all the previously mentioned technologies, our categories, and whether using this technology in Bitcoin is plausible. Not being plausible does not mean it will be impossible to use the technology in Bitcoin, but we see it is impractical for Bitcoin. Not being plausible also does not mean being inferior. Bitcoin was originally meant to be a Decentralized Payment System, making it difficult to use technologies like SolarCoin's centralized incentive system or Motocoin's Proof-of-Play (good for a gaming environment) in Bitcoin. We also discuss if some Distributed Computing Grid coins can compete with bitcoin or ether. Table 4 shows our discussion's main outcome.

TABLE 4. Plausibility of green and justification technologies for bitcoin.

Technology	Category	Plausible for Bitcoin?
Proof-of-Stake	Green	Yes
The Lightning Network	Green	Yes
Optical Computing	Green	Yes
Reversible Computing	Green	No and Yes
Ternary Computing	Green	Yes
SolarCoin	Green	No
Proof-of-Elapsed-Time	Green	No and Yes
Renewable and Nuclear Energy	Green	Yes
Application-Specific Integrated Circuits	Green	Yes
Proof-of-Deep-Learning	Justification	Yes
Proof-of-Evolution	Justification	Yes
Prime Chain Proof-of-Work	Justification	Yes
Distributed Computing Grids	Justification	Yes and No
Merge-mining	Justification	Yes
Many-money Economy	Justification	Yes
Hash Recycling	Justification	Yes
Satcoin	Both	Yes
Decentralized Storage Solutions	Both	Yes and No
MultiAlgo	Both	Yes
Blockchain Games	Both	No

A. GREEN TECHNOLOGIES

Green technologies are discussed in this part of the paper.

1) PROOF-OF-STAKE

We categorize Proof-of-Stake as Green because this consensus method will reduce the energy consumption of Ethereum by 99% [61]. We think this method is plausible for Bitcoin because PoS is already being tested on Ethereum, and although ether is not designed to be a cryptocurrency for a DPS like bitcoin, it has the second-largest market capitalization as seen in Figure 4.

2) THE LIGHTNING NETWORK

There are at least two reasons why the Lightning Network (LN) is Green. First, the LN increases the number of bitcoin transactions from several transactions per second to at least thousands of transactions per second without increasing the energy consumption of bitcoin mining. Second, the LN will also save storage space and Internet bandwidth by recording off-chain the transactions happening between the opening and closing transactions of the micropayments channel. LN is also plausible for Bitcoin because it is already used in Bitcoin.

3) OPTICAL COMPUTING

According to our judgment, Optical Computing is Green because OPoW introduces optical computing methods for cryptocurrency mining. OPoW is plausible for Bitcoin because it is tailor-made for Bitcoin. Optical computing is a possibility for making Bitcoin greener.

4) REVERSIBLE COMPUTING

Reversible Computing should be categorized as Green because it has the potential to be from 1,000 to 100,000 times as cost-effective as irreversible computing in the 2050s. It is plausible for Bitcoin if a reversible computing architecture is developed first. At the moment of writing this, there is no such architecture.

5) TERNARY COMPUTING

Ternary Computing should also be categorized as Green because the theory states that the ternary system has the highest density of information representation. It should not be impossible to make bitcoin mining ASIC chips based on the ternary system. Therefore, we categorize it as plausible for Bitcoin.

6) SolarCoin

SolarCoin is categorized as Green because it incentivizes solar power for blockchain applications. We think it is not directly applicable to Bitcoin because SolarCoin is a very centralized model, and Bitcoin is meant to be very decentralized.

7) PROOF-OF-ELAPSED-TIME

PoET is a Green technology because it replaces the computing power competition of PoWs with a random time length of napping. PoET is designed for permissioned blockchains, and it is not directly applicable to Bitcoin. Still, maybe it is not difficult to make a version of PoET that is workable for permissionless blockchains like Bitcoin and Ethereum.

8) RENEWABLE AND NUCLEAR ENERGY

Renewables (solar power, wind power, and hydropower) and nuclear energy are Green and very much plausible for Bitcoin to use even when writing this article. As was mentioned earlier, Bitcoin mining might be cleaner than generally assumed. Bitcoin mining might also make OTEC profitable.

9) APPLICATION-SPECIFIC INTEGRATED CIRCUITS

ASICs are Green because they are faster (more energy-efficient) at bitcoin mining than CPUs, GPUs, and FPGAs. There are probably still some innovations coming for ASICs to make them even more energy-efficient for bitcoin mining. ASICs are plausible for Bitcoin because they have been used in bitcoin mining since 2013.

B. JUSTIFICATION TECHNOLOGIES

Justification technologies are discussed in this part of the paper.

1) PROOF-OF-DEEP-LEARNING

Deep Learning is known for consuming lots of energy for training the models. Typically, models are trained on GPUs. Research article [7] proposes the PoDL method, which consists of replacing current PoW with the procedure of training deep learning models and submitting trained models that will be evaluated on an independent dataset. Then, the miner who submitted the model with the highest performance (such as accuracy) will validate a block and gain the reward. Bitcoin is one of the cryptocurrencies that could use the method. Therefore, we list PoDL as a plausible technology for Bitcoin. We only categorize PoDL as a Justification Technology.

2) PROOF-OF-EVOLUTION

We think PoE is a Justification technology because it adds additional value (executes genetic algorithms) to the mining process. According to the research [97], PoE is closely related to Bitcoin's PoW, so we categorize PoE as plausible for Bitcoin.

3) PRIME CHAIN PROOF-OF-WORK

Prime Chain PoW should be categorized as a Justification technology because it gives some scientific value (finds new prime numbers) to the mining process. It is difficult to say if Prime Chain PoW would work for Bitcoin as well as it has worked for Primecoin, but maybe the MultiAlgo method could be used in Bitcoin and have at least some of the Bitcoin blocks mined by the Prime Chain PoW consensus.

4) DISTRIBUTED COMPUTING GRIDS

We downloaded historical market capitalization data in US Dollars for bitcoin (BTC), ether (ETH), gridcoin (GRC), curecoin (CURE), and foldingcoin (FLDC) from CoinGecko (https://coingecko.com) for date ranges from 2013-JAN-01 to 2022-MAY-18. The lin-log plot of the market capitalization data is in Figure 4. From the data, gridcoin, curecoin, and foldingcoin are older cryptocurrencies than ether, and their market capitalizations are still considerably lower than ether's market capitalization. Foldingcoin's market capitalization did not get any updates after October 2018 in CoinGecko. The highest market capitalization for gridcoin was about 83.6 million US dollars on 9 January 2018. Bitcoin's highest market capitalization is more than 10 thousand times that. We conclude that Distributed Computing Grid coins cannot compete yet with bitcoin and ether.

The technology of Distributed Computing Grids is more about Justification than Green technology. Could Bitcoin's PoW be replaced by the methods used in Gridcoin, Curecoin, or Foldingcoin? Probably it could not be replaced by them directly because Bitcoin is all about decentralization, and having a centralized source of analyzable data (for example, protein folding data) makes the system very centralized, giving an advantage [8] for those organizations that control the analyzable data. We still believe that there could be some ways to introduce useful Distributed Computing Grids in bitcoin mining. On blockchains that use an advanced form of smart contracts, like the Ethereum blockchain, one could use customizable PoWs for tokens. Maybe the Bitcoin blockchain will also use more advanced smart contracts directly in the future; nowadays, they can be run on the Rootstock (RSK) sidechain [152]. However, another possibility we can think of is a form of Hybrid Proof-of-Work & "Proof-of-X" method, where only some of the blocks are ASIC-mined SHA256d PoW blocks and some of the blocks are CPU & GPU mined Distributed Computing Grid "Proof-of-X" blocks that will use the spare computing cycles for scientific computing. Therefore, we have categorized Distributed Computing Grids as Justification Technology that could be and could not be plausible for Bitcoin.

5) MERGE-MINING

Merge-mining is a Justification Technology because it gives new value to cryptocurrency mining: instead of securing only one blockchain, merge-mining makes it possible to secure two or more blockchains without extra mining efforts. The miner will get not only one but two (or more) cryptocurrencies as a reward for the merge-mining. Merge-mining could also be labeled as Green technology because, in a way, it might lower the total energy consumption used for cryptocurrency mining. However, it is uncertain if cryptocurrencies with low market capitalizations are attractive enough for large-scale mining without the merge-mining technology.

Bitcoin has been merge-mined for years with several other SHA256d PoW cryptocurrencies. Therefore, merge-mining for Bitcoin is plausible. However, there are some security

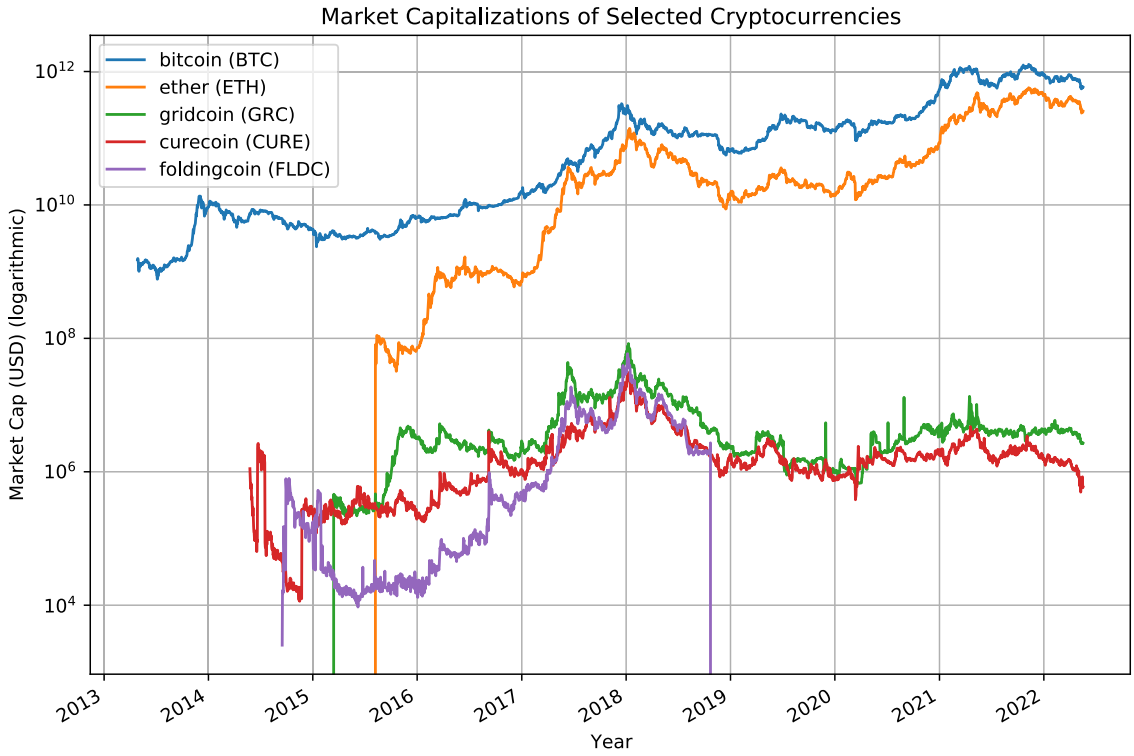


FIGURE 4. Market capitalizations for bitcoin (BTC), ether (ETH), gridcoin (GRC), curecoin (CURE), and foldingcoin (FLDC) in US Dollars (USD).

issues with merge-mining regarding cryptocurrencies with less mining power available than Bitcoin.

6) MANY-MONEY ECONOMY

Introducing new coin types for the Bitcoin blockchain would not reduce energy consumption, but it would make the Bitcoin cryptoeconomy more valuable if the new coin is better as a daily payment method than the regular bitcoin coin (BTC). It would be even better if the miners (using old, non-profitable, ASIC mining hardware) were given the second type of bitcoin coin as a block reward. This method should solve, at least partially, the problem of e-waste. Therefore, we judge this technology as a Justification technology, and we believe it could work for Bitcoin as a hard fork.

7) HASH RECYCLING

Hash Recycling does not reduce the energy usage of bitcoin mining, but it gives new value to the hashes that would be otherwise wasted and erased. We categorize it as a Justification Technology. We believe this technology could be implemented in Bitcoin today.

C. "A MIX OF BOTH" TECHNOLOGIES

"A Mix of Both" technologies are discussed in this part of the paper.

1) SATCOIN

We think Satcoin is both Green and Justification technology because SAT solvers have the potential to reduce energy utilization due to more efficient algorithms, and SAT is useful itself, and they can solve practical SAT instances. We also think this could be used in Bitcoin.

2) DECENTRALIZED STORAGE SOLUTIONS

We think Decentralized Storage Solutions could be both Green and Justification technologies. There are many different Decentralized Storage Solutions like Chia, Permacoin, Filecoin, and many others.

For example, Chia could be labeled as a Green Technology because it does not use lots of computing power, but, on the other hand, Chia is known for the Flash drive e-waste problem.

Permacoin is a Justification technology because important data like open-source scientific research articles and old books could be stored in a decentralized manner. What if Bitcoin used this method to store Wikipedia articles or the research articles of Ledger Journal, or the free books of the Project Gutenberg? Storing important public data would make Bitcoin more valuable and justified even for those who do not use the bitcoin cryptocurrency itself. We believe solutions like Permacoin could be plausible for Bitcoin.

3) MultiAlgo

MultiAlgo could potentially mean some changes in energy usage if Bitcoin started using it. For example, if Bitcoin had an ASIC-resistant PoW, it would mean that more people could have access to bitcoin mining by using hardware like CPUs and GPUs. There would also not be such a considerable e-waste problem because CPUs, GPUs, and FPGAs can easily

be repurposed for general computing if mining cryptocurrencies is neither profitable nor exciting anymore. We have categorized MultiAlgo as both Green and Justification technologies, and we believe it could be plausible for Bitcoin as a hard fork.

4) BLOCKCHAIN GAMES

Proof-of-Thought (or Proof-of-Play) is an exciting consensus method for blockchain videogames. HunterCoin has the concept of Human mining, which means that a human player can collect coins inside the game world. We categorize these technologies as Green technologies because there is a potential for less electricity usage if human cognitive power is used. We categorize them also as Justification technologies because they have the potential to revolutionize video gaming and science. What if a protein folding game like Foldit (https://fold.it) or neuron resolving and tracing game like Mozak (https://www.mozak.science/) started using these technologies? They could attract more human cognitive power to scientifically valuable games. We believe they are not plausible for Bitcoin, at least not directly, because a change to become a sort of a gaming platform would be too radical a change for a DPS like Bitcoin.

VIII. CONCLUSION

Our Research Question was: What technological solutions do we have to make various cryptocurrencies, including bitcoin (BTC) and ether (ETH), greener and more justified? We answer that there are many solutions already in place: Hybrid Proof-of-Stake and Proof-of-Work have been used since 2012 in Peercoin and various other cryptocurrencies since then; SolarCoin started in 2014; Proof-of-Elapsed-Time has been used in some permissioned blockchains; sustainable energy has been used more for cryptocurrency mining than it has been used in the default US energy mix according to estimates based on a survey of miners; Bitcoin ASICs have been used since 2013; Primecoin started in 2013; distributed computing grid coins (gridcoin, curecoin, foldingcoin) were introduced around the mid-2010s; merge-mining has been possible since the early 2010s; there are many attractive Decentralized Storage Solutions (like Chia); digibyte and quarkcoin are classical examples of cryptocurrencies using the MultiAlgo method, and there have been at least two video gaming blockchains (Motocoin and HunterCoin) to use human cognitive power for cryptocurrency mining. There are now plans to use unconventional computing methods (reversible computing, ternary computing, optical computing, analog computing) to solve some of the issues regarding the vast energy consumption of conventional computing (including cryptocurrency mining).

We think using spare computing cycles for grid computing efforts is justified. For example, there are billions of smartphones in the world. Many smartphones are being recharged every day. If this daily recharging period of twenty to sixty minutes would be used for grid computing, for example, finding new cures to cancer, it would probably be a significant breakthrough for medical research simulations. We call on the cryptocurrency communities to research and develop grid computing and unconventional computing methods for the most significant cryptocurrencies: bitcoin (BTC) and ether (ETH).

Further research could include writing a new part for this survey with more technologies analyzed. It would also be interesting to analyze issues and find solutions regarding the vast energy consumption of video gaming, including PCs, consoles, tablets, smartphones, and cloud gaming. There should also be research on how much should a regular chip (in a PC or a smartphone) have to perform distributed computing during its lifetime in order to pay back "the manufacturing debt".

REFERENCES

[1] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.

[2] H. Müller and M. Seifert, "Blockchain, a feasible technology for land administration," in *Proc. FIG Work. Week, Geospatial Inf. Smarter Life Environ. Resilience*, 2019, pp. 22–26.

[3] *Bitcoin Could Become World Reserve Currency, Says Senator Rand Paul | NASDAQ*. Accessed: Jun. 3, 2022. [Online]. Available: https://web.archive.org/web/20211221170532/https://www.nasdaq.com/articles/bitcoin-could-become-world-reserve-currency-says-senator-rand-paul-2021-10-25

[4] *How Blockchain-Based Apps and Sites Resist DDoS Attacks | VentureBeat*. Accessed: Jun. 3, 2022. [Online]. Available: https://web.archive.org/web/20220420032420/https://venturebeat.com/2017/06/25/how-blockchain-based-apps-and-sites-resist-ddos-attacks/

[5] K. Raworth, *Doughnut Economics: Seven Ways to Think Like a 21st Century Economist*. New York, NY, USA: Penguin Random House, 2018.

[6] M. Dubrovsky, M. Ball, L. Kiffer, and B. Penkovsky, "Towards optical proof of work," *Cryptoecon. Syst.*, vol. 11, 2020. [Online]. Available: https://assets.pubpub.org/xi9h9rps/01581688887859.pdf

[7] C. Chenli, B. Li, Y. Shi, and T. Jung, "Energy-recycling blockchain with proof-of-deep-learning," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 19–23.

[8] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 104–121.

[9] *Crypto Letter to EPA*. Accessed: May 8, 2022. [Online]. Available: https://web.archive.org/web/20220508191606/https://www.ewg.org/sites/default/files/2022-04/Crypto%20letter%20to%20EPA.pdf

[10] *Bitcoin Letter to the Environmental Protection Agency*. Accessed: May 8, 2022. [Online]. Available: https://web.archive.org/web/20220504230929/https://bitcoinminingcouncil.com/wp-content/uploads/2022/05/Bitcoin_Letter_to_the_Environmental_Protection_Agency.pdf

[11] A. de Vries and C. Stoll, "Bitcoin's growing e-waste problem," *Resour., Conservation Recycling*, vol. 175, Dec. 2021, Art. no. 105901.

[12] A. de Vries, U. Gallersdörfer, L. Klaaßen, and C. Stoll, "Revisiting Bitcoin's carbon footprint," *Joule*, vol. 6, no. 3, pp. 498–502, 2022.

[13] *U.S. Energy Facts Explained—Consumption and Production—U.S. Energy Information Administration (EIA)*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220530223952/https://www.eia.gov/energyexplained/us-energy-facts/

[14] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, "Towards a green blockchain: A review of consensus mechanisms and their energy consumption," in *Proc. 17th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Jul. 2021, pp. 503–511.

[15] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[16] N. S. Kardashev, "Transmission of information by extraterrestrial civilizations," *Sov. Astron.*, vol. 8, p. 217, Oct. 1964.
[17] F. Z. D. N. Costa and R. J. G. B. de Queiroz, "A blockchain using proof-of-download," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 170–177.
[18] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, Apr. 2019, pp. 119–124.
[19] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun.; IEEE 15th Int. Conf. Smart City; IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473.
[20] *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Nov. 4, 2021. [Online]. Available: https://web.archive.org/web/20211103223918/https://bitcoin.org/bitcoin.pdf
[21] J. Heusser. (2013). *Sat Solving—An Alternative to Brute Force Bitcoin Mining*. [Online]. Available: https://web.archive.org/web/20220111172035/https://jheusser.github.io/2013/02/03/satcoin.html
[22] N. Manthey and J. Heusser, "SATcoin—Bitcoin mining via SAT," in *Proc. SAT COMPETITION*, 2018, p. 67.
[23] *Bitcoin Mining on Track to Consume All of the World's Energy by 2020 | Newsweek*. Accessed: Apr. 27, 2022. [Online]. Available: https://web.archive.org/web/20220416205334/https://www.newsweek.com/bitcoin-mining-track-consume-worlds-energy-2020-744036
[24] C. Mora, R. L. Rollins, K. Taladay, M. B. Kantar, M. K. Chock, M. Shimada, and E. C. Franklin, "Bitcoin emissions alone could push global warming above 2 °C," *Nature Climate Change*, vol. 8, no. 11, pp. 931–933, 2018.
[25] N. Houy, "Rational mining limits Bitcoin emissions," *Nature Climate Change*, vol. 9, no. 9, p. 655, 2019.
[26] E. Masanet, A. Shehabi, N. Lei, H. Vranken, J. Koomey, and J. Malmodin, "Implausible projections overestimate near-term Bitcoin CO_2 emissions," *Nature Climate Change*, vol. 9, no. 9, pp. 653–654, Sep. 2019.
[27] L. Dittmar and A. Praktiknjo, "Could Bitcoin emissions push global warming above 2 °C?" *Nature Climate Change*, vol. 9, no. 9, pp. 656–657, Sep. 2019.
[28] A. de Vries, "Bitcoin's growing energy problem," *Joule*, vol. 2, no. 5, pp. 801–805, May 2018.
[29] Wikipedia Contributors. (2022). *Kardashev Scale—Wikipedia, the Free Encyclopedia*. Accessed: May 16, 2022. [Online]. Available: https://web.archive.org/web/20220516222019/https://en.wikipedia.org/w/index.php?title=Kardashev_scale&oldid=1087802566#Current_status_of_human_civilization
[30] *Bitcoin Energy Per Transaction Metric is Misleading—Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220429052319/https://bitcoinmagazine.com/business/bitcoin-energy-per-transaction-metric-is-misleading
[31] *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20210504080905/https://cbeci.org/faq/
[32] *Bitcoin Average Energy Consumption Per Transaction Compared to That of Visa as of April 25, 2022 (in Kilowatt-Hours) | Statista*. Accessed: Apr. 28, 2022. [Online]. Available: https://web.archive.org/web/20220428200955/https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/
[33] *Ethereum Average Energy Consumption Per Transaction Compared to That of Visa as of January 10, 2022 (in Kilowatt-Hours) | Statista*. Accessed: Apr. 28, 2022. [Online]. Available: https://web.archive.org/web/20220428201539/https://www.statista.com/statistics/1265891/ethereum-energy-consumption-transaction-comparison-visa/
[34] *Facebook Electricity Usage Globally 2019 | Statista*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20210818230043/https://www.statista.com/statistics/580087/energy-use-of-facebook/
[35] *Alphabet (Google): Energy Consumption 2019 | Statista*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20211029095928/https://www.statista.com/statistics/788540/energy-consumption-of-google/
[36] C. Stoll, L. Klaaßen, and U. Gallersdörfer, "The carbon footprint of bitcoin," *Joule*, vol. 3, no. 7, pp. 1647–1661, 2019.
[37] *The Soviet Weapons Program—The Tsar Bomba*. Accessed: May 23, 2022. [Online]. Available: https://web.archive.org/web/20220523140227/http://www.nuclearweaponarchive.org/Russia/TsarBomba.html
[38] Wikipedia Contributors. (2022). *Tsar Bomba—Wikipedia, the Free Encyclopedia*. Accessed: May 23, 2022. [Online]. Available: https://web.archive.org/web/20220523155143/https://en.wikipedia.org/w/index.php?title=Tsar_Bomba&oldid=1085809420
[39] N. Mills and E. Mills, "Taming the energy use of gaming computers," *Energy Efficiency*, vol. 9, no. 2, pp. 321–338, Apr. 2016.
[40] *Statistics Finland—Energy Supply and Consumption*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20210414035155/https://www.stat.fi/til/ehk/2019/ehk_2019_2020-12-21_tie_001_en.html
[41] *Ethereum Energy Consumption Index—Digiconomist*. Accessed: Apr. 21, 2022. [Online]. Available: https://web.archive.org/web/20220421133343/https://digiconomist.net/ethereum-energy-consumption
[42] *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20211108150128/https://docsend.com/view/adwmdeeyfvqwecj2
[43] *Final Consumption of Energy—Motiva*. Accessed: Oct. 26, 2021. [Online]. Available: https://web.archive.org/web/20211026171442/https://www.motiva.fi/en/solutions/energy_use_in_finland/final_consumption_of_energy
[44] M. G. Millis, "Energy, incessant obsolescence, and the first interstellar missions," 2011, *arXiv:1101.1066*.
[45] *Interstellar Travel Not Possible Before 2200ad, Suggests Study | MIT Technology Review*. Accessed: May 22, 2022. [Online]. Available: https://web.archive.org/web/20220522162743/https://www.technologyreview.com/2011/01/07/197702/interstellar-travel-not-possible-before-2200ad-suggests-study/
[46] *Statistical Review of World Energy—2021 | 70th Edition*. Accessed: May 23, 2022. [Online]. Available: https://web.archive.org/web/20220523121939/https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2021-full-report.pdf
[47] *Bitcoin's Energy Usage isn't a Problem. Here's Why*. Accessed: Nov. 8, 2021. [Online]. Available: https://web.archive.org/web/20211103232331/https://www.lynalden.com/bitcoin-energy/
[48] *Carbon Dioxide Emissions—Motiva*. Accessed: Oct. 26, 2021. [Online]. Available: https://web.archive.org/web/20201030003703/https://www.motiva.fi/en/solutions/energy_use_in_finland/carbon_dioxide_emissions
[49] *9,000 Transactions Per Second: Bitcoin SV Hits New Record*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20211218070345/https://www.prnewswire.com/news-releases/9-000-transactions-per-second-bitcoin-sv-hits-new-record-301217145.html
[50] *Why Some Bitcoin Devs Say Lasers Can Cut Mining's Energy Costs*. Accessed: Apr. 25, 2022. [Online]. Available: https://web.archive.org/web/20220412181134/https://www.coindesk.com/layer2/miningweek/2022/03/22/why-some-bitcoin-devs-say-lasers-can-cut-minings-energy-costs/
[51] *Returned 'Proof-of-Work' Ban in EU Crypto Markets Bill Fails in Committee | the Block*. Accessed: Apr. 25, 2022. [Online]. Available: https://web.archive.org/web/20220315224829/https://www.theblockcrypto.com/linked/137690/returned-proof-of-work-ban-in-eu-crypto-markets-bill-fails-in-committee
[52] A. Y. Hoekstra and A. K. Chapagain, "Water footprints of nations: Water use by people as a function of their consumption pattern," in *Integrated Assessment of Water Resources and Global Change*. Dordrecht, The Netherlands: Springer, 2006, pp. 35–48. [Online]. Available: https://waterfootprint.org/media/downloads/Hoekstra_and_Chapagain_2007.pdf and https://link.springer.com/chapter/10.1007/978-1-4020-5591-1_3, doi: 10.1007/978-1-4020-5591-1_3.
[53] *Volunteer Computing—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220603163710/https://en.wikipedia.org/wiki/Volunteer_computing
[54] *Folding@home—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220603161605/https://en.wikipedia.org/wiki/Folding@home
[55] E. D. Williams, "Environmental impacts of microchip manufacture," *Thin Solid Films*, vol. 461, no. 1, pp. 2–6, Aug. 2004.

[56] V. Buterin. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: May 30, 2022. [Online]. Available: https://web.archive.org/web/20220529222621/https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
[57] M. B. Taylor, "Bitcoin and the age of bespoke silicon," in *Proc. Int. Conf. Compil., Archit. Synth. Embedded Syst. (CASES)*, Sep. 2013, pp. 1–10.
[58] A. de Vries, "Renewable energy will not solve Bitcoin's sustainability problem," *Joule*, vol. 3, no. 4, pp. 893–898, Apr. 2019.
[59] *PPCoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake*. Accessed: Jun. 3, 2022. [Online]. Available: https://web.archive.org/web/20220603155906/https://www.peercoin.net/papers/peercoin-paper.pdf
[60] *Proof of Stake Versus Proof of Work—White Paper*. Accessed: Jun. 2, 2022. [Online]. Available: https://web.archive.org/web/20220423164140/https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf
[61] *Why Ethereum is Switching to Proof of Stake and How it Will Work | MIT Technology Review*. Accessed: Apr. 21, 2022. [Online]. Available: https://web.archive.org/web/20220421132111/https://12ft.io/proxy?ref=&q=https%3A%2F%2Fwww.technologyreview.com%2F2022%2F03%2F04%2F1046636%2Fethereum-blockchain-proof-of-stake%2F
[62] *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220530113520/https://lightning.network/lightning-network-paper.pdf
[63] A. A. Sawchuk and T. C. Strand, "Digital optical computing," *Proc. IEEE*, vol. 72, no. 7, pp. 758–779, Jul. 1984.
[64] *Bips/Bip-0052.Mediawiki at Master*. Accessed: Apr. 25, 2022. [Online]. Available: https://web.archive.org/web/20220412200428/https://github.com/bitcoin/bips/blob/master/bip-0052.mediawiki
[65] *A Radical Computer Learns to Think in Reverse—The New York Times*. Accessed: May 28, 2022. [Online]. Available: https://web.archive.org/web/20220525233044/https://www.nytimes.com/1999/06/15/science/a-radical-computer-learns-to-think-in-reverse.html
[66] *Reversible Computing: The Only Future for General Digital Computing*. Accessed: Oct. 1, 2021. [Online]. Available: https://web.archive.org/web/20210401031527/https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/LPS21-talk-v5.pdf
[67] M. P. Frank, *Nanocomputer Systems Engineering*. Boca Raton, FL, USA: CRC Press, 2006.
[68] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM J. Res. Develop.*, vol. 5, no. 3, pp. 183–191, Jul. 1961.
[69] T. G. Lewis, "Art Scott and Michael Frank on energy-efficient computing," *Ubiquity*, vol. 2017, pp. 1–17, Sep. 2017.
[70] H. Thapliyal and M. Zwolinski, "Reversible logic to cryptographic hardware: A new paradigm," in *Proc. 49th IEEE Int. Midwest Symp. Circuits Syst.*, vol. 1, Aug. 2006, pp. 342–346.
[71] H. T. Heinonen and A. Semenov, "Recycling hashes from reversible Bitcoin mining to seed pseudorandom number generators," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, Feb. 2022, pp. 103–117. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-96527-3_7, doi: 10.1007/978-3-030-96527-3_7.
[72] J. Connelly, C. Patel, A. Chavez, and P. Nico, "Ternary computing testbed: 3-trit computer architecture," Dept. Comput. Eng., California Polytech. State Univ., San Luis Obispo, CA, USA, 2008. [Online]. Available: http://xyzzy.freeshell.org/trinary/CPE%20Report%20-%20Ternary%20Computing%20Testbed%20-%20RC6a.pdf
[73] *Ternary Systems | IOTA Beginners Guide*. Accessed: May 13, 2022. [Online]. Available: https://web.archive.org/web/20220513200417/https://iota-beginners-guide.com/future-of-iota/iota-x-0-ternary-vision-abandoned/ternary-systems/
[74] A. Srivastava and K. Venkatapathy, "Design and implementation of a low power ternary full adder," *VLSI Des.*, vol. 4, no. 1, pp. 75–81, 1996.
[75] A. P. Dhande and V. T. Ingole, "Design and implementation of 2 bit ternary ALU slice," in *Proc. 3rd Int. Conf., Sci. Electron., Technol. Inf. Telecommun. (SETIT)*, Tunisia, North Africa, vol. 17, Mar. 2005. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/ 34671762/312-with-cover-page-v2.pdf?Expires=1657829511&Signature=ISnvixrH1~BUd9XfmciBZumncM8AYGKqWFX7tG~aENJ221fA7jcsg6npCq9aGXJhqlbNpuH~qa~Bm81-iM4v1XaNIy3SN0xjNiiD-Z8C387pifQdiSggF8y6DdR16i6RGMvjwX1-NDgB7oGCWfnmaIW-ZfD-i8wbSWmFz76FqNQkzHrUXT2R-50nqdZkoVFgT3ZensAANas4HCRjk9pcaxN0y6q0KSHEmTJW6TLlofcoT8FLQk0XJFq7k6ct4yisNm53bilM4WM2mAuxnmCIwe~YTryEO65iIJh4PqAP-d5MIyEq3Q0SVc2kvmiwDjTVADinUgq3tQyCLYPjgzoSwQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
[76] P. C. Balla and A. Antoniou, "Low power dissipation MOS ternary logic family," *IEEE J. Solid-State Circuits*, vol. SSC-19, no. 5, pp. 739–749, Oct. 1984.
[77] D. Porat, "Three-valued digital systems," *Proc. Inst. Electr. Eng.*, vol. 116, no. 6, pp. 947–954, 1969.
[78] K. C. Smith, "The prospects for multivalued logic: A technology and applications view," *IEEE Trans. Comput.*, vol. C-30, no. 9, pp. 619–634, Sep. 1981.
[79] PH. D. Chung-Yu Wu and H.-Y. Huang, "Design and application of pipelined dynamic CMOS ternary logic and simple ternary differential logic," *IEEE J. Solid-State Circuits*, vol. 28, no. 8, pp. 895–906, Aug. 1993.
[80] *Douglas W. Jones on Ternary Computing*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220121012304/http://homepage.divms.uiowa.edu/~jones/ternary/
[81] B. Cambou, P. Flikkema, J. Palmer, D. Telesca, and C. Philabaum, "Can ternary computing improve information assurance?" *Cryptography*, vol. 2, no. 1, p. 6, Mar. 2018.
[82] S. Caraiman and V. Manta, "Image representation and processing using ternary quantum computing," in *Proc. Int. Conf. Adapt. Natural Comput. Algorithms*. Berlin, Germany: Springer, 2013, pp. 366–375. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-37213-1_38, doi: 10.1007/978-3-642-37213-1_38.
[83] *IOTA Token | IOTA Beginners Guide*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220513200502/https://iota-beginners-guide.com/iota-token/
[84] L. Johnson, A. Isam, N. Gogerty, and J. Zitoli. (Dec. 11, 2015). *Connecting the Blockchain to the Sun to Save the Planet*. [Online]. Available: https://ssrn.com/abstract=2702639, doi: 10.2139/ssrn.2702639.
[85] *What's Proof of Elapsed Time. Proof of Elapsed Time is One More | by Henrique Centieiro | Nerd for Tech | Medium*. Accessed: May 31, 2022. [Online]. Available: https://web.archive.org/web/20220531150855/https://medium.com/nerd-for-tech/whats-proof-of-elapsed-time-4f67cf3f45b3
[86] *Floating the Sawtooth Raft: Implementing a Consensus Algorithm in Rust—Hyperledger Foundation*. Accessed: May 31, 2022. [Online]. Available: https://web.archive.org/web/20220531152518/https://www.hyperledger.org/blog/2019/01/11/floating-the-sawtooth-raft-implementing-a-consensus-algorithm-in-rust
[87] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
[88] *Proof of Elapsed Time (PoET) Definition*. Accessed: May 31, 2022. [Online]. Available: https://web.archive.org/web/20220531151229/https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp
[89] D. Minniti, F. Capponi, A. Valcarce, and J. Gallardo, "A new search for Dyson spheres in the Milky Way," in *Life in the Universe*. Dordrecht, The Netherlands: Springer, 2004, pp. 173–176. [Online]. Available: https://link.springer.com/chapter/10.1007/978-94-007-1003-0_36, doi: 10.1007/978-94-007-1003-0_36.
[90] R. Pelc and R. M. Fujita, "Renewable energy from the ocean," *Mar. Policy*, vol. 26, no. 6, pp. 471–479, 2002.
[91] *Ocean Thermal Energy Conversion: An Extensive, Environmentally Benign Source of Energy for the Future*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20040805102014/http://www.sustdev.org/energy/articles/energy/edition3/SDI3-10.pdf
[92] *Bitcoin Unlocks Ocean Energy—Bitcoin Magazine*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220601050830/https://bitcoinmagazine.com/business/bitcoin-unlocks-ocean-energy
[93] *Compact Fusion | Lockheed Martin*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220526074314/https://www.lockheedmartin.com/en-us/products/compact-fusion.html
[94] T. Clynes, "5 big ideas for fusion power: Startups, universities, and major companies are vying to commercialize a nuclear fusion reactor," *IEEE Spectr.*, vol. 57, no. 2, pp. 30–37, Feb. 2020.
[95] *Antminer S19 Pro—The Future of Mining*. Accessed: Sep. 6, 2021. [Online]. Available: https://web.archive.org/web/20210906102302/https://shop.bitmain.com/release/AntminerS19Pro/overview
[96] A. L. Hicks, T. L. Theis, and M. L. Zellner, "Emergent effects of residential lighting choices: Prospects for energy savings," *J. Ind. Ecol.*, vol. 19, no. 2, pp. 285–295, Apr. 2015.
[97] F. Bizzaro, M. Conti, and M. S. Pini, "Proof of evolution: Leveraging blockchain mining for a cooperative execution of genetic algorithms," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 450–455.

[98] N. Shibata, "Proof-of-search: Combining blockchain consensus formation with solving optimization problems," *IEEE Access*, vol. 7, pp. 172994–173006, 2019.

[99] *Primecoin: Cryptocurrency With Prime Number Proof-of-Work*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220303094529/https://primecoin.io/primecoin-paper.pdf

[100] *Primecoin*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220424043230/https://primecoin.io/

[101] *Gridcoin Blue Paper Section 1: Expected Time to Stake and Net Weight*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220126074036/https://gridcoin.us/assets/docs/grc-bluepaper-section-1.pdf

[102] *Gridcoin White Paper: The Computation Power of a Blockchain Driving Science & Data Analysis Version 1.0.1*. Accessed: May 10, 2022. [Online]. Available: https://web.archive.org/web/20220130073115/https://gridcoin.us/assets/docs/whitepaper.pdf

[103] *White Paper—Curecoin*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503220122/https://curecoin.net/white-paper/

[104] *Folding Coin White Paper V4.0*. Accessed: May 3, 2022. [Online]. Available: https://web.archive.org/web/20210422115555/https://foldingcoin.net/images/Whitepapers/Folding%20Coin%20White%20Paper%20v4.0.pdf

[105] *Frequently Asked Questions | Counterparty*. Accessed: May 30, 2022. [Online]. Available: https://web.archive.org/web/20220525232939/https://counterparty.io/docs/faq/

[106] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX Annu. Tech. Conf. (USENIX ATC)*, 2016, pp. 181–194.

[107] *Merged Mining Specification—Bitcoin Wiki*. Accessed: May 9, 2022. [Online]. Available: https://web.archive.org/web/20171124212153/https://en.bitcoin.it/w/index.php?title=Merged_mining_specification&oldid=58250

[108] A. Judmayer, A. Zamyatin, N. Stifter, A. G. Voyiatzis, and E. Weippl, "Merged mining: Curse or cure?" in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham, Switzerland: Springer, Sep. 2017, pp. 316–333. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-67816-0_18, doi: 10.1007/978-3-319-67816-0_18.

[109] A. Zamyatin, "Merged mining: Analysis of effects and implications," Ph.D. thesis, Dept. Inform., Vienna Univ. Technol., Vienna, Austria, 2016. [Online]. Available: https://sec.cs.univie.ac.at/fileadmin/user_upload/i_sec/docs/teaching/thesis/azamyatin_merged_mining.pdf

[110] H. T. Heinonen, "On creation of a stablecoin based on the Morini's scheme of Inv&Sav wallets and antimoney," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 409–416.

[111] D. Stosic, D. Stosic, T. B. Ludermir, and T. Stosic, "Collective behavior of cryptocurrency price changes," *Phys. A, Stat. Mech. Appl.*, vol. 507, pp. 499–509, Oct. 2018.

[112] H. T. Heinonen, A. Semenov, and V. Boginski, "Collective behavior of price changes of ERC-20 tokens," in *Proc. Int. Conf. Comput. Data Social Netw.* Cham, Switzerland: Springer, Jan. 2021, pp. 487–498. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-66046-8_40, doi: 10.1007/978-3-030-66046-8_40.

[113] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM J. Comput.*, vol. 15, no. 2, pp. 364–383, 1986.

[114] J. Kelsey, B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator," in *Proc. Int. Workshop Sel. Areas Cryptogr.* Berlin, Germany: Springer, Jul. 2001, pp. 13–33. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-46513-8_2, doi: 10.1007/3-540-46513-8_2.

[115] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*. Hoboken, NJ, USA: Wiley, 2011.

[116] *Quantum Random Number Generator | QuintessenceLabs*. Accessed: May 17, 2022. [Online]. Available: https://web.archive.org/web/20220516223748/https://www.quintessencelabs.com/products/qstream-quantum-true-random-number-generator/

[117] L. C. Noll, R. G. Mende, and S. Sisodiya, "Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system," U.S. Patent 5 732 138, Mar. 24, 1998.

[118] *Comparison of Hardware Random Number Generators—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20180812092012/https://en.wikipedia.org/wiki/Comparison_of_hardware_random_number_generators

[119] *Hardware Random Number Generator—Wikipedia*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220607150642/https://en.wikipedia.org/w/index.php?title=Hardware_random_number_generator&oldid=1088716271

[120] M. Baker, "DNA data storage breaks records," Aug. 2012. [Online]. Available: https://www.nature.com/articles/nature.2012.11194.pdf?origin=ppub

[121] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *Proc. Int. Conf. Theory Appl. Satisfiability Test.* Berlin, Germany: Springer, 2009, pp. 244–257. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-02777-2_24, doi: 10.1007/978-3-642-02777-2_24.

[122] I. Mironov and L. Zhang, "Applications of SAT solvers to cryptanalysis of hash functions," in *Proc. Int. Conf. Theory Appl. Satisfiability Test.* Berlin, Germany: Springer, 2006, pp. 102–115. [Online]. Available: https://link.springer.com/chapter/10.1007/11814948_13, doi: 10.1007/11814948_13.

[123] F. Massacci, "Using Walk-SAT and Rel-SAT for cryptographic key search," in *Proc. IJCAI*, vol. 99, 1999, pp. 290–295.

[124] B. W. Bloom, "SAT solver attacks on CubeHash," Dept. Comput. Sci., Rochester Inst. Technol., Rochester, NY, USA, Tech. Rep., Apr. 2010. [Online]. Available: https://www2.cs.sfu.ca/~mitchell/cmpt-827/2011-Fall/Project-Readings/CubeHashAttackViaSAT.pdf

[125] *The Chia Network Blockchain*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220401140759/https://www.chia.net/assets/ChiaGreenPaper.pdf

[126] *Chia Business Whitepaper*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220502153433/https://www.chia.net/assets/Chia-Business-Whitepaper-2022-02-02-v2.0.pdf

[127] *FAQ—Chia Network*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502153406/https://www.chia.net/faq/

[128] *What is Chia (XCH)? How to Farm it With a Hard Drive—Decrypt*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502191327/https://decrypt.co/resources/what-is-chia-how-to-farm-with-a-hard-drive

[129] *'Green' Bitcoin Alternative Chia is Leading to Hard Disc Shortages | New Scientist*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502195513/https://www.newscientist.com/article/2277076-green-bitcoin-alternative-chia-is-leading-to-hard-disc-shortages/

[130] *Chia Farming Already Causing SSDs to Fail at Scale, Storage Device Shortages on the Horizon | TechPowerUp*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502185841/https://www.techpowerup.com/281979/chia-farming-already-causing-ssds-to-fail-at-scale-storage-device-shortages-on-the-horizon

[131] B. Fisch, "Tight proofs of space and replication," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, Apr. 2019, pp. 324–348. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-17656-3_12, doi: 10.1007/978-3-030-17656-3_12.

[132] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 475–490.

[133] J. Benet, D. Dalrymple, and N. Greco, "Proof of replication," *Protocol Labs*, vol. 27, p. 20, Jul. 2017.

[134] *Power Fault Tolerance—Technical Report (WIP) | Protocol Labs*. Accessed: May 29, 2022. [Online]. Available: https://web.archive.org/web/20220528215413/https://research.filecoin.io/assets/power-fault-tolerance.pdf

[135] *Sia: Simple Decentralized Storage*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220529211009/https://sia.tech/sia.pdf

[136] *How Decentralized Storage Works*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220601135450/https://www.storj.io/how-it-works

[137] *Safe Network—How it Works*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220510030202/https://safenetwork.tech/how-it-works/

[138] *Safe Network—Frequently Asked Questions*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220510030202/https://safenetwork.tech/faq/

[139] *MaidSafeCoin Price Today, MAID to USD Live, MarketCap and Chart | CoinMarketCap*. Accessed: Jun. 7, 2022. [Online]. Available: https://web.archive.org/web/20220602052227/https://coinmarketcap.com/currencies/maidsafecoin/
[140] *Let's Talk About MultiAlgo + MultiShield | by Josiah Spackman | Medium*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20210123181006/https://josiah-digibyte.medium.com/lets-talk-about-multialgo-multishield-45e6a375a7a
[141] *QuarkCoin: Noble Intentions, Wrong Approach—Bitcoin Magazine*. Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20220531220104/https://bitcoinmagazine.com/business/quarkcoin-noble-intentions-wrong-approach-1387343686
[142] *X11 Algorithm—ASIC Miners, Coins, Pool—BitcoinWiki*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20220606202510/https://en.bitcoinwiki.org/index.php?title=X11&oldid=383584
[143] *SP×36—Spondoolies*. Accessed: Jun. 6, 2022. [Online]. Available: https://web.archive.org/web/20210904095926/https://www.spondoolies-tech.com/products/spx36?variant=12551612104776
[144] *Digibyte Community Infopaper V1.0*. Accessed: May 2, 2022. [Online]. Available: https://web.archive.org/web/20220502154737/https://digibyte.org/docs/infopaper.pdf
[145] *Quarkcoin vs. Bitcoin | What's the Difference?* Accessed: Jun. 1, 2022. [Online]. Available: https://web.archive.org/web/20140215035604/http://www.quarkcoins.com/bitcoin-vs-quarkcoin.html
[146] H. Y. Yuen, F. Wu, W. Cai, H. C. B. Chan, Q. Yan, and V. C. M. Leung, "Proof-of-play: A novel consensus model for blockchain-based peer-to-peer gaming system," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, 2019, pp. 19–28.
[147] *Motocoin Whitepaper*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503221910/https://motocoin-dev.github.io/motocoin-site/Motocoin.pdf
[148] D. Kraft, "Game channels for trustless off-chain interactions in decentralized virtual worlds," *Ledger*, vol. 1, pp. 84–98, Dec. 2016.
[149] *Motocoin*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503224920/https://motocoin-dev.github.io/motocoin-site/
[150] *HunterCoin | Xaya*. Accessed: May 4, 2022. [Online]. Available: https://web.archive.org/web/20220503224135/https://xaya.io/huntercoin-legacy/
[151] *The Humble Beginnings of Blockchain Gaming—CoinQuora*. Accessed: Jun. 4, 2022. [Online]. Available: https://web.archive.org/web/20220130165557/https://coinquora.com/the-humble-beginnings-of-blockchain-gaming/
[152] *RSK Rootstock Platform—Bitcoin Powered Smart Contracts—White Paper*. Accessed: May 30, 2022. [Online]. Available: https://web.archive.org/web/20220525233107/https://www.rsk.co/Whitepapers/RSK-White-Paper-Updated.pdf

HENRI T. HEINONEN was born in Jyväskylä, Finland, in 1984. He received the Bachelor of Science and Master of Science degrees in physics from the University of Jyväskylä, Finland, in 2006 and 2009, respectively. He has written several research articles on blockchain technologies, run volunteer computing projects like SETI@home and BOINC, since the early 2000s on his home computers, and worked on Bitcoin, since 2013. His research interests include particle physics, blockchains, cryptocurrencies, many-money cryptoeconomies, and unconventional computing.

ALEXANDER SEMENOV received the Ph.D. degree in computer science from the University of Jyväskylä, Jyväskylä, Finland, in 2013.

He worked at the University of Jyväskylä and for multiple startup companies in e-commerce and transportation. He worked as a Visiting Scholar at several universities, including SUNY Buffalo, the University of Memphis, the University of Florida, the University of Central Florida, and the University of Sydney in Australia. He has coauthored over 50 peer-reviewed publications and has been a recipient of multiple research grants. His research interests include network science, efficient algorithms, analysis of large datasets, optimization, and machine learning. He is an Associate Editor of the *Journal of Combinatorial Optimization* and *IET Blockchain* journal.

JARI VEIJALAINEN received the B.Sc. degree in mathematics and the M.Sc. degree in computer science from the University of Helsinki, Finland, in 1978 and 1983, respectively, and the Dr.-Ing. degree from the Technical University of Berlin, Germany, in 1989. He worked at the University of Helsinki, as a Teaching Assistant; at the Technical Research Center of Finland (VTT), as a Senior Research Scientist; and at the University of Jyväskylä, as a Full Professor of data management/software engineering, since 1996. He also worked as a Visiting Scholar in Germany at different research institutions and universities, including Waseda University, Tokyo, Japan. He has published about 150 refereed papers in scientific journals and conference proceedings. He has researched advanced transaction management, mobile computing, and social media analysis, and he has acted as an Editor, among others, of *Very Large Data Bases Journal* and *ACM Wireless Networks*. He is currently an Associate Editor of *Social Network Analysis and Mining* journal.

TIMO HÄMÄLÄINEN (Senior Member, IEEE) received the Ph.D. degree in telecommunication from the University of Jyväskylä, Jyväskylä, Finland, in 2002. In 1997, he joined the University of Jyväskylä, where he is currently a Professor of computer networks. He has more than 25 years of research and teaching experience in computer networks. He has led many external-funded network management-related projects. He has launched and led master's programs with the University of Jyväskylä (SW & Communication Engineering) and teaches network management-related courses. He has more than 200 internationally peer-reviewed publications and supervised 40 Ph.D. dissertations. His research interests include network resource management, the IoT, and networking security.

PV

BITCOIN MINING COULD REVOLUTIONIZE GRID COMPUTING AND UNCONVENTIONAL COMPUTING

by

Henri T. Heinonen and Alexander Semenov 2022

Computer (IEEE Computer Society, ISSN 0018-9162), unpublished

IEEE INSTRUMENTATION & MEASUREMENT SOCIETY

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version XX Month, XXXX.

Digital Object Identifier 10.1109/OJIM.2022.1234567

Bitcoin Mining Could Revolutionize Grid Computing and Unconventional Computing

HENRI T. HEINONEN*, AND ALEXANDER SEMENOV†

[1]University of Jyväskylä, Jyväskylä, 40014 Jyväskylän yliopisto, Finland (e-mail: henri.t.heinonen@student.jyu.fi)
[2]Department of Industrial and Systems Engineering, Herbert Wertheim College of Engineering, University of Florida, FL, USA (e-mail: asemenov@ufl.edu)

CORRESPONDING AUTHOR: Henri T. Heinonen (e-mail: henri.t.heinonen@student.jyu.fi).

This work was supported by the University of Jyväskylä, Finland.

ABSTRACT Volunteer computing became popular during the late 1990s with software like SETI@home. In the early days of bitcoin mining, CPUs and GPUs were used similarly to volunteer computing: spare computing cycles are used to solve a problem (securing a blockchain in the case of cryptocurrency mining). Then came the specialized hardware of ASICs, and using CPUs and GPUs for bitcoin mining was not profitable anymore. We argue that bitcoin mining has revolutionized the development of specialized hardware, and it could continue doing so in the industry of unconventional computing (optical, reversible, quantum). There is also a significant source of unused spare computing cycles in home computers and smartphones that could be used for grid computing purposes with the help of cryptocurrency mining.

INDEX TERMS Bitcoin, Blockchain, Cryptocurrency Mining, Distributed Computing, Ether, Green Technology, Grid Computing, Optical Computing, Reversible Computing, Unconventional Computing, Volunteer Computing.

I. Introduction

A blockchain is a distributed decentralized database that maintains a continuously growing list of records (blocks) linked to each other. A blockchain database is resistant to data modification, and once the block is recorded on the ledger, it cannot be modified. The most popular blockchain applications are the cryptocurrencies such as bitcoin (BTC) and ether (ETH). At the time of writing this article, the market capitalization of bitcoin was 460 billion (10^9) USD, and that of ether was 231 billion USD.

In order to keep nodes in agreement regarding the data state in the blockchain, the nodes implement a consensus mechanism. The popular consensus method requires nodes to solve a complex computational puzzle to add a block to the blockchain (and update the data state). The mechanism is referred to as Proof-of-Work (PoW) and is executed during cryptocurrency mining. Bitcoin mining is generating lots of double SHA256 (”SHA256d”) hashes to secure the Bitcoin blockchain. In practice, the PoW process needs lots of electricity to form a consensus. Although bitcoin mining’s colossal energy consumption is a feature, not a bug, there must be ways to achieve the same level of security with lower energy consumption.

Once a suitable SHA256d hash is found, and the block is added to the Bitcoin blockchain, the miner receives a block reward of 6.25 bitcoins (150 thousand USD). In the case of ether mining, the block reward is two ethers (4 thousand USD). Blocks are mined continuously, and only the first node that finds a suitable hash gets a reward. Thus, the mining process is a form of competition. Could the science world take advantage of this competition?

Initially, bitcoin mining was done on standard Central Processing Units (CPUs). However, due to a race, miners moved to Graphics Processing Units (GPUs), then to Field-Programmable Gate Arrays (FPGAs), and to specialized data centers [1]. Currently, bitcoin mining is done using specialized hardware, Application-Specific Integrated Circuits (ASICs), designed and manufactured solely for one kind of computations. For example, Bitcoin ASICs are only able to do SHA256d hashing. The price of one Bitcoin ASIC

miner is usually several thousand US dollars [2]. Besides that, the leading manufacturer of GPUs, nVidia, has recently started to produce GPUs that are specifically designed for cryptocurrency mining. NVIDIA Cmp Hx [3] can be used to mine many kinds of cryptocurrencies. Usually, ethers are mined using GPUs, and nVidia Cmp specifications say that it can reach up to 86 MH/s (megahashes per second) in ETH mining. High demand for GPUs can be illustrated by the fact that numerous retailers have been restricting sales of high-performance GPUs [4], as miners often buy many GPUs and quickly become sold out.

Evidence that manufacturers are ready to design ASICs and GPUs specifically for cryptocurrency mining suggests that the mining is already driving research in GPUs and other integrated circuits forward. Also, it has been shown that the ether price is significantly positively correlated with the GPU prices [5]. This paper reviews other unconventional computing trends that can be revolutionized by bitcoin mining.

Grid computing is about combining the resources of many, often physically separated, computers to solve a computing task. Unconventional computing is any computing that is not conventional. Conventional computing is usually classical, digital, binary, irreversible, and electrical. A famous modern example of unconventional computing would be quantum computing, and an example of an old method of unconventional computing is analog computing. Some examples of unconventional computing that are not entirely practical just yet are reversible and DNA computing. It is fascinating to think about the connection between bitcoin mining, grid computing, and unconventional computing. Our Research Question is thus: In what ways could bitcoin mining revolutionize grid computing and unconventional computing?

A recent survey [6] listed many technologies which have the potential to make bitcoin mining greener and more justified. The paper discusses grid computing and unconventional computing, categorizes technologies into ”Green”, ”Justification” and ”Both” categories, and lists the following computing categories as unconventional computing: analog, ternary, decimal, reversible, mechanical, DNA, optical, and quantum.

Next, we discuss optical computing, reversible computing, and grid computing from the point of view of cryptocurrency mining.

II. Unconventional Computing: Optical Computing

Using light waves for processing, storage, and communication is an old dream of information technology [7]. A full-scale optical computer has the following components

- optical processor;
- optical data transfer; and
- optical storage.

A project tries to achieve low-energy consuming bitcoin mining with optical and analogical computing chips. The method is called ”Optical Proof-of-Work” (oPoW) [8]. The aim is to change the cost model of the bitcoin mining process from OPEX (operation expenses) to CAPEX (capital expenses) so that bitcoin mining would be profitable in areas with high electricity costs.

The oPoW project has changed the existing Bitcoin PoW algorithm to fit the optical computing platform better. Almost all the previous efforts in modifying PoW algorithms for specialized hardware have been about making the PoW algorithms more ASIC-resistant. ASIC-resistance makes (or keeps) mining profitable with the regular home computing hardware consisting of CPUs and GPUs. The oPoW project engineers claim that engineering an optical PoW is more straightforward than making an ASIC-resistant PoW [8].

III. Unconventional Computing: Reversible Computing

Reversible computing is unconventional computing, and it does not erase information [9]. It is possible to use the outputs of a reversible computing chip to go back to the intermediate states and the input states.

At room temperature of 293.15 kelvins, erasing one bit of information generates about $2.805 \cdot 10^{-21}$ joules of heat [10], which can be calculated from the equation by Landauer [11]

$$E = k_{\mathrm{B}} T \ln(2). \tag{1}$$

In Equation 1, E is the heat dissipated by a logically irreversible gate to its environment, k_{B} is the Boltzmann constant, T is the temperature of the environment in kelvins, and $\ln(2)$ is the natural logarithm of 2.

Reversible computing preserves signal energies and reuses them [12]. On the one hand, the more popular method of unconventional computing - quantum computing - might only give some speedups on a few specialized applications. Conversely, reversible computing might achieve greater energy efficiency and performance for all digital computing applications. Reversible computing could be at least 1000 times as cost-effective as irreversible computing in the 2050s [13].

Hash recycling of bitcoin mining and reversible bitcoin mining are two examples of technologies to justify the mining process and make it greener [14]. The Bitcoin ASIC industry was started with small teams and low budgets but achieved great results [15]. In early 2022, Intel announced its plans for developing ASICs for bitcoin mining [16]–[19]. Next, it would be interesting to see the Bitcoin ASIC developers jump-starting the research and development on reversible bitcoin mining chips as was proposed in the paper [14].

IV. Grid Computing: Gridcoin, Curecoin and Foldingcoin

SETI@home, BOINC, GIMPS, distributed.net, and Folding@home are examples of volunteer computing grids. There are numerous spare computing cycles in desktop computers, laptops, video game consoles, tablets, and smartphones. With the software mentioned above, it is possible to use these spare cycles to solve scientific problems like protein folding.

The advantages of volunteer grid computing include the following:

- It tends to be cheaper than buying the same amount of computing power from a supercomputer.
- An average citizen can participate in doing science with a home computer.
- The electricity usage is not concentrated in one data center, but it is distributed around the world.
- The manufacturing process of a home computer is very wasteful, so donating some spare computing cycles from that computer for a science project justifies the resource consumption.

An iPhone 6 (introduced in 2014) has seven gigaFLOPS of computing power [20]. 2.5 billion smartphones like that would form a computing network of about 17.5 exaFLOPS, and if the computing power is used during recharging the phone's battery (about one hour per day is used for recharging), this would still mean a computing grid of about 0.73 exaFLOPS. For comparison, the world's fastest supercomputer in 2022 can achieve about 1.1 exaFLOPS [21].

V. Conclusion

Our Research Question was: In what ways could bitcoin mining revolutionize grid computing and unconventional computing? Gridcoin, Curecoin, and Foldingcoin are Distributed Computing Grid coins. They are cryptocurrencies that use some volunteer computing applications, like BOINC or Folding@home, during the mining process to solve scientific problems. A vast untapped resource of spare computing power is available in smartphones, laptops, gaming consoles, tablets, and desktop computers. The combined spare computing power of consumer gadgets would easily outplay the computing power of the fastest supercomputers. The Distributed Computing Grid coins have a problem of low market capitalizations [6]. The problem with using useful computational puzzles for cryptocurrency mining is that they should be automatically generated and verified with no trusted parties [22]. Still, we believe these problems are solvable, and bitcoin mining could solve useful scientific puzzles shortly. Bitcoin mining has already revolutionized the GPU and ASIC industries. Next, it could also revolutionize unconventional computing like optical and reversible computing.

REFERENCES

[1] M. B. Taylor, "The evolution of bitcoin hardware," *Computer*, vol. 50, no. 9, pp. 58–66, 2017.

[2] "Bitmain shop." https://web.archive.org/web/20220202103523/https://shop.bitmain.com/. Accessed: 2022-08-15.

[3] "A crypto mining gpu for professionals — nvidia." https://web.archive.org/web/20220731230526/https://www.nvidia.com/en-us/cmp/. Accessed: 2022-08-15.

[4] "Best buy restricts gpu sales to members of its $199 perks program — pcmag uk." https://web.archive.org/web/20220409094451/https://uk.pcmag.com/graphics-cards/138653/best-buy-restricts-gpu-sales-to-members-of-its-199-perks-program. Accessed: 2022-08-15.

[5] L. Wilson, "Gpu prices and cryptocurrency returns," *Applied Finance Letters*, vol. 11, no. 1, pp. 2–8, 2022.

[6] H. T. Heinonen, A. Semenov, J. Veijalainen, and T. Hämäläinen, "A survey on technologies which make bitcoin greener or more justified," *IEEE Access*, vol. 10, pp. 74792–74814, 2022.

[7] A. A. Sawchuk and T. C. Strand, "Digital optical computing," *Proceedings of the IEEE*, vol. 72, no. 7, pp. 758–779, 1984.

[8] M. Dubrovsky, M. Ball, L. Kiffer, and B. Penkovsky, "Towards optical proof of work," *Cryptoeconomic Systems*, vol. 11, 2020.

[9] "A radical computer learns to think in reverse - the new york times." https://web.archive.org/web/20220525233044/https://www.nytimes.com/1999/06/15/science/a-radical-computer-learns-to-think-in-reverse.html. Accessed: 2022-05-28.

[10] T. G. Lewis, "Art scott and michael frank on energy-efficient computing," *Ubiquity*, vol. 2017, no. September, pp. 1–17, 2017.

[11] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM journal of research and development*, vol. 5, no. 3, pp. 183–191, 1961.

[12] "Reversible computing: The only future for general digital computing." https://web.archive.org/web/20210401031527/https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/LPS21-talk-v5.pdf. Accessed: 2021-10-01.

[13] M. P. Frank, *Nanocomputer systems engineering*. CRC Press, 2006.

[14] H. T. Heinonen and A. Semenov, "Recycling hashes from reversible bitcoin mining to seed pseudorandom number generators," in *International Conference on Blockchain*, pp. 103–117, Springer, 2021.

[15] M. B. Taylor, "Bitcoin and the age of bespoke silicon," in *2013 international conference on compilers, architecture and synthesis for embedded systems (CASES)*, pp. 1–10, IEEE, 2013.

[16] "Intel has two generations of bitcoin asic: Bzm1 is built on 7nm, 137 gigahash/sec at 2.5 w — anandtech." https://web.archive.org/web/20220809205605/https://www.anandtech.com/show/17218/intels-next-gen-bitcoin-asic-called-bzm2-built-on-7nm-137-gigahashsec-at-25-w. Accessed: 2022-08-15.

[17] "Ultra-low-voltage energy-efficient bitcoin mining asic from intel (23 feb 2022) — bitcoin forum." https://web.archive.org/web/20220525233005/https://bitcointalk.org/index.php?topic=5382058.msg59069878. Accessed: 2022-08-15.

[18] "2022 ieee international solid-state circuits conference." https://web.archive.org/web/20220219004223/https://submissions.mirasmart.com/ISSCC2022/PDF/ISSCC2022AdvanceProgram.pdf. Accessed: 2022-08-15.

[19] "Intel bonanzamine revealed: Bitcoin asic miner consumes 3600w of power — tweaktown." https://web.archive.org/web/20220318012710/https://www.tweaktown.com/news/84684/intel-bonanzamine-revealed-bitcoin-asic-miner-consumes-3600w-of-power/index.html. Accessed: 2022-08-15.

[20] "Gridcoin white paper: The computation power of a blockchain driving science data analysis version 1.0.1." https://web.archive.org/web/20220130073115/https://gridcoin.us/assets/docs/whitepaper.pdf. Accessed: 2022-05-10.

[21] "June 2022 — top500." https://web.archive.org/web/20220813010646/https://www.top500.org/lists/top500/2022/06/. Accessed: 2022-08-15.

[22] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, pp. 104–121, IEEE, 2015.

HENRI T. HEINONEN was born in Jyväskylä, Finland, in 1984. He got a Bachelor of Science degree in Physics in 2006 and a Master of Science degree in Physics in 2009 from the University of Jyväskylä, Finland. He has written several research articles on blockchain technologies, run volunteer computing projects like SETI@home and BOINC since the early 2000s on his home computers, and worked on Bitcoin since 2013. His research interests include particle physics, blockchains, cryptocurrencies, many-money cryptoeconomies, and unconventional computing.

ALEXANDER SEMENOV received a Ph.D. degree in Computer Science from the University of Jyväskylä, Jyväskylä, Finland, in 2013. His research interests include network science, efficient algorithms, analysis of large datasets, optimization, and machine learning. Dr. Semenov has worked at the University of Jyväskylä and for multiple startup companies in e-commerce and transportation.

Dr. Semenov has co-authored over 50 peer-reviewed publications and has been a recipient of multiple research grants. He has served as a visiting scholar at several universities, including SUNY Buffalo, the University of Memphis, the University of Florida, the University of Central Florida, and the University of Sydney in Australia. Dr. Semenov is an Associate Editor for the Journal of Combinatorial Optimization and IET Blockchain Journal.