SEP 2019 • VOL 1

CRYPTO REVIEW

GOSS INSTITUTE OF RESEARCH MANAGEMENT LIMITED

COLLEGE OF BUSINESS
CITY UNIVERSITY OF HONG KONG

B2 FINTECH SCHOOL

ACADEMIC INSIGHTS

GLOBAL(CRYPTO)-CURRENCIES AND CURRENCY COMPETITION

Pierpaolo Benigno,
Linda Schilling,
Harald Uhlig

INDUSTRIAL INSIGHTS

GOSS Research Management

城大商學院 College of Business

B2 FinTech School

CRYPTO REVIEW

CONTENTS

A MESSAGE FROM THE EDITOR-IN-CHIEF

We are pleased to announce the inaugural issue of Crypto Review.

It began in the winter of 2018, when mainstream opinions voiced the end of cryptocurrency. We believed otherwise. Thanks to nearly one year's effort and contribution from our colleagues, friends, and supporters, Crypto Review is created to bring you cryptocurrency focused, forward looking content with long term impact from both industry and academic perspective.

Austrian School economist and Nobel Laureate Friedrich August von Hayek published "The Denationalization of Money" in 1976, five years after U.S. President Richard Nixon unilaterally ended the international convertibility of the US dollar to gold and replaced the Bretton Woods system with pure fiat monetary regime. In his book, Professor Hayek envisioned a world with competing currencies issued by private businesses, and individuals choose the best ones to use. It is a world of the Separation of Money and State.

Professor Hayek passed away in 1992, too soon to witness his proposal being gradually realized by Cypherpunk programmers, not economists, in the age of Internet. The pursuit of a digital, peer-to-peer, non-sovereign monetary system utilizing cryptography began with David Chaum's "Blind Signatures for Untraceable Payments" in 1983. Many projects in the 1990s, including b-money, Bitgold, and Hashcash, did not result in an actual cryptocurrency but nevertheless tested the essential technical building blocks. Finally, our world was forever changed on January 3rd, 2009, when a mysterious genius called Satoshi Nakamoto combined public-key cryptography, distributed nodes, blockchain structure, and proof-of-work in a functioning way and mined Bitcoin's genesis block.

Ten years later, Bitcoin is currently serving as a borderless, censorship-free, apolitical, digital medium of exchange and store of value for whoever has access to the internet. As of September 2019, the existing supply of Bitcoin has a market capitalization of near 200 billion US dollar. We believe it is still very early, thus create Crypto Review to glimpse into the future.

Cryptocurrency is an interdisciplinary subject that depends on the knowledge of mathematics, computer science, game theory, and economics. It may impose great technological, economic, and political impact to our world. Crypto Review will provide full-spectrum coverage on cryptocurrency to our readers and focus on topics that have potential long-term impact.

In this inaugural issue, we bring you the following six articles:

"Global (Crypto) Currencies and Currency Competition" is authored by scholars associated with Becker Friedman Institute for Economics at The University of Chicago. It theoretically explores the dynamic of currency competition introduced by cryptocurrencies. It derives profound implications on monetary policy and the foreign exchange market.

"Impacts of Consensus Algorithms in Cryptocurrency: A Theoretical Analysis of PoW versus PoS in Ethereum" compares the current Proof-of-Work consensus mechanism with the proposed Proof-of-Stake mechanism. It suggests that neither can dominate. The choice between PoW and PoS is a trade-off and should depends on Ethereum community's preference.

"Swimming with Fishes and Sharks: Beneath the Surface of Queue-based Ethereum Mining Pools" investigates the reward distribution scheme of Ethereum mining pool and finds a vulnerability of the queue-based reward scheme. Its result can be applied to other Proof-of-Work based cryptocurrencies that utilize mining pools to coordinate hash power.

"Making Tokens Governable" provides a practitioner's perspective about reconciling crypto tokens and the regulatory environment. It suggests the positive feedbacks between crypto industry and regulators may lead to a more decentralized regulatory regime in the future.

"Cryptocurrency as Directly Investable Protocol" takes the decentralized crypto ecosystem as a new method of financing projects, such as open source software, that have difficulty in raising fund through the traditional capital market. It also analyzes the benefit vs cost of funding a project through decentralized cryptocurrency.

We also provide an English version of "Conceptual Prototype of Chinese Digital Fiat Currency", which may has served as the guidance for the upcoming central bank digital currency (CBDC). Although many voices in the crypto community do not consider CBDC as real cryptocurrency, we believe serious discussion about this subject is beneficial to the development of crypto industry as it is part of the grand currency competition game.

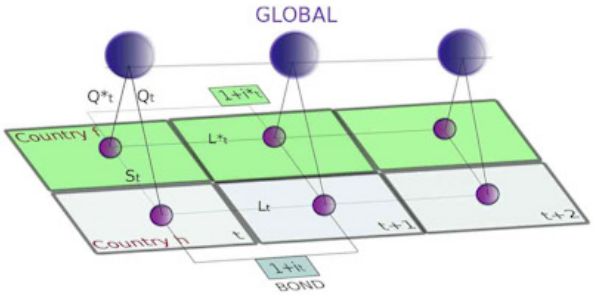
We hope you will find these articles informative and inspiring. We believe cryptocurrency will provide humanity a future with greater liberty and prosperity.

Dr. Zhong Zhang
Editor-in-Chief

Global (Crypto)-Currencies and Currency Competition

Pierpaolo Benigno, LUISS Guido Carli University
Linda Schilling, Ecole Polytechnique CREST
Harald Uhlig, The University of Chicago

At the Jackson Hole conference of August 2019, Mark Carney, the Bank of England governor, has argued that it is time to ween the world off its reliance on the U.S. dollar, and replace it by a new international monetary system instead. He eloquently argued that more thought should be given to creating a global electronic currency that could act as "synthetic hegemonic currency", thus "dampen[ing] the domineering influence of the US dollar on global trade".



Mark Carney: be careful what you wish for! Your wish may be granted: sooner than you think and in a different manner. The rise of cryptocurrencies, starting with Bitcoin, has shown that the introduction and circulation of a global currency no longer requires a central bank: private entities can create them too. While many find fault with the design of Bitcoin and other early entries, competitive pressure has resulted in ever more attractive-looking proposals. The latest attempted entry making a considerable splash is Libra, a cryptocurrency to be issued by a Facebook-led consortium, and it surely will not be the last. We believe that we will soon have one or several well-established and much-liked privately issued global cryptocurrencies. What then are the consequences for national monetary policies? What are the consequences for exchange rates?

These are the questions that we seek to answer in our recent working paper, called "Cryptocurrencies, Currency Competition, and the Impossible Trinity." In that paper, we envision a two-country world, where each country has its own national currency and national central bank, but where there is also a global currency in circulation. We also allow bonds and other financial assets to be traded and assume that capital flows freely. However, money is special, as it is used as a means of payment, and therefore provides additional liquidity services compared to, say, interest-bearing bonds. These services must be equal to the opportunity cost of the foregone nominal interest rate on bond that agents could have held instead of money. We suppose that the global currencies can potentially offer same liquidity services as traditional money in each national market.

What are the consequences of all currencies being incirculation, i.e. the national currencies in their home country, and the global currency in both? We show that this leads to what we call a "crypto-enforced monetary policy synchronization" or CEMPS. This means, that nominal interest rates set by the monetary authorities in the two countries must now be equal, and that the exchange rate between the two national currencies must be a martingale: the expected exchange rate tomorrow is equal to the exchange rate today. The monetary authorities are no longer free to pursue their own monetary policy or to set exchange rates as they please!

This result is reminiscent of the classic "Impossible Trinity" result. According to the "Impossible Trinity", one cannot have free capital flows, fixed exchange rates and independent monetary policy, all at the same time. But things are even tighter here: the exchange rate must be fixed or, at least, a martingale, and monetary policy must be synchronized! The "Impossible Trinity" becomes even less reconcilable.

The logic for this result can be understood most easily without stochastic uncertainty. Consider the nominal return on holding a unit of the home currency, expressed in that currency. That return is zero percent: a Dollar bill today is still a Dollar bill tomorrow. On a nominal bond, one might earn some nominal interest, but not on the home currency. This is the price to pay for its liquidity services. One can now ask, what is the nominal return on holding a unit of the global currency? One unit of the global currency today is one unit of the global currency tomorrow: so, expressed in units of the global currency, the return is zero too. But what is that return, expressed in units of the home currency given that the global currency is purchased today at the global-to-home exchange rate and sold tomorrow at that prevailing

exchange rate? This return is the variation in the exchange rate between today and tomorrow. When both the global and the local currency are used at home, it means that households must be indifferent between either currency. Since the liquidity services provided are (assumed) to be the same, it then must be that the return expressed in the home currency is the same as well. It follows, that the time variation in the exchange rate between the home and the global currency must be zero and therefore their exchange rate constant.

One can go through the same logic in the foreign country. And again, it follows that the exchange rate between the foreign currency and the global currency must be constant. Putting the results together, it then must be the case that the exchange rate between the home and the foreign currency is constant! With a constant exchange rate, one can then show that the nominal interest rates at home and abroad must be the same too. The two monetary policies are synchronized, enforced by that global cryptocurrency.

Are there really no choices for the national monetary policies? Not really. Assume that the global currency is used abroad alongside the foreign currency. The home central bank could then seek a monetary policy, making its own currency more attractive than the global currency, by preventing its adoption at home. Such a monetary policy would require setting the home nominal interest rate below that of the foreign country. While this may sound good at first, troubling implications immediately arise. The home and foreign-country central banks may both seek to free themselves from the shackles imposed by that global currency by racing towards the zero-lower bound. In the end, they will both find themselves there: a situation that has plagued the major central banks throughout the world and that no one seeks to repeat.

What happens if the home country raises the nominal interest rate at home instead, while the global currency is used abroad alongside the foreign currency? In that case, the home currency becomes too expensive to use at home and only the global currency will circulate there. The home central bank effectively abolishes its own raison d'être and might enter unknown territories.

If all this already sounds rather constraining for national central banks, things become even tighter, if that global cryptocurrency is issued by a private consortium against a basket of interest-bearing bonds. This is, essentially, the idea of Libra: anyone can exchange a Libra coin for the underlying bonds and vice versa, thereby fixing the exchange rate of Libra against that bond portfolio. If the consortium does not charge a management fee, its assets and liabilities should grow at the same rate, i.e. the rate of interest on the bond portfolio. This means that Libra coin should appreciate at the same rate of interest. At the end of the day, the consortium is transforming less liquid assets into very liquid money, both with the same return. The first result is that all liquidity premia will be eradicated to zero and the economy satiated in its liquidity needs. The second result is that government money, with zero return, will be completely crowded out by a Libra coin having same liquidity value but paying a positive return. The only way out for national central banks to have their currency circulating at all is to be again stuck at the zero-lower bound.

Presumably, though, the consortium will charge a management fee for the trouble of administering the bond portfolio, so then things relax a bit. But if that management fee is small, this relaxation is small too: the nominal interest rates charged in these two countries are now bound from above by that (small) fee.

Our paper lays out all these arguments in more careful and mathematical detail, including stochastic considerations.

One might wish to argue that such a bond-backed cryptocurrency is just a money market fund in disguise. Can't one also convert a money market fund unit into the underlying bonds and vice versa? Where is the difference, and why has this not yet led to monetary policy synchronization? We view the distinction as a matter of degree. Cryptocurrencies are just that: currencies. Currencies are the tokens used as a medium of exchange, while money market funds still typically need the detour of conversion into the home currency, so they might be less liquid. Moreover, it is hard to find a money market fund, which is widely used on a global scale for transaction purposes. Therefore, money market funds differ in their economic impact from Libra.

Will Mark Carney be happy then? Perhaps. Only time will tell. ■

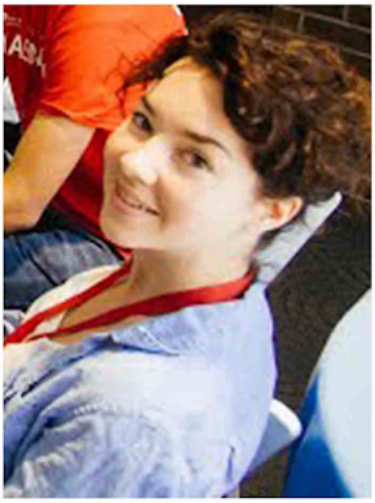
REFERENCES

Benigno, Pierpaolo, Linda Schilling and Harald Uhlig (2019). "Cryptocurrencies, Currency Competition and The Impossible Trinity," CEPR Discussion Paper No. 13943.

Pierpaolo Benigno

Professor of Economics
LUISS Guido Carli University

Dipartimento di Economia e Finanza
LUISS Guido Carli
Viale Romania 32
00197 Rome
ITALY



Linda Schilling

Assistant Professor
for Financial Economics
Ecole Polytechnique CREST

CREST,
5 Avenue Henry Le Chatelier,
91120 Palaiseau,
FRANCE

Harald Uhlig

The Bruce Allen and Barbara Ritzenthaler Professor
in Economics and the College
The University of Chicago

Department of Economics
The University of Chicago
Saieh Hall of Economics #317
5757 South University Avenue
Chicago, IL 60637
USA

SWIMMING WITH FISHES AND SHARKS: BENEATH THE SURFACE OF QUEUE-BASED ETHEREUM MINGING POOLS

A. Zamyatin[*,‡], *K. Wolter*[†], *S. Werner*[‡], *C.E.A. Mulligan*[‡], *P.G. Harrison*[‡] *and W.J. Knottenbelt*[‡]
[*] *SBA Research, Austria,* [†] *Freie Universität Berlin, Germany*
[‡] *Imperial College London, United Kingdom*

Abstract

Cryptocurrency mining can be said to be the modern alchemy, involving as it does the transmutation of electricity into digital gold. The goal of mining is to guess the solution to a cryptographic puzzle, the difficulty of which is determined by the network, and thence to win the block reward and transaction fees. Because the return on solo mining has a very high variance, miners band together to create so-called mining pools. These aggregate the power of several individual miners, and, by distributing the accumulated rewards according to some scheme, ensure a more predictable return for participants.

In this paper we formulate a model of the dynamics of a queue- based reward distribution scheme in a popular Ethereum mining pool and develop a corresponding simulation. We show that the underlying mechanism disadvantages miners with above-average hash rates. We then consider two-miner scenarios and show how large miners may perform attacks to increase their profits at the expense of other participants of the mining pool. The outcomes of our analysis show the queue-based reward scheme is vulnerable to manipulation in its current implementation.

INTRODUCTION

The field of cryptocurrencies has experienced a rapid growth in popularity since the introduction of Bitcoin [19] in 2008. Today, over 750 alternative cryptocurrencies or *altcoins*[1] exist. Ethereum [6] is the most highly capitalised cryptocurrency after Bitcoin. Its primary innovation is a Turing-complete scripting language allowing the creation of programs governing the transfer of value, known as *smart contracts*.

A fundamental data structure underpinning many cryptocurrencies is the *blockchain*. This provides an append-only immutable record of digitally-signed *transactions*. Transactions, each of which represents the transfer of some token of value from source wallets to recipient wallets, are consolidated into *blocks*. Each block is identified by a unique hash over all included transactions and the block header, which contains (amongst other things) the hash of the previous block and a nonce. The fact that the hash of the previous block is referenced in the next block effectively *chains* the blocks together, such that it is impossible to change the contents of a block without also updating every subsequent block.

Participating nodes in a cryptocurrency network communicate in a peer-to-peer fashion using a gossip protocol, broadcasting blocks so that each node stores a complete copy of the blockchain. Since there is no central point of control, a key element of this system is the distributed consensus mechanism used to agree on the content accepted into the blockchain.

In Bitcoin and Ethereum, and most altcoins, the mechanism used is referred to as *Nakamoto consensus* and involves nodes competing to solve a challenging cryptographic puzzle, known as Proof-of-Work (PoW)[2]. The latter is designed such that there exists no better strategy than enumerating all possible candidates, while the verification of a potential solution is trivial. The process of attempting to solve this puzzle is defined as *mining* and the participating nodes are referred to as *miners*. Each attempt at a solution is known as a *hash* and the computational power of a miner is given by its *hash rate*. Miners collect all transactions they receive over the peer-to- peer network and consequently try to generate a new block by brute-forcing the solution to the required PoW puzzle. Each time a miner succeeds in creating a new block, the latter is appended to the public blockchain and propagated through the network. As reward for investing computational effort, the miner is granted a fixed amount of newly generated or minted units of the underlying currency. Furthermore, transactions include a small fee to incentivise the winning miner to include them in the latest block.

In Ethereum, the PoW consists of finding a nonce input to the Ethash [8] algorithm, such that the result is below a certain threshold depending on the *difficulty* [10]. Since

[1] Source: http://coinmarketcap.com. Accessed: 2017-04-11

[2] While other consensus mechanisms, such as Proof-of-Stake [14], [11], are currently being researched and developed, PoW, as of this writing, remains by far the most adopted consensus approach in permissionless blockchains.

miners can leave or join the race for generating the next block at any time, Ethereum implements a mechanism to dynamically adjust the difficulty of the PoW, such that a new block is found on average approximately every fifteen seconds. At the time of writing, the difficulty, i.e. the expected number of hashing operations required to find a solution to the PoW, amounts to approximately 740 trillion hashes [1].

To reduce the variance of the time between finding blocks and hence stabilise revenue over time, miners cooperate to create so-called *mining pools*. The hash rate of such mining pools usually significantly exceeds that of single miners and, as a result, the average interval between finding blocks is reduced.

Taken together with a scheme which ideally distributes block rewards proportionally to the effort invested by miners, this allows each participant to more accurately predict the overall accumulated revenue over time and ensures a steadier payment stream. In return, miners are usually charged a small proportion of their revenue by the pool. To measure the effort invested by miners, the mining pool accepts solutions to a cryptographic puzzle that has a considerably relaxed difficulty threshold; these solutions are known as *shares*.

The schemes used for dividing rewards among miners can differ substantially from pool to pool. Some pools split each mined block into fractions and award each miner the part of the block that corresponds to their mining investment in terms of shares, while other pools rank miners according to the invested work as evidenced by shares and award a mined block always to the top-ranked miner. Previous research work by Rosenfeld provided an overview of such reward schemes [20] and introduced so-called *pool-hopping* attacks, where miners dynamically switch between pools to increase their profit. Lewenberg et al. pointed towards problems in preventing pool-hopping [16], while Schrijvers et al. conducted a study on incentive compatibility of common reward schemes [21]. Further research evaluated potential attack scenarios between pools, including denial-of-service attacks [13], [15] and less direct *withholding attacks* [12], [7], [17], where pools infiltrate competitors and cause damage by withholding valid blocks.

In this paper we focus on a recently-introduced approach for distributing block rewards among miners [4] which we refer to as a *queue-based* reward payout scheme. Under this scheme, the block reward is paid to the miner residing at the first position of a priority queue sorted by credits received for submitted shares over time. We evaluate the expectation and variance of miners' revenues under this scheme, comparing the results to the PPLNS *(Pay-Per-Last-N-Shares)* reward payout scheme. Thereby we aim to show which type of miners, in terms of different hash rates, benefit the most from the queue - based reward payout scheme as opposed to an alternative 'fair' reward scheme. To this end, we introduce a discrete event - based simulation, which allows us to model the ecosystem of a single mining pool including the dynamics of miner behaviour. We make use of data extracted from Ethpool [2], a popular Ethereum mining pool, which was the first to implement the queue-based payout scheme. For comparative purposes we use a conventional PPLNS scheme, as implemented by the Ethermine Ethereum mining pool. Furthermore, we highlight a potential vulnerability rooted in the uneven distribution of credits in the queue-based approach, which can be exploited in several ways by miners with above average hash rates to increase their long-term revenue. A real-world scenario, in which this vulnerability is being exploited to the benefit of a small group of miners, has been observed in Ethpool.

The remainder of this paper is organised as follows. Section II outlines useful background and notation. Section III explains the mechanics of the queue-based reward payout scheme, while Section IV discusses the numerical results obtained from a simulation of this model, highlighting howlarge miners are at a natural disadvantage in such a scheme and comparing the economic benefit of different simulated attack scenarios. Section V introduces three different attack scenarios arising from the nature of the queue - based reward scheme. Section VI concludes and outlines future work.

II. PRELIMINARIES

In this section we will provide an overview of different mining approaches, more specifically solo and pooled mining, as well as explain the structure of miner rewards and the most common conventional reward payout schemes.

A. *Notation*

In the process of mining for a cryptocurrency a miner m_j will perform the necessary hashing operations at rate h_j. Commonly, the hash rate of a miner will range between a few hundred megahashes[3] per second (MH/s), and several gigahashes per second (GH/s). The total hash rate of a group of miners is the sum of the individual hash rates, denoted by *H*. The difficulty *D* indicates the expected number of hashes needed to find the next block. The pool difficulty d indicates the expected number of hashes needed to find a share that is submitted to the pool; such shares enable the mining pool to objectively assess miner hash rate and may also be candidates for a new block.

B. *Miner rewards*

The Ethereum mining protocol differentiates between full and so-called *uncle* blocks. The latter represent valid blocks, which did not become the new head of the blockchain [9]. This occurs if a block submitted by a competing miner is propagated faster to the majority of all nodes in the network. We denote the probability of a block being an uncle, which depends on the miner's network connectivity γ, as p_u.

[3] i.e. 108 hashes

In contrast to Bitcoin, miners receive payouts not only for full, but also for uncle blocks in Etherum. As of this writing, the reward for a full block R_b is 5 ETH[4], while the reward R_u for an uncle block is 3.75 ETH, excluding transaction fees. On the Ethereum public blockchain, as in most other cryptocurrencies, the revenue generated by finding a block consists of the block reward and fees collected from the included transactions. Since the transaction fees are hard to model, while representing only a small share of the total block reward, they are omitted in this paper for simplification. Hence, we denote the expected revenue per block as:

$$R_e = R_b(1 - p_u) + R_u p_u \quad (1)$$

C. *Solo mining*

Miners participating in the consensus finding mechanism on an individual basis, and thereby receiving the entire reward for each found block, are referred to as *solo miners*. The number of blocks found by a solo miner per time unit follows a Poisson distribution with rate parameter $\lambda = h/D$, where D is the current difficulty and h represents the solo miner's hash rate.

The expected revenue per performed hashing operation can be hence formulated as

$$E[R_h] = \frac{R_e}{D} \quad (2)$$

The variance of the revenue per hashing operation is

$$\mathrm{Var}[R_h] = R_e^2 \lambda = \frac{R_e^2}{D} \quad (3)$$

D. *Mining pools*

Mining pools are a way for solo miners to join their resources (mining power) together in order to increase their probability of finding a block. These pools are run by so-called *operators*, whose main task, apart from maintaining the mining software and scripts, is to estimate each participating miner's hash rate and their contribution to the generated blocks. To this end, the mining pool operator sends to each miner a PoW problem, identical to the network PoW puzzle, but with a lower difficulty[5].

Miners participate in the pool by continuously employing computational power in solving the pool's problem. Each time a miner finds a solution, i.e. finds a nonce input to the Ethash algorithm yielding a result below the required threshold, she submits a *share* to the block to be found next by the mining pool. Sometimes, the submitted solution to the mining pool's problem will also be a solution to the more difficult network problem. As a result, the mining pool will generate the next block and collect the block reward. The latter is then distributed among the pool's miners based on each miner's contribution and according to the reward payout scheme.

The time between submitted shares is exponentially distributed with mean d/h_i, where h_i is the hash rate of miner m_i and d is the pool problem difficulty. Each share is the solution to the current network PoW puzzle with probability d/D. The time it takes the mining pool as a block can be modelled as an exponentially distributed random variable with mean D/H, where $H = \sum_{i=1}^{n} h_i$ h_i is the sum of the hash rates of the n individual miners in the pool and D is the network difficulty. The number of blocks found in a specific time period in turn follows a Poisson distribution with rate parameter $\lambda = H/D$.

Shares can be *stale*, i.e. valid but no longer applicable to the current PoW puzzle of the network. In other words, if a miner submits a share for block b_j only after it has been found and the pool is already mining on block b_{j+1}, the share is ignored. The rate of stale shares depends on each miner's network connectivity γ.

E. *Conventional reward payout schemes*

The first mining pools were created around 2011, mostly implementing reward schemes that equally distribute each block reward among all or a subset of miners, based on shares submitted during a specific time period. To compensate their administrative effort, mining pools charge a fee f, which is a small proportion of the revenue. Below, we briefly summarize some well known reward payout schemes, as initially described by Rosenfeld [20].

1) Proportional Payout: In a proportional scheme, also referred to as *Round-based Pay-Per-Share*, miners receive payouts each time the mining pool finds a block, according to their contribution to this block, as measured by the number of valid shares s_i submitted by miner m_i since the last block. Hence, the expected reward per block of a miner m_i is

$$E[R_i] = (1 - f) R_e \frac{s_i}{\sum_{j=1}^{n} s_j} \quad (4)$$

where n is the size of the mining pool. The counted shares of each miner are then reset to zero, as the mining pool starts with computations for the next block.

The number of expected shares per block is

$$E[S] = \frac{D}{d} \quad (5)$$

The expected revenue per hashing operation is the same as in solo mining, decreased by the mining pool's fee f:

$$E[R_h] = \frac{(1 - f) R_e}{D} \quad (6)$$

The variance, however, is lower than in solo mining by approximately a factor $D/(\ln D)$. Thereby, only small miners effectively profit from the reduced variance: for large miners, accounting for significant portions of the mining pool's hash rate, the variance can only be

[4] Ether – abbreviated ETH – is the underlying currency in Ethereum.

[5] If the problem difficulty were equal to the network difficulty, each submitted share would also be generating the next block. Hence, the mining pool operator would know how much work the finder of the block has performed, but would have no information on other miners' contributions.

multiplied by factor h_i/H, representing the miner's portion of the pool's hash rate [20].

2) *Pay-Per-Last-N-Shares (PPLNS)*: The PPLNS payout scheme is a modified version of the proportional scheme, aiming at the prevention of pool hopping. This is achieved by performing the calculation of the reward payout only after the miners have submitted $N > E[S]$ shares in total. Hence, the expected revenue of miner m_i per payout is

$$E[R_i] = (1-f)BR_e\frac{s_i}{N} \tag{7}$$

where B is the number of blocks found by the pool during the last N shares and si the number of shares miner m_i contributed to N.

Due to the proportionality of the reward payouts, miners are incentivised to employ their maximal mining capacity for as long as possible in both of the above schemes.

III. MODELLING THE QUEUE-BASED PAYOUT

This section provides a detailed overview of the queue-based reward payout scheme. We showcase the structure of the scheme, as implemented by Ethpool, as well as point out the workings and problems of the underlying mechanisms for credits accounting.

A. *Structure of reward payouts*

The queue-based reward payout scheme was first implemented by Ethpool in late 2015 and introduces a new way of handling payouts, while relying on a mechanism to account for each miner's contribution similar to that of conventional payout schemes. By submitting valid shares, miners earn so-called *credits*. Each valid share increments the miner's credits by d, the expected number of hashes required to solve the mining pool's PoW problem.

The mining pool maintains a ranking in form of a priority queue, where the priority of each miner is defined by her earned credits. A miner's priority increases with each of her submitted shares. Based on their hash rate and network connectivity, miners race for the top position in the queue. As a result, the ordering of the priority changes dynamically after each submitted share.

Each time the mining pool finds a block, the *complete*[6] reward is allocated to the miner $m_{(1)}$ currently positioned at the top of the queue. Consequently, the winning miner's credits are reset to the difference between her and the second placed miner's credits:

$$c(m_{(1)}) := c(m_{(1)}) - c(m_{(2)}) \tag{8}$$

Uncle blocks are considered differently, in the sense that they do not lead to a re-calculation of the winner's credit balance. Hence, the winner of an uncle block will receive uncle reward R_u and continue to reside on top of the queue, until being overtaken or winning a full block.

While in theory, the possible range of miners' credits is $[0, +\infty)$, Ethpool states each miner is expected to collect approximately D credits, before winning a block [4]. However, due to the special treatment of uncles, the expected amount of credits of the miner at the top of the priority queue is:

$$E[c(m_{(1)})] = (1+p_u)D \tag{9}$$

B. *Discussion of potential problems*

We now move on to highlight two potential problems of the queue-based payout scheme.

TABLE I: Priority queue showing a gap between large and medium/small miners.

(a) Before Block i

Position	Miner	Credits
1	Alice	110
2	Bob	105
3	Eve	60
4	Dave	30

(b) After Block i

Position	Miner	Credits
1	Bob	105
2	Eve	60
3	Dave	30
4	Alice	5

(c) Before Block i+1

Position	Miner	Credits
1	Bob	115
2	Eve	65
3	Dave	35
4	Alice	15

(d) After Block i+1

Position	Miner	Credits
1	Eve	65
2	Bob	50
3	Dave	35
4	Alice	15

1) Unequal variance impacts: As we can see, this scheme only takes into account the credits and hence the work performed by the second placed miner, instead of looking at the amount of shares submitted/credits earned by all miners, for the credit resetting policy. This particularly impacts the revenue of large miners, which account for significant portions of the mining pool's hash rate. Since these miners produce significantly more shares than the average miner, they reach the top of the queue more frequently. Thereby, large miners also end up absorbing more of the mining pool's variance caused by lucky/unlucky streaks[7]. Small miners, on the other hand, reach the top of the queue less frequently. Thus, the probability of a small miner reaching the top at a time when the pool is having an unlucky streak is comparatively low to that of a large miner. As a result, small miners will be earning over-proportional revenue shares with regards to their invested computational effort.

2) *Non-uniform credits redistribution:* In a scenario where two or more miners maintain significantly high hash rates compared to the rest of the miners in the pool, the large miners will be rapidly moving up the queue

[6] Less pool fees.

[7] Given some time interval, pool luck is the ratio of blocks actually mined by a pool to the mathematical expectation of the number of mined blocks.

and overtaking slower miners. Consequently, there is a high probability of at least two large miners being positioned at the top of the queue with far more credits than smaller miners, when the pool finds the next block. Such a scenario is illustrated in Table I. Here the two large miners, Alice and Bob, consistently earn 10 credits per round, while the small miners, Eve and Dave, earn 5.

The calculation of the new credits for the winner of the block, in our case Alice, takes into account only the credits earned by Bob, placed second (cf. Table Ia). Since Bob too collected a high amount of credits, Alice will find herself re-positioned at the end of the queue (cf. Table Ib). In the next round, Bob will win the block reward. However, due to the significant gap between Bob's and Eve's credits, Bob will be re-positioned both in front of Dave and Alice, thus receiving an advantage (cf. Table Id).

We see the redistribution of credits is only fair if the credits difference between each two consecutive miners is constant. However, since real world observations show the logarithm of mining power in Ethpool resembles a Gaussian distribution (cf. Section IV-B), we argue that this is very unlikely to be the case in reality.

IV. SIMULATING THE QUEUE-BASED PAYOUT SCHEME

In this section we present simulation results for our model of the queue-based reward payout scheme and show how large miners are disadvantaged in Ethpool's current implementation. In Subsection IV-A, we provide simulation results for a pool containing only two miners, one with large hash rate and one with small hash rate, while simulation results for a realistic population of miners (as sampled from Ethpool) are given in Subsection IV-B.

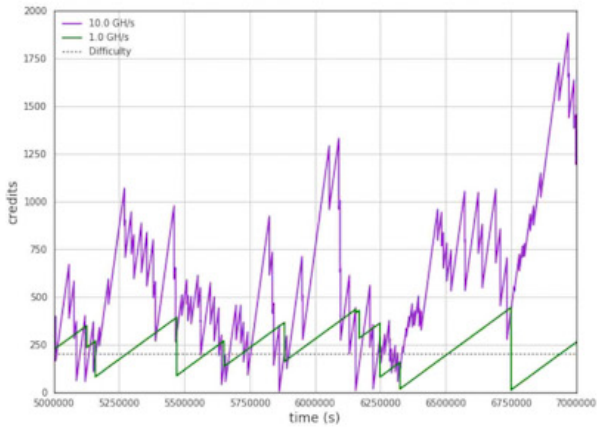


Fig. 1: The evolution of Ethpool credits in a two-miner scenario.

Our event-based simulator constructs the time between shares submitted by miners as a random number[8] following an exponential distribution with rate parameter $\lambda = h/d$. All simulations run for 500 000 blocks and are performed under constant network difficulty D = 200TH (trillion hashes), network connectivity γ = 1 (no uncle blocks), pool problem difficulty d = 3.6b and proportional pool fee f = 0.01. We further assume an uptime of 100% for all miners (with no stale or invalid shares).

A. *Simulating a two-miner pool*

First, we simulate the simple model of a mining pool containing only two miners, one large miner m_l with a hash rate of 10 GH/s and a miner ms with a significantly lower hash rate of 1 GH/s. Although arguably such a scenario will not be observed in reality, we use this set-up to better understand the benefits and disadvantages of large and small miners in the queue-based reward payout scheme.

The development of earned credits is visualised in Figure1. We can see the credits of the small miner $c(m_s)$ lie only slightly above the network difficulty when winning a block. The credits of the 10 GH/s miner $c(m_l)$, on the other hand, by far exceed the credits expected according to the network difficulty and are subject to high variance.

Closer observations of the credits development in Figure 1 show a repeating pattern. The large miner remains on top of the queue with significantly high credits for prolonged periods. However, this trend changes once the small miner has accumulated more credits than the large miner earns between winning two blocks. We can see that the credits of the large miner start to decrease quickly, while those of the small miner continue to grow. At some point, the small miner takes over the lead and wins a block. Consequently, $c(m_s)$ is reset to $c(m_s) - c(m_l)$ and the small miner is overtaken by the large, whose credits then start increasing significantly.

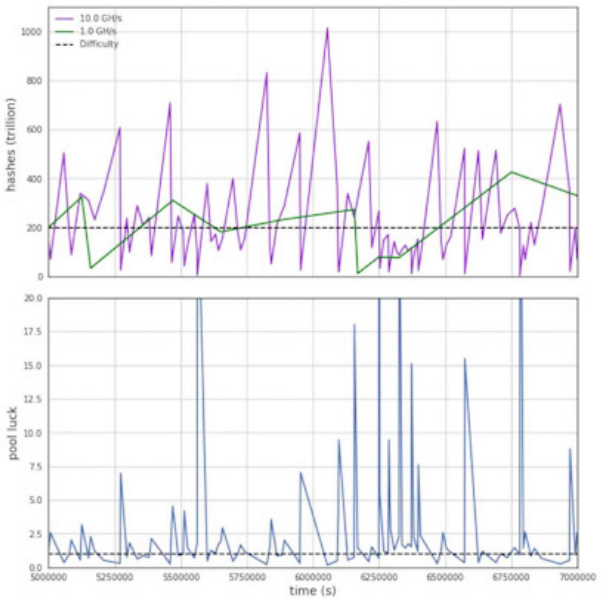


Fig. 2: Performed work per block (top) in comparison to pool luck in the two-miner scenario (bottom). Each peak in pool luck correlates with a drop in required work per block and vice versa.

[8] The generation of random numbers is accomplished by the Mersenne Twister [18] algorithm.

As mentioned in Section II, it has been found in earlier work that miners responsible for significant portions of the total hash rate H of a mining pool can adjust their revenue variance by a maximum factor h_i / H. Hence, the revenue variance of ml can be improved only by 9%, while the small miner profits from a variance reduction of over 90%. This is also evident from the top graph in Figure 2, which shows the development of performed work per block and its correlation with pool luck. As we can see, the variance of performed work is significantly higher for the large miner: 35 872.5 compared to 21 137.0 for the small miner. Furthermore, the large miner on average has to invest more computational effort per block than the small miner: 201.52TH in contrast to 186.82TH, which is surprisingly less than the network difficulty.

These observations are also mirrored in the miner's generated revenues: the small miner received rewards for 3442 blocks more than she mined, as shown in Table II.

TABLE II: Blocks mined and rewarded in the queue-based scheme in the two-miner scenario.

Miner	Blocks			Average performed work (trillion hashes)
	Rewarded	Mined	Ratio	
Large (10 GH/s)	451,316	454,758	0.9924	201.52
Small (1 GH/s)	48,684	45,242	1.0761	186.82

B. *Simulating Ethpool*

Next, we use a large data set of miners as input for our simulation to generate realistic results. In particular, the data set consists of 729 miners extracted from Ethpool's public API [3] in the period between 2017-02-21 and 2017-04-09, accumulating a total hash rate of 699.18GH/s. Figure 3 shows the distribution of hash rates in the extracted data set on a logarithmic scale, which resembles a Gaussian curve.

Figure 4 shows the number of credits necessary to win a block. While it is not clear from visual inspection whether the credits form a stationary random process with normal variation, Figure 5 very clearly illustrates the high autocorrelation in the number of credits necessary to win a block.

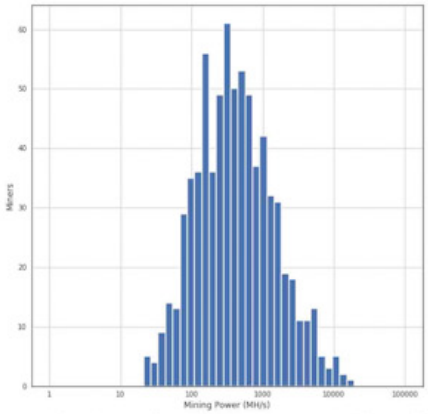


Fig. 3: Distribution of mining power in Ethpool (logarithmic scale). The largest miner controls 18.07 GH/s, the smallest 22 MH/s. The average mining power is approximately 960 MH/s, while the median amounts to 380 MH/s. Standard deviation is 1.74 GH/s.

Figure 6 visualizes the development of performed work for small, medium and large miners in Ethpool. As already seen in the two-miner scenario, the variance of the necessary work per block decreases with the respective miner's hash rate, i.e., miners accounting for significant portions of the overall hash rate are most affected by lucky/unlucky streaks.

Since the list of credits for Ethpool is public the interested miner is advised to study pool luck and the current level of credits when deciding which pool to join. Given the strong autocorrelation, the observed credit levels when the pool wins a block may also serve as a decision criterion whether or not to leave a pool.

Furthermore, the large miners must invest more computational power on average to win a block than small miners, as is evident in Figure 7. While miners with hash rates of more than 10 GH/s perform slightly more work than required by the network difficulty, miners in the 10th percentile of mining power evade approximately 5–7 trillion hashes (2.5–3.5% of total) of work per block. When put in relation to the average computational effort, the relative difference between of the smallest and largest miner amounts to nearly 5%. The results yielded by the simulation of Ethpool confirm the observations made in the two-miner scenario.

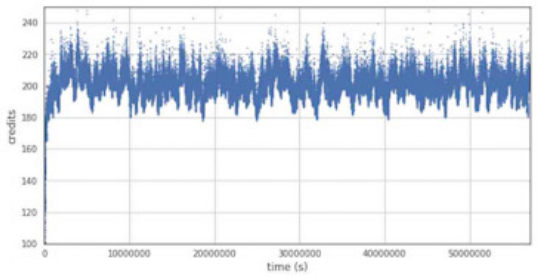


Fig. 4: Development of credits when winning a block in the multi-miner scenario.

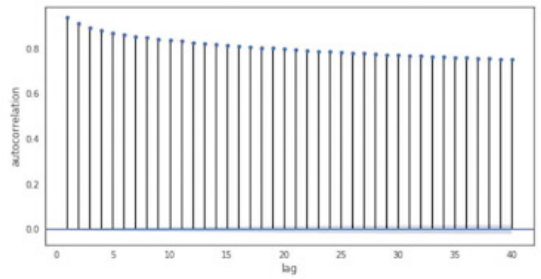


Fig. 5: Autocorrelation of credits when winning a block for lags 1:40.

As in the two-miner scenario, the disadvantage of large miners is reflected in their economic performance, since small miners are rewarded for more blocks than they are entitled to. To better express the deviation of economic output between small and large miners, we compare the performance of miners in the queue-based scheme implemented by Ethpool, to the PPLNS scheme

implemented by Ethermine, where N is equal to the shares submitted in the last 60 minutes [5]. We introduce *return per computed MH* as a performance metric and illustrate our results in Figure 8. It can be seen that there is a clear bias towards small and medium-sized miners with regards to profitability in Ethpool, while large miners have higher return on investment in Ethermine.

Figure 9 sorts the return on invested work by the hash rate and clearly shows that in a queue-based scheme like Ethpool miners with low hash rate receive above average return on investment, while miners with large hash rate are at a disadvantage.

We note that while the numerical difference between Ethpool and Ethermine is very small in this performance metric, the absolute bias scales up quickly over time. For example, a miner with a hash rate of 18.07 GH/s loses 1.406×10^{-10} ETH every million hashes, when choosing Ethpool over Ethermine.

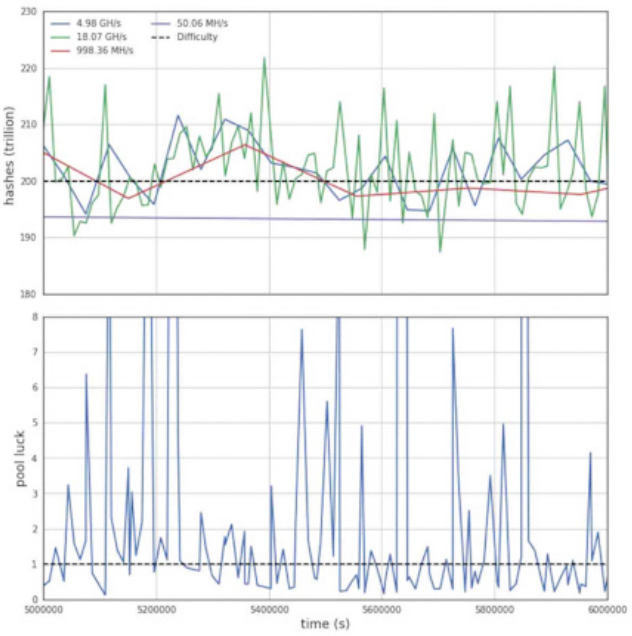


Fig. 6: Performed work per block in comparison to pool luck for small, medium and large miners. The large miner absorbs most of the variance.

Consequently, her loss per day will amount to 0.2187 ETH[9] and approximately 79 ETH per year. We observe that small fish have a happier life in Ethpool than in Ethermine and are better off than the large sharks, at least if the latter do not attack in some way.

A summary of the simulation results with regards to economic performance of miners in Ethpool is provided in Table III. We find that miners with low hash rate benefit considerably from joining a queue-based mining pool. They can reduce the variance in their gained revenue and even receive better return on investment than the average miner. This must come at the expense of miners with large hash rate, who are at disadvantage with respect to both criteria.

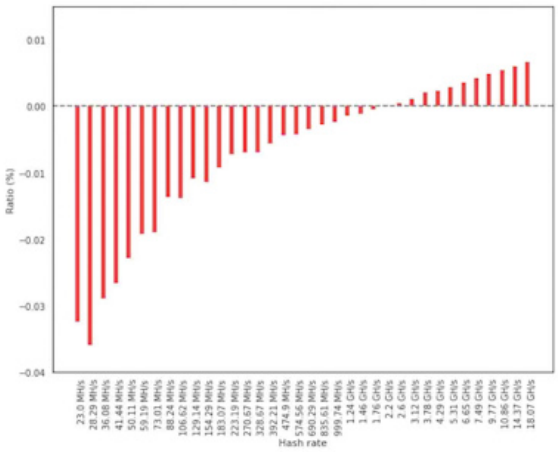


Fig. 7: Ratio of performed work per block by miners in Ethpool, relative to the work performed on average. Miners are grouped according to their hash rate.

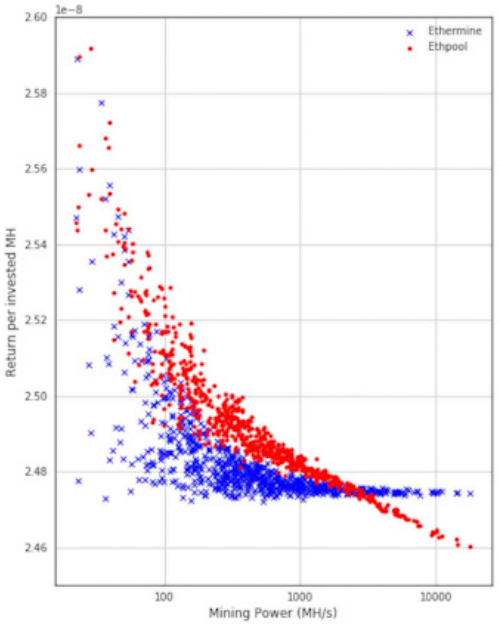


Fig. 8: Return per computed MH in a multi-miner scenario (logarithmic x-axis).

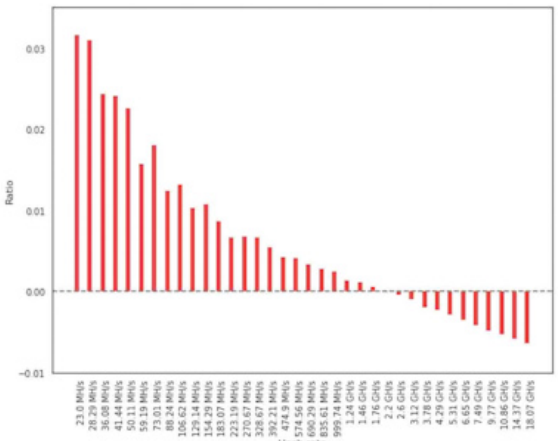


Fig. 9: Ratio of return per computed MH for miners in Ethpool, relative to the average return per computed MH. Miners are grouped according to their hash rate.

[9] At the time of writing this amounts to approximately US$ 78.

TABLE III: Miner performance in the multi-miner scenario.

Hash rate	Miners	Blocks			Average performed work (trillion hashes)	Average revenue per computed MH (10^{-8} ETH)		
		Rewarded	Mined	Ratio		Ethpool	Ethermine	Ratio
23.0 MH/s	5	16	12	1.3387	193.42	2.5540	2.5228	1.0124
29.84 MH/s	4	21	18	1.1944	193.08	2.5475	2.5112	1.0145
42.27 MH/s	15	30	31	0.9640	194.74	2.5338	2.5032	1.0122
57.75 MH/s	21	41	41	0.9965	195.77	2.5217	2.5022	1.0078
78.97 MH/s	33	56	54	1.0309	196.64	2.5140	2.4902	1.0096
107.79 MH/s	48	77	76	1.0148	197.19	2.5073	2.4873	1.0080
152.11 MH/s	75	108	106	1.0211	197.75	2.5011	2.4854	1.0063
203.06 MH/s	44	144	142	1.0169	198.25	2.4952	2.4803	1.0060
284.16 MH/s	78	202	200	1.0096	198.48	2.4927	2.4789	1.0056
384.63 MH/s	74	273	266	1.0258	198.76	2.4896	2.4782	1.0046
538.74 MH/s	73	383	379	1.0095	199.06	2.4861	2.4771	1.0036
729.49 MH/s	54	518	509	1.0186	199.27	2.4837	2.4760	1.0031
988.34 MH/s	55	703	694	1.0127	199.43	2.4818	2.4758	1.0024
1.39 GH/s	48	987	977	1.0107	199.67	2.4788	2.4754	1.0014
1.84 GH/s	24	1 305	1 294	1.0088	199.83	2.4769	2.4751	1.0007
2.54 GH/s	27	1 802	1 779	1.0125	200.01	2.4748	2.4749	1.0000
3.59 GH/s	18	2546	2519	1.0107	200.27	2.4716	2.4747	0.9987
4.99 GH/s	15	3 531	3 483	1.0140	200.46	2.4692	2.4745	0.9979
6.72 GH/s	8	4 744	4 739	1.0010	200.66	2.4668	2.4745	0.9969
9.91 GH/s	6	7 046	7 044	1.0002	200.92	2.4637	2.4745	0.9956
13.47 GH/s	3	9 457	9 436	1.0023	201.07	2.4618	2.4744	0.9949
18.07 GH/s	1	12 844	12 864	0.9984	201.22	2.4602	2.4742	0.9943

C. *Exponential Difficulty*

The presented simulations were conducted under the assumption of a constant difficulty of Ethereum's PoW. However, in practice the difficulty is adjusted after every block and has been observed to increase at a high rate. In fact, between March and June 2017 the difficulty has increased from 200 to 740 trillion hashes, resembling exponential growth at ap- proximate rate $k = 2.726 \times 10^{-6}$.

We simulate both the two-miner and multi-miner scenarios under exponentially increasing PoW difficulty, using an initial difficulty d = 200 trillion hashes and the measured growth rate k. Apart from an expected increase in performed work, the results in the two-miner scenario remain approximately the same as described in Section IV-A. In the multi-miner case, large miners remain disadvantaged, however at a slightly smaller scale. The relative difference between the average computational effort of the smallest and largest miner decreases from to 5% to approximately 3%, while the effects on the return per computed MH are negligible. Detailed simulation results are provided in Appendix VII-A.

V. MODELLING ATTACKS

In observations of the Ethpool mining pool we have noticed behavioural artefacts, such as occasional donations of hashing power by one miner to another or sudden drop of hash rate of a top ranked miner. In this section we want to explore the motivations behind such behaviour. To this end, we extend our model by allowing miners to withhold valid shares, donate their mining power in a tactical manner and maintain multiple wallets in a pool. We further provide simulations for the introduced attacks in a scenario with two miners and discuss their effectiveness in Subsection V-D.

A. *Share withholding*

We assume that the queue-based reward scheme introduces a new attack scenario, allowing malicious miners to increase their profits at the expense of other miners in the pool.

Looking at other schemes, it may seem that reaching the top of the miner ranking as often as possible appears to be the highest rewarding strategy. However, since the credits resetting policy and hence the new credits of a miner winning a block depend solely on the credits of the miner ranked second, the optimal strategy is different. Instead of simply trying to win the next block, a miner can increase her long term revenue by winning the next block when there is a large gap between her and the second placed miner's credits. We describe a possible attack strategy in the example below.

TABLE IV: Profit improvement by exploiting a non-uniform credits dispersion. Alice stops submitting shares (a), allows Bob to pass (b) and profits from the new queue constellation (c)–(f).

(a) Before block i

Position	Miner	Credits
1	**Alice**	**110**
2	Bob	105
3	Dave	55

(b) Block i found

Position	Miner	Credits
1	Bob	115
2	**Alice**	**110**
3	Dave	60

(c) After block i

Position	Miner	Credits
1	**Alice**	**110**
2	Dave	60
3	Bob	5

(d) Block i+2 found

Position	Miner	Credits
1	**Alice**	**120**
2	Dave	65
3	Bob	15

(e) After block i+2

Position	Miner	Credits
1	Dave	65
2	**Alice**	**55**
3	Bob	15

(f) After block i+3

Position	Miner	Credits
1	**Alice**	**65**
2	Bob	25
3	Dave	10

We make use of a simplified version of our example from Section III-B. The modified setup is shown in Table IVa: Alice, in our case the attacker, is ranked first, only a few credits ahead of Bob. We observe a significant gap between the credits of the second and third placed miners. Again, we assume the two large miners, Alice and Bob, constantly earn 10 credits per round, while the small miner, Dave, earns 5. Furthermore, we assume the ranking is visible to all miners, as in the case of Ethpool [4].

By comparing the differences in credits between the first and second (Alice vs Bob) and second and third (Bob vs Dave) ranked miners, it can be seen that Bob will benefit a lot more from the credit-resetting mechanism than Alice, should this order sustain, namely 50 in contrast to 5 credits. Therefore, Alice is incentivized to stop submitting shares, this way allowing Bob to win the next block (cf. Table IVb). In the next round, Alice will be ranked first and now profits from the large difference between her and the next miner's credits (cf. Table IVc). As a result, Alice will be re-positioned in the ranking ahead of both Dave and Bob, gaining a significant advantage for the next few rounds (cf. Table IVe). This theoretical example shows that although the underlying motivation for such a credit resetting policy is to reward large miners for their above average work, Bob finds himself in a situation of having been cheated out of a significant amount of credits, which negatively impacts his long-term revenue.

B. *Tactical donation of mining power*

In order to further improve the chances of Bob overtaking her, Alice can dedicate her mining power to Bob, by spoofing the payout address she uses when submitting shares. According to the current implementation of the mining protocol, the mining pool operator will believe Bob has increased his mining power, hence rewarding him with more credits. Assuming Bob does not respond to this "forced-donation", Alice will end up even more likely in the same favourable position as discussed in the previous sub-section. An observed real-world occurrence of such a donation strategy is shown in Figure 10, where a miner in Ethpool receives an unexpected boost of mining power when they are about to win the next block.

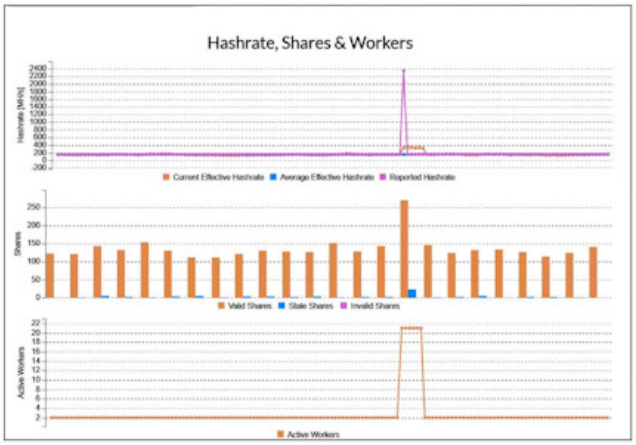


Fig. 10: Screenshot: A miner in Ethpool receives an unexpected donation of computing power at around the time at which they win a block – generosity or self-interest on behalf of the donor?

C. *Using multiple payout addresses*

Due to the pseudo-anonymity constraints in permissionless blockchains such as Ethereum, the mining pool operator cannot prevent miners from using multiple payout addresses in parallel. While miners gain no advantage from this in conventional schemes such as PPLNS, maintaining multiple accounts can be used to optimize revenues in the queue-based scheme.

Since in the current implementations, miners are not fairly rewarded for hash rate overhead, a potential solution is to start mining for other payout addresses, once reaching the top of the queue. This strategy be can be applied as an improvement to the exploitation of the non-uniform credits distribution: instead of ceasing to submit shares or investing mining power in another miner, an attacker can dedicate overhead mining capacity to her other addresses.

D. *Simulating attack scenarios*

In order to model the three different attack scenarios introduced in Section V, we use the same initial simulation setup as for the two-miner case from Subsection IV-A.

TABLE V: Attack simulation results in a two-miner scenario.

Attack strategy	Miner	Average performed work (trillion hashes)	Blocks		
			Rewarded	Mined	Ratio
Share withholding	Attacker	194.398	456 433	443 476	1.0292
	Victim	260.105	43 567	56 524	0.7707
Tactical donation of mining power	Attacker	189.85	468 678	445 227	1.0527
	Victim	349.775	31 322	54 773	0.5719
Using a second wallet	Attacker	220.61	457 161	445 668	1.0258
	Victim	253.53	42 839	54 332	0.7885

For each of the three different scenarios, the following *attacking condition* prevails: the 10 GH/s miner attacks as soon as the 1 GH/s miner's credits reach the 90% threshold of the attacker's credits[10].

Recall that the first attack described was share withholding, whereby the attacker stops the submission of shares with the aim to significantly increase the probability of the victim surpassing her before the next block is found. Once the small miner wins the block, the large miner would continue her work. After 500 000 blocks, following this strategy the attacker was rewarded an additional 12 957 blocks more than the number of blocks she actually mined (Table V).

The second attacking scenario simulated is the tactical donation of mining power,whereby the large miner directs his submitted shares to the smaller miner's payout address. This has the effect of temporarily increasing the hash rate and thereby the credits of the small miner. Following such a behaviour, the attacker received an extra 23 451 blocks.

The third attacking strategy discussed was the systematic use of multiple payout addresses. For simplicity, we simulated only one additional payout address, or a second wallet, for the 10 GH/s miner. Each time the attacking condition was met, the large miner redirected her hash rate/mining power to her second wallet. Thereby the attacker did not have to give away any of her credits to the victim. For applying this attack strategy, the 10 GH/s miner received rewards for 11 493 additional blocks.

The reason why this last attack performs worse in terms of extra blocks rewarded than the first two attack scenarios is due to the second wallet itself. By including the attacker's second wallet we are essentially adding a third miner to the simulation. However, this can lead to the scenario in which the attacker's own wallet eats into her first wallet's credits. The attacker therefore requires a strategy explicitly for protecting herself against such unfortunate queue constellations in order to increase her profits. However, we do not provide detailed suggestions for an optimal solution in this paper.

[10] After having tested and compared results using multiple thresholds, 90% proved to be the most rewarding.

E. *Other attack vectors*

Two other attack vectors include *pool-hopping* and the withholding of blocks from the mining pool. As described by Rosenfeld [20], pool-hopping refers to a miner's practice of dynamically switching between different pools in order to increase profits. In such scenarios, miners join a mining pool only when the expectation of earning rewards is high and leave as soon as the expectation drops, thereby increasing the variance of the mining pool's total hash rate. As a consequence, the expected revenues of non-pool-hopping miners decrease, making the mining pool less attractive compared to pool-hopping resistant pools.

In the current implementation of the Ethereum PoW protocol, miners are able to determine whether a found solution to the mining pool's problem also represents a solution to the network's PoW puzzle. Consequently, a miner can decide to withhold such blocks from the mining pool, which is generally referred to as block withholding. Depending on the pursued goal, an attacker can either simply damage the mining pool as a whole [20], or gamble to increase their own revenue at the cost of other miners or the mining pool operator [7].

We note these two attack strategies are not specific to the queue-based reward distribution scheme. Rather, they are applicable to mining pools regardless of the underlying payout mechanism. We therefore leave the evaluation of these attack scenarios to future work.

VI. CONCLUSION AND FUTURE WORK

We have conducted what we believe to be the first academic study of the queue-based reward payout approach implemented by Ethpool, and compared it to the Pay-Per-Last-*N*-Shares approach implemented in Ethermine. We have created a discrete event-based simulation model to analyse whether the queue-based scheme offers a fair return on investment, both for miners with large hash rates (the sharks) and those with small hash rates (the fish). From our simulation results we have seen that in a two-miner scenario and, more significantly, in the case of Ethpool, a large miner is at a disadvantage compared to the small miner(s). When compared to Ethermine's PPLNS scheme it could be seen that a large miner in Ethpool had to perform significantly more hashing operations per block won than a small miner. Obviously, miners find strategies to optimise their revenue. Real-world data from Ethpool indicates that some miners with high mining power have noticed this disadvantage and attempt to compensate for it through the exploitation of the credit resetting policy. We highlighted three different potential attacking scenarios stemming from this non- uniformity: the stalling of mining power, a tactical donation of mining power, and the use of multiple payout addresses. From our attack simulation it could be seen that attackers can indeed strategically manipulate queue constellations, receive a substantial number of additional blocks and thereby offset their initially skewed work per block ratio.

It should be noted that we have demonstrated the existence of attacks specific to the current implementation of the queue- based reward payout scheme. We modelled these attack scenarios assuming the victim miners do not defensively respond and have ignored possible pool-hopping scenarios as part of a second wallet strategy. A thorough game-theoretic analysis of such behaviour entailing multiple attackers in a multi-miner scenario, as well as an investigation into protective mechanisms to resist such exploitation attempts, could thus prove to be a fruitful avenue of future research.

VII. APPENDIX

A. *Results under Exponential Difficulty Growth*

TABLE VI: Miner performance in the multi-miner scenario under exponential difficulty increase with growth rate k = 2.726×10^{-6}.

Hash rate	Miners	Blocks			Average performed work (trillion hashes)	Average revenue per computed MH (10^{-8} ETH)		
		Rewarded	Mined	Ratio		Ethpool	Ethermine	Ratio
22.99 MH/s	5	15	13	1.1449	414.30	1.1919	1.2350	0.9651
29.9 MH/s	4	20	21	0.9765	414.63	1.1914	1.2148	0.9807
42.29 MH/s	15	29	29	1.0091	417.87	1.1804	1.1956	0.9873
57.75 MH/s	21	40	40	0.9907	417.34	1.1838	1.1932	0.9921
78.96 MH/s	33	55	55	1.0165	420.02	1.1769	1.1798	0.9975
107.81 MH/s	48	76	74	1.0234	420.80	1.1749	1.1745	1.0003
152.1 MH/s	75	107	106	1.0161	422.06	1.1719	1.1702	1.0015
203.07 MH/s	44	144	143	1.0073	422.53	1.1707	1.1677	1.0026
284.15 MH/s	78	202	200	1.0101	423.14	1.1693	1.1661	1.0027
384.66 MH/s	74	273	272	1.0023	423.22	1.1692	1.1656	1.0031
538.73 MH/s	73	383	382	1.0020	423.74	1.1679	1.1643	1.0031
729.49 MH/s	54	518	519	0.9996	423.98	1.1673	1.1638	1.0030
988.35 MH/s	55	703	702	1.0018	424.39	1.1662	1.1634	1.0024
1.39 GH/s	48	987	982	1.0054	424.78	1.1652	1.1631	1.0018
1.84 GH/s	24	1306	1302	1.0031	425.15	1.1642	1.1629	1.0011
2.54 GH/s	27	1802	1808	0.9969	425.60	1.1630	1.1626	1.0003
3.59 GH/s	18	2548	2551	0.9987	426.05	1.1618	1.1623	0.9996
4.99 GH/s	15	3534	3529	1.0013	426.52	1.1605	1.1622	0.9985
6.72 GH/s	8	4748	4772	0.9949	426.88	1.1596	1.1621	0.9978
9.91 GH/s	6	7053	7119	0.9908	427.37	1.1582	1.1621	0.9966
13.47 GH/s	3	9464	9510	0.9952	427.81	1.1570	1.1620	0.9957
18.07 GH/s	1	12858	12960	0.9921	428.05	1.1564	1.1620	0.9952

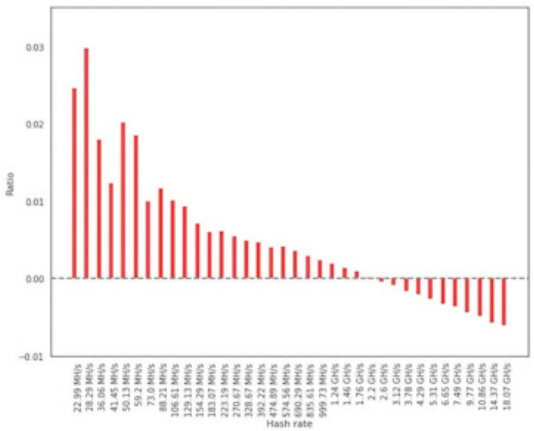


Fig. 11: Ratio of return per computed MH for miners in Ethpool, relative to the average return per computed MH under exponentially increasing difficulty with growth rate k = 2.726×10^{-6}. Miners are grouped by hash rate.

VIII. ACKNOWLEDGEMENTS

The authors would like to thank Iain Stewart for helpful discussions and insightful observations. Katinka Wolter contributed to this work while on sabbatical leave at Imperial. ■

REFERENCES

[1] Ethereum statistics. https://ethstats.net/. Accessed: 2017-06-18.

[2] Ethpool mining pool. http://ethpool.org/. Accessed: 2017-06-18.

[3] Ethpool public API. http://ethpool.org/api/credits. Accessed: 2017-06-18.

[4] Ethpool reward payout scheme. http://ethpool.org/credits. Accessed: 2017-06-18.

[5] bitfly e.U. Terms of service. http://bitfly.at/GTS v1.0.pdf. Accessed: 2017-06-18.

[6] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/ White-Paper, 2014. Accessed: 2017-06-18.

[7]N. T. Courtois and L. Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718, 2014.

[8] Ethereum community. Ethash. https://github.com/ethereum/wiki/wiki/ Ethash. Accessed: 2017-06-18.

[9] Ethereum community. Ethereum mining rewards. https://github.com/ ethereum/wiki/wiki/Mining#mining-rewards. Accessed: 2017-06-18.

[10] Ethereum community. Mining. https://github.com/ethereum/wiki/wiki/ Mining. Accessed: 2017-06-18.

[11] Ethereum community. Proof of stake FAQ. https://github.com/ethereum/ wiki/wiki/Proof-of-Stake-FAQ. Accessed: 2017-06-18.

[12] I. Eyal. The miner's dilemma. In Security and Privacy (SP), 2015 IEEE Symposium on, pages 89–103. IEEE, 2015.

[13] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore. Game- theoretic analysis of DDoS attacks against Bitcoin mining pools. In International Conference on Financial Cryptography and Data Security, pages 72–86. Springer, 2014.

[14] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof- of-stake. self-published paper, August, 19, 2012.

[15] A. Laszka, B. Johnson, and J. Grossklags. When bitcoin mining pools run dry. In International Conference on Financial Cryptography and Data Security, pages 63–77. Springer, 2015.

[16] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In Proceedings of the 2015 International Conference on Au- tonomous Agents and Multiagent Systems, pages 919–927. International Foundation for Autonomous Agents and Multiagent Systems, 2015.

[17] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor. On power splitting games in distributed computation: The case of bitcoin pooled mining. In Computer Security Foundations Symposium (CSF), 2015 IEEE 28th, pages 397–411. IEEE, 2015.

[18] M. Matsumoto and T. Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo - random number generator. ACM Trans- actions on Modeling and Computer Simulation (TOMACS), 8(1):3–30, 1998.

[19] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, Dec 2008. Accessed: 2017-06-18.

[20] M. Rosenfeld. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011.

[21] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgar-den. Incentive compatibility of bitcoin mining pool reward functions. Financial Cryptography and Data Security, 2016.

Alexei Zamyatin

Mr. Zamyatin is a research assistant and PhD student at the Imperial College London Centre for Cryptocurrency Research and Engineering. His research focuses on trustless and scalable cross-chain communication protocols under the supervision of Professor William Knottenbelt and Dr. Arthur Gervais, funded by Blockchain (GB) Ltd.

His research interests include security, sustainability and scalability of proof-of-work blockchains, as well as cross-blockchain information and asset exchange. Recent work also includes empirical analysis of blockchain data, evaluation of fairness in mining pools and modeling of miner behavior. He is also interested in blockchain sharding proposals and non-intrusive protocol update mechanisms for permissionless blockchains.

Katinka Wolter

Prof. Wolter is heading the Dependable Systems Group. Their field of research is adaptive and resilient distributed computing systems using stochastic models and online versions of machine learning techniques.

She is interested in measuring and evaluating the dependability, performance, and security of complex computing systems, with a particular focus on timing behaviour. Within their group they employ a broad range of assessment and evaluation techniques for computing systems and networks, ranging from fault-injection test-beds to simulation and analytical techniques. They develop efficient and accurate modelling and evaluation techniques, applying e.g. Phase-Type distributions in fault-modelling for fault-injection experiments and hybrid discrete-event simulation. They study a large variety of systems, including wireless networks, mobile telephony networks, service-oriented systems, and Computing Clouds.

They also conduct extensive statistical analysis of data collected from test beds as well as for medical data.

She teaches courses on Dependable Systems, Model-based Evaluation of Computing Systems, and Distributed Systems in the Master's program and Mathematics and Computer Architecture in the Bachelor's program.

IMPACTS OF CONSENSUS ALGORITHMS IN CRYPTOCURRENCY

THEORETICAL ANALYSIS OF POW VERSUS POS IN ETHEREUM

Dapeng Pan, Harbin Institute of Technology, China
J. Leon Zhao, City University of Hong Kong, China*
Shaokun Fan, Oregon State University, USA

Abstract

The plan of switching from PoW to PoS system in the blockchain has been around for a while. However, the impact of this changeover is not clearly defined although discussions on the pros and cons of PoW and PoS consensus algorithms have been ongoing in the cryptocurrency community. In this paper, we examine the bookkeeper behavior and the fairness issues of switching from PoW to PoS from a theoretical perspective. By modeling the utility of PoW versus PoS bookkeepers in the two cryptocurrency systems, respectively, we find that the distribution of bookkeepers tends to polarize in both cases as some real-world data have indicated. Our static comparison shows that in the PoS system, the bookkeepers polarize further and the top bookkeepers turn to grab even more power. That is, the efficiency advantage of PoS must be paid by giving in on market fairness.

INTRODUCTION

Most cryptocurrencies, including Bitcoin, use "proof of work" (PoW) as the consensus mechanism. However, the PoW consensus protocol has been challenged for its efficiency because the computation process requires an immense amount of energy [1]. To address this challenge, alternative consensus protocols that can achieve similar security goals are proposed to improve efficiency of cryptocurrency systems. Ethereum, as one of the most famous cryptocurrency systems, is considering transferring to the proof of stake (PoS) consensus mechanism. The PoS protocol that is designed for Ethereum is named as "Casper" [2], [3]. Since the idea about Casper was first put forward in 2015, the implementation date has been delayed for several times. Recently, Ethereum launched the Constantinople and St. Petersburg updates as preparations for the Casper upgrade. However, there are still much doubt about the efficiency, fairness, and incentive issues of switching from PoW to PoS. For example, Vitalik Buterin, the founder of the Ethereum project, expressed four concerns [4]: (1) Lower than expected participation rates in transaction validation; (2) Stake pooling becomes too popular; (3) Sharding turns out more technically complicated than expected; and (4) Operating nodes turns out more expensive than expected.

Researchers have also discussed differences between PoW and PoS on issues related to scalability, security [5], stability, incentive compatibility [6] and so on. So far, it is still not clear what could happen when a cryptocurrency's consensus mechanism switches from PoW to PoS. In this paper, we try to provide insights to this problem based on theoretical analysis of groups of bookkeepers in the system. The consensus mechanism allows participators of blockchain to run for bookkeeper in order to earn rewards. A bookkeeper needs to validate transactions, create new blocks, and verify the validity of newly created blocks [7]. A bookkeeper sometimes is also called miner or validator [8]. By modeling the bookkeepers' utilities in different systems, we first analyze the bookkeepers' behavior characteristics in PoW and PoS systems respectively. Then we make a comparative static analysis to study the impacts of protocol switch on the bookkeepers.

Bookkeepers in a PoW system

We assume that, in a PoW-based blockchain network, N bookkeepers participate in the consensus process. Let x_i denote the hash rate provided by bookkeeper i. It measures the speed at which bookkeeper i's computing power can compute the hash function in a cryptocurrency system. Hash rate is usually calculated at hashes per second. Then the bookkeeper i's relative hash rate [9] can be defined as:

$$h_i = \frac{x_i}{\sum_{j \in N} x_j} = \frac{x_i}{x_i + x_{-i}}. \qquad (1)$$

Wherein, $x_{-i} = \sum_{j \in N, j \neq i} x_j$ represents all hash rate provided by the bookkeepers other than i. Therefore, $\sum_{i \in N} h_i = 1$. The reward for bookkeeper i consists of fixed reward r_f, i.e. the mining reward and the variable reward r_{vi}, i.e., the transaction fee, which is the average

fee per transaction r_v, times t_i, the total number of trades processed by bookkeeper i. Bookkeeper i's expected utility is therefore,

$$u_i = (r_f + r_v t_i)P_i - c_i x_i. \quad (2)$$

Where, P_i and c_i denote the probability of success and the mining cost involved, respectively. A complete successful process of validation includes a mining step and a propagation step. The success probability of the mining step is directly determined by its relative computing power h_i. This is because only the first node who obtain the right hash value by solving the proof-of-work puzzle could be the bookkeeper of this block. Thus, the more computing power a node has, the more likely the node will become the bookkeeper. In the propagation step, the bookkeeper needs to propagate the mined block, which has a possibility of being discarded by other bookkeepers. This is called orphaning, which is usually caused by long network latency [10]. We use the Poisson distribution with the mean value λ to model the process of solving the proof-of-work puzzle [9], [11]. Denote P_o as the probability of orphaning, and then we can get

$$p_0 = 1 - e^{-\lambda\sigma} \text{ and } P_i = h_i(1 - P_o) = h_i e^{-\lambda\sigma}, \quad (3)$$

where σ denotes the propagation time. σ is positively related with block size which represents the number of transactions in a block but we make a simplification to assume that it is static [9], [11]. Then, Equation 2 is translated into

$$u_i = (r_f + r_v t_i)\frac{x_i}{x_i + x_{-i}} e^{-\lambda\sigma} - c_i x_i. \quad (4)$$

The objective function for bookkeeper i is

$$\begin{aligned} &\text{Max } u_i, \\ &s.t. 0 \le x_i \le \infty. \end{aligned} \quad (5)$$

By taking its first order derivative with respect to x_i, we can obtain

$$\frac{\partial u_i}{\partial x_i} = (r_f + r_v t_i)\frac{x_i + x_{-i} - x_i}{(x_i + x_{-i})^2} e^{-\lambda\sigma} - c_i.$$

According to the first order derivative condition, we have $\frac{\partial u_i}{\partial x_i} = 0$. Solve the equation, and we obtain bookkeeper i's optimal strategy in terms of hash rate to provide as

$$x_i^* = \sqrt{(r_f + r_v t_i)e^{-\lambda\sigma}\frac{x_{-i}}{c_i}} - x_{-i}. \quad (6)$$

Substitute x_i^* into equation (4) and we have

$$\begin{aligned} u_i^* &= c_i x_{-i} - 2\sqrt{(r_f + r_v t_i)c_i e^{-\lambda\sigma} x_{-i}} + (r_f + r_v t_i)e^{-\lambda\sigma} \\ &= \left(\sqrt{c_i x_{-i}} - \sqrt{(r_f + r_v t_i)e^{-\lambda\sigma}}\right)^2. \end{aligned} \quad (7)$$

It is obvious that this quadratic equation of $\sqrt{x_{-i}}$ intersects with the $\sqrt{x_{-i}}$ - axis at $\sqrt{\frac{(r_f + r_v t_i)e^{-\lambda\sigma}}{c_i}}$ and u_i^* -axis at $(r_f + r_v t_i)e^{-\lambda\sigma}$. Then we can qualitatively draw the graph of Equation 7 in MATLAB. Figure 1 shows that u_i^* has the maximal value when x_{-i} approaches 0 or ∞ (and h_i approaches 1 or 0). This demonstrates that for the bookkeepers whose relative computing power is in the middle range between 1 and 0, they would choose to reduce it to near 0 or raise it close to 1 in order to maximize profit. Bookkeepers who own sufficient financial resources and hold optimistic view about future development of the blockchain certainly would choose to raise their relative computing power to maximize profits by upgrading or purchasing more mining machines. They generally hold a large number of tokens at the same time. Even the bookkeepers who do not have much money would choose to form a collective top bookkeeper i.e. mining pool. However, the bookkeepers who only care for immediate interest but not long-term development would choose to reduce relative computing power to maximize profit, such as selling some mining machines to new bookkeepers. Even the conservative bookkeepers who do not do anything would be passively pushed to bottom bookkeepers. This is because as time goes by, their mining machines gradually lag behind the new ones and top bookkeepers control increasing computing power. Then, the conservative bookkeepers' relative computing power decreases gradually.

Hence, in the PoW-based blockchain, the amount of top and bottom bookkeepers would grow over time and the distribution of bookkeepers tends to polarize. Figure 2 shows the computing power of Ethereum bookkeepers denoted by the proportion of blocks mined in a month. We can see that most of the computing power in the system is under the control of several top bookkeepers. In fact, the top 5 bookkeepers control more than 80% of the computing power. Figure 3 shows that the bottom bookkeepers' computing power decreases in the month. Therefore, the theoretical result about bookkeepers' strategy is supported by real world data in Ethereum blockchain.

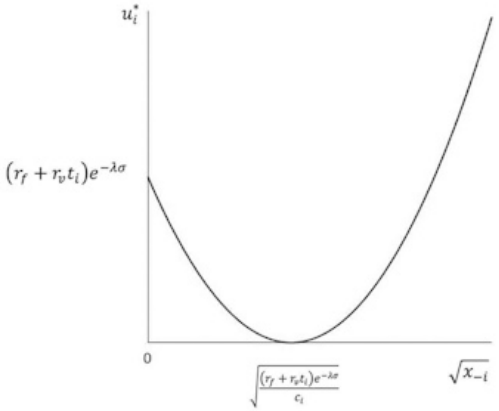


Fig. 1 Optimal Strategy in PoW based Blockchain

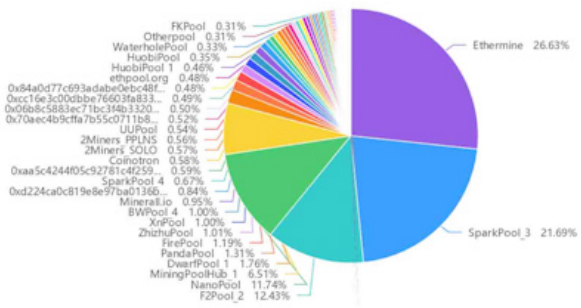


Fig. 2 Bookkeepers Distribution by Blocks[1]

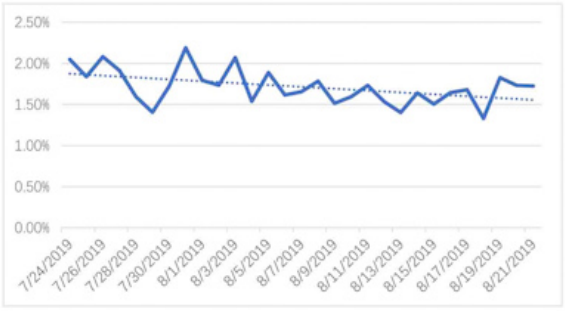


Fig. 3 Proportion of Blocks Mined by Bottom Bookkeepers[2]

Bookkeepers in a PoS system

Assume that a blockchain uses the consensus protocol PoS, let y_i denote the number of tokens staked by bookkeeper i for block creation. Then, bookkeeper i's relative stake s_i, with respect to the total stake, can be formulated [12] as

$$s_i = \frac{y_i}{\sum_{j\in N} y_j} = \frac{y_i}{y_i+y_{-i}}. \tag{8}$$

Wherein, $y_{-i} = \sum_{j\in N, j\neq i} y_j$ represents all tokens staked collectively by bookkeepers other than i. Then, the probability of success P_i can be formulated as

$$P_i = s_i e^{-\lambda\sigma}. \tag{9}$$

Same as Kang et al.'s research about PoS-based consortium blockchain [12], we model bookkeeper i's expected utility in a PoS-based blockchain as followed

$$U_i = r_f P_i + r_v t_i s_i - d_i y_i \tag{10}$$

Bookkeepers do not need to bear the cost of mining in a PoS-based blockchain. But they have to hold tokens required for staking, such that the risk of token price volatility d_i takes the place of mining cost.

Definitions of r_f, r_v and t_i are the same as defined in Section 2. By substituting (8) and (9) into (10), we can obtain

$$U_i = r_f e^{-\lambda\sigma}\frac{y_i}{y_i+y_{-i}} + r_v t_i \frac{y_i}{y_i+y_{-i}} - d_i y_i. \tag{11}$$

The objective function for bookkeeper i is therefore,

$$\begin{aligned} &\max\ U_i \\ &s.t.\ \underline{y_i} \le y_i \le \overline{y_i}. \end{aligned} \tag{12}$$

$\underline{y_i}$ denotes the minimum number of tokens required by the system regulations. For example, this number is 32 ETHs according to Casper protocol in Ethereum. And $\overline{y_i}$ denotes the total number of tokens in circulation. Note that no participator would be willing or allowed to hold all the tokens because the system will be controlled by one individual and lose its value as a public blockchain. Differentiate U_i with respect to y_i, we have

$$\frac{\partial U_i}{\partial y_i} = (r_f e^{-\lambda\sigma} + r_v t_i)\frac{y_i+y_{-i}-y_i}{(y_i+y_{-i})^2} - d_i.$$

By solving $\frac{\partial U_i}{\partial y_i} = 0$ we can obtain bookkeeper i's optimal strategy formulated as

$$y_i^* = \sqrt{\frac{(r_f e^{-\lambda\sigma}+r_v t_i)y_{-i}}{d_i}} - y_{-i}. \tag{13}$$

Substitute y_i^* into equation (11) and we have

$$\begin{aligned} U_i^* &= r_v t_i + r_f e^{-\lambda\sigma} + d_i y_{-i} - 2\sqrt{(r_f e^{-\lambda\sigma} + r_v t_i)y_{-i} d_i} \\ &= \left(\sqrt{d_i y_{-i}} - \sqrt{(r_f e^{-\lambda\sigma} + r_v t_i)}\right)^2. \end{aligned} \tag{14}$$

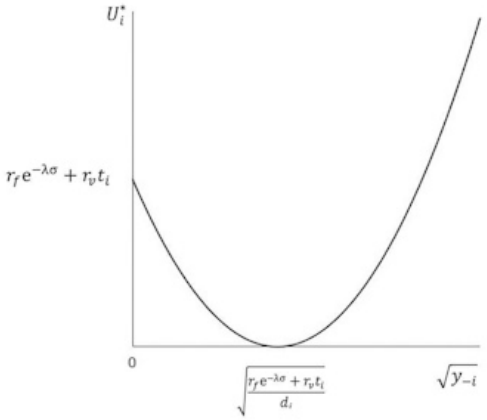


Fig. 4 Optimal Strategy in PoS based Blockchain

Similar to the results in Section 2, Equation 14 is a quadratic equation of $\sqrt{y_{-i}}$ that intersects with the $\sqrt{y_{-i}}$ -axis at $\sqrt{\frac{r_f e^{-\lambda\sigma}+r_v t_i}{d_i}}$ and U_i^* -axis at $r_f e^{-\lambda\sigma} + r_v t_i$. Then we can also qualitatively draw the graph of Equation 7. As shown in Figure 4, U_i^* achieves the maximal value when y_{-i} close to 0 or ∞, which means s_i is close to 1 or 0. Therefore, the same to the PoW situation, the distribution of bookkeepers still tends to be polarized in a PoS-based blockchain.

In addition, when a blockchain switches from PoW to PoS, in order to participate in transaction validation, bookkeepers have to hold tokens for staking. In the PoW-based blockchain, the bookkeepers who own most of the computing power (top bookkeepers) also hold most of the tokens, while the bookkeepers who own less computing power always sell out the tokens they earn immediately or hold only a few tokens (bottom bookkeepers). Therefore, the coin-holding cost of top bookkeepers is far less than the mining cost in PoW system. Equation 13 indicates that a small d_i results in

[1] https://eth.btc.com/miningstats
[2] https://www.etherchain.org/charts/miner

bigger number of tokens on hold. Therefore, top bookkeepers under PoS would buy more tokens than under PoW. Similarly, for the bottom bookkeepers, holding tokens brings more cost burden as well. Consequently, a large d_i in Equation 13 reduces the bottom bookkeepers' optimal number of tokens on hold. This means that the bottom bookkeepers may wish to hold fewer tokens than the staking minimum so as to drop out of the game.

Since the bigger computing power a bookkeeper has, the more tokens he holds, we assume this correlation is linear and can be formulated as $y_i = ax_i$, where a is unknown parameter. Then, Equation 14 can be translated into

$$U_i^* = \left(\sqrt{d_i a x_{-i}} - \sqrt{(r_f e^{-\lambda\sigma} + r_v t_i)}\right)^2. \quad (15)$$

We can see that Equation 15 intersects with the $\sqrt{x_{-i}}$ -axis at $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{d_i a}}$ and U_i^*-axis at $r_f e^{-\lambda\sigma} + r_v t_i$. By comparing Equations 7 and 15, we can obtain three cases as shown in Figure 5, where the vertical axis represents "bookkeeper utility". In this figure, we use the solid curve to indicate the utility function of bookkeeper i in a PoS system and the dotted curve to indicate the utility function of bookkeeper i in a PoW system. When $\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{a d_i}} > \sqrt{\frac{(r_f + r_v t_i) e^{-\lambda\sigma}}{c_i}}$, we have case 1. In this case, the top bookkeepers, whose h_i approaches 1 ($\sqrt{x_{-i}}$ approaches 0), would obtain more utility in the PoS system $(U_i^* > u_i^*)$ as shown in Figure 5a, where the solid curve is above the dotted curve. However, the bottom bookkeepers whose h_i approaches 0 ($\sqrt{x_{-i}}$ approaches ∞) would obtain less utility in the PoS system $(U_i^* < u_i^*)$, where the solid curve is under the dotted curve. Therefore, when system switches from PoW to PoS, the top bookkeepers have more incentive to mass more power. But the bottom bookkeepers would stay the same. This is because even though the bottom bookkeepers' utility decreases, they still obtain more utility to stay in the bottom group than in middle range. When

$$\sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{a d_i}} = \sqrt{\frac{(r_f + r_v t_i) e^{-\lambda\sigma}}{c_i}} \text{ or } \sqrt{\frac{r_f e^{-\lambda\sigma} + r_v t_i}{a d_i}} < \sqrt{\frac{(r_f + r_v t_i) e^{-\lambda\sigma}}{c_i}},$$

we have cases 2 and 3. Similar to case 1, both the top and bottom bookkeepers would obtain more utility in PoS system as shown in Figure 5b and 5c. That is to say, both the top and bottom bookkeepers have more incentive to aggregate toward to the opposite sides under PoS than PoW.

In summary, when a blockchain switches to the PoS consensus protocol from PoW, top bookkeepers tend to mass even more influence. For bottom bookkeepers, they would be weakened further or maintain the status quo. Because some bottom bookkeepers turn to quit the game due to the requirement of minimum staking tokens, the relative power of top bookkeepers under PoS would be even higher than under PoW. Of course, this theoretical result still requires validation in practice.

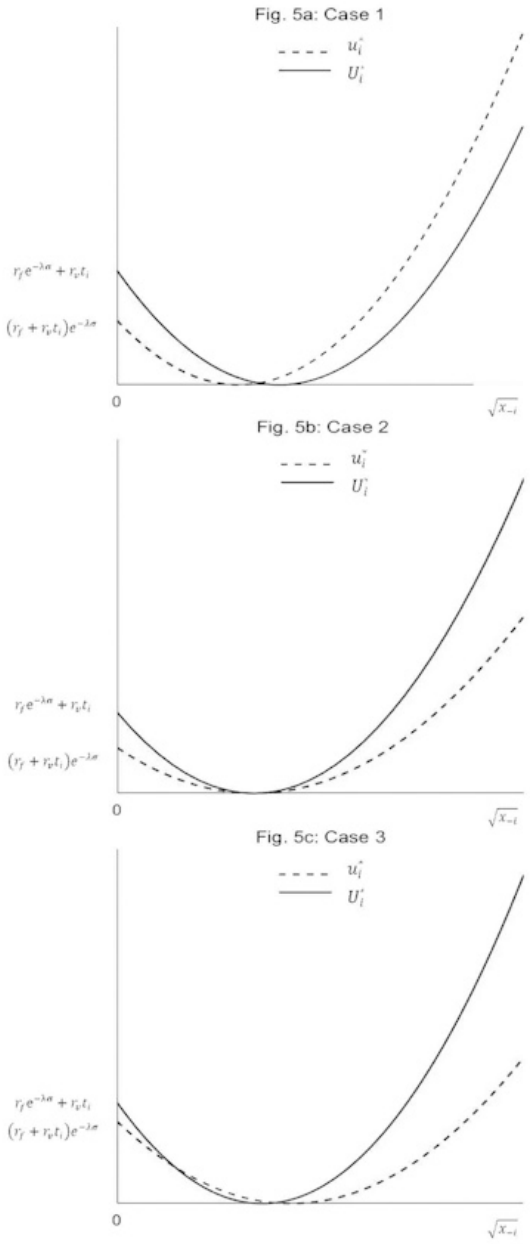


Fig. 5 Comparison of Optimal Strategies in PoW and PoS

CONCLUSION

In this paper, we develop economic models to analyze bookkeeper behavior in PoW and PoS systems and study how their behavior changes when switching from PoW to PoS by means of comparative static analysis. This theoretical research method helps us understand reasons and principles of phenomenon theoretically and generates useful insights about future development. First, we find that the distribution of bookkeepers tends to polarize in PoW systems. The validity and accuracy of result is verified by the descriptive statistical analysis in Section 2. Then we draw attention to the PoS system that Ethereum might implement in the near future. By the same method, we find that the distribution of bookkeepers tends to polarize further. Furthermore, the

degree of polarization becomes higher and both the staking power and tokens aggregate more towards to the top bookkeepers. Therefore, our findings show that although the PoS consensus protocol could solve the efficiency problem to a great degree by removing mining cost, it would make the fairness issue even more serious.

The insights of this paper are important for managers and developers of public blockchains. Decentralization as one of the most significant features of public blockchain cannot be guaranteed. The bookkeeping opportunities are always controlled by the top bookkeepers. If a blockchain such as Ethereum pays more attention to decentralization or fairness, it should be aware of this issue. When a blockchain values higher efficiency and lower energy consumption, it may switch to the PoS system. But, this comes at the expense of less fairness. In order to alleviate this negative effect, managers should reduce the minimum staking number to retain more bottom bookkeepers or encourage pooling of bookkeepers with lower staking power.

An interesting phenomenon we realized while working on this short paper is that starting with PoW and then switch to PoS once the blockchain system stabilizes is necessary because the system requires the bookkeepers to be settled down with sufficient tokens for staking. That is to say, a PoS system may be difficult to start by itself, and an initial PoW system is the necessary evil as the foundation of its PoS successor.

This study can be extended in a few directions. First, we only conducted a static analysis at the moment when the consensus protocol is switched from PoW to PoS. Future work could study the dynamics and long-term evolution of bookkeeper behavior and consider the volatility of token price. Second, with the implementation of the Casper protocol in Ethereum, empirical research could be done to validate our theoretical findings in the future. ■

REFERENCES

[1] M. Swan, *Blockchain: Blueprint for a New Economy*. 2015.

[2] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," 2017. [Online]. Available: https://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf.

[3] V. Buterin and E. Foundation, "Incentives in Casper the Friendly Finality Gadget Recap : The Casper Protocol," 2017. [Online]. Available: https://github.com/ethereum/research/blob/master/papers/casper- economics/casper_economics_basic.pdf.

[4] G. Machado, "Vitalik Buterin's Four Major Points of Emphasis Regarding the Transition to Proof of Stake Mining," 2019. [Online]. Available: https://bitcoinexchangeguide.com/vitalik-buterins-four-major-points-of-emphasis-regarding-the-transition-to-proof-of-stake-mining/.

[5] L. M. Bach, M. Branko, and M. Zagar, "Comparative Analysis of Blockchain Consensus Algorithms," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. (MIPRO). IEEE*, pp. 1545–1550, 2018.

[6] W. Wang *et al.*, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv Prepr. arXiv1805.02707*, pp. 1–33, 2018.

[7] H. Arslanian and F. Fabrice, *The Future of Finance*. 2019.

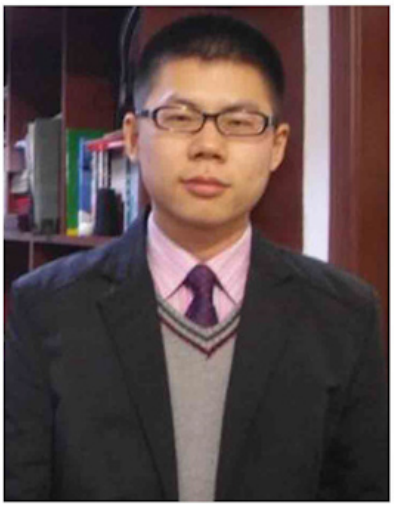
[8] G. Massarotto, "Massarotto G. From Digital to Blockchain Markets: What Role for Antitrust and Regulation," *Available SSRN 3323420*, pp. 1–22, 2019.

[9] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Edge Computing Resource Management and Pricing for Mobile Blockchain," *arXiv Prepr. arXiv1710.01567*, 2017.

[10] N. Houy, "The Bitcoin Mining Game," *Ledger*, vol. 1, pp. 53–68, 2016.

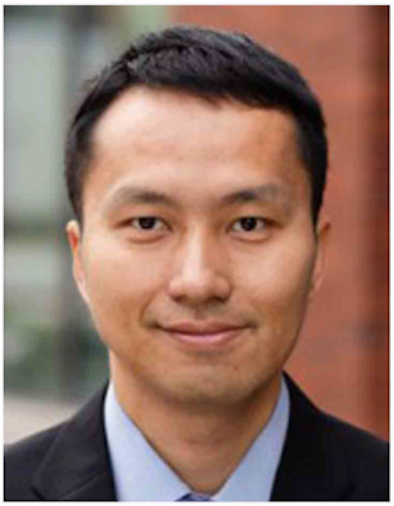
[11] R. Peter, "BLOCK SIZE LIMIT DEBATE WORKING PAPER A Transaction Fee Market Exists Without a Block Size Limit," *Work. Pap.*, pp. 1–16, 2015.

[12] J. Kang, Z. Xiong, D. Niyato, and P. Wang, "Incentivizing Consensus Propagation in Proof-of- Stake Based Consortium Blockchain Networks," *IEEE Wirel. Commun. Lett.*, no. August, 2018.



Dapeng Pan

Dapeng Pan received the B.S. degree from the School of Science, China University of Mining & Technology, Beijing, and the M.S. degree from the School of Science, Heilongjiang University. He is currently a Ph.D. student in the School of management, Harbin Institute of Technology. His research interests include consensus mechanism and incentive mechanism in blockchain network.



Shaokun Fan

Shaokun Fan is an assistant professor in Business Information Systems at Oregon State University. He received his Ph.D. in Management Information Systems from the University of Arizona. His research interests involve fintech, big data analytics, and business process management. He has taught courses on data/text mining, database, programing and system analysis and design. He has published research articles in journals such as Informs Journal on Computing, Decision Support Systems, and Information & Management.

J. Leon Zhao

J. Leon Zhao is currently Chair Professor in Information Systems, City University of Hong Kong (CityU), where he was Head of Information Systems from 2009 to 2015. Before joining CityU, He was Interim Head and Eller Professor in MIS, University of Arizona. He holds Ph.D. in Information Systems from Haas School of Business, UC Berkeley. He is currently director of the CityU Center on Global Internet Finance (since 2015), the CityUSRI Lab on Enterprise Process Innovation and Computing (since 2007), and CityUCRI Center on Blockchain-centric Business Innovation (since 2017). His research has been funded by CityU, NSF, NSFC, RGC, SAP, IBM, Shenzhen Government among others; as PI, he has received over 20 million HKD in total research funding (including two recent grants on blockchain). He received IBM Faculty Award at the University of Arizona in 2005 and Chang Jiang Scholar Chair Professorship at Tsinghua University in 2009. His research is in information technology and applications, with a special focus on FinTech and Blockchain. He has been co-editor of Springer journal on Financial Innovation, Senior Editor of Decision Support Systems, and Associate Editor of IEEE Transactions on Service Computing, ACM Transactions on MIS, and Electronic Commerce Research and Applications among others. Since 2003, He has co-edited over 20 special issues in various academic journals; most recently, he is co-editor of Big Data Special Issue for MIS Quarterly (published in December 2016) and co-editor of FinTech for Information Systems Research (to be completed in 2020). He has chaired numerous conferences and is the lead founder of several academic conferences including China Summer Workshop on Information Management (since 2007) and International Conference on Smart Finance (since 2016).

CONCEPTUAL PROTOTYPE OF CHINESE DIGITAL FIAT CURRENCY

YAO Qian
General Manager of the China Securities Depository and Clearing Corporation and former Director-General of the Institute of Digital Money of the People's Bank of China

INTRODUCTION

Design of Chinese digital fiat currency (DFC) follows the basic idea that it should be a PBOC-led initiative where digital currency based on encryption algorithm be issued in parallel with physical cash, and the DFC would be part of M0.

Governor ZHOU Xiaochuan of the People's Bank of China has made full elaboration in a series of speeches on the theoretical basis and design concepts of Chinese digital fiat currency (DFC), based on which we should draw upon international knowledge and experience and conduct in-depth analysis of the core technologies regarding digital currency. It is important, on one hand, to construct the theoretical foundation of Chinese DFC by reviewing domestic and international literature on cryptocurrency, and on the other hand, to build a basic prototype of Chinese DFC by studying various types of typical electronic and digital currency systems currently in operation.

Development History of Cryptocurrency

Relationship between digital currency and cryptographic technology

Currently in China, payment realized via electronic accounts has become very common, however it is by nature merely an informatized representation of the existing fiat currency rather than digital currency by strict definition. DFC must be issued by central bank as it is by itself a currency instead of a mere tool of payment.

A hotspot of various studies is to try to ensure digital currency security with cryptographic technologies. It is fair to say that cryptographic technology is the supporting pillar of digital currency of which issuance and circulation should be built on cryptographic principles, and that cryptographic protocols should be adopted to meet all kinds of security demands.

Centralized scheme for digital currency and its cryptographic solution

In 1982, David Chuam, known as the "father of digital currency", published a paper called B*lind Signatures for Untraceable Payments* at the International Cryptology Conference where he presented a new cryptographic protocol called blind signature based on which an anonymous and untraceable e-cash system could be constructed. The paper is regarded as the earliest elaboration on digital currency. The digital currency model proposed by Chaum is based on the tripartite model involving banks, individuals and merchants. In this model, the banks serve as an authoritative central institution which transactions between the other two parties have to rely on. The design of this solution adopts the RSA-based blind signature mechanism. A typical use case involves six steps as follows:

1. Consumer blinds transaction message M (i.e. to hide the information) and sends the blinded information B to the bank.
2. The bank signs on the blinded message B as a proof of the effectiveness of the involved digital currency. The bank then sends the signature to the consumer and at the same time deducts the corresponding amount from the consumer's account.
3. The consumer verifies the effectiveness of the blinded message B—if effective, the consumer will unblind B, thus getting message M and signature S which will be sent to the merchant.
4. The merchant verifies whether M and S are issued by the bank with the bank's public key. Valid M and S will be sent by the merchant to the bank for settlement.
5. The bank verifies if M and S are legally issued. If not, the transaction will be blocked. If yes, the bank will continue to examine if the message has existed in the consumption list—if not, the transaction will be validated and corresponding amount of money will be added to the merchant's account, otherwise the transaction will be blocked.
6. The bank informs the merchant that the transaction has been completed.

This process has become a classic cryptographic solution for centralized digital currency scheme. David Chaum founded DigiCash in 1990 and developed E-cash. Following studies on group bind signatures, fair transaction, offline trading and divisibility of currency are all based on Chaum's scheme.

The centralized scheme for digital currency relies heavily on the central party to ensure security and efficiency. Over the past few decades, studies on such scheme have focused on improving security and efficiency of the tripartite model.

Decentralized scheme for digital currency and its cryptographic solution

In 2008, Satoshi Nakamoto published a paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System* which proposed to eliminate the central institution (i.e. the banks) in the transaction process. In the digital currency scheme proposed by Nakamoto's paper, the tripartite model is replaced with a peer-to-peer two-party model. Bitcoin is by far the most mature use case of decentralized digital currency scheme. Other decentralized digital currencies all share basic features similar to those of Bitcoin.

The basic unit of Bitcoin transaction is an unused transaction output called UTXO. Essentially, the existence of Bitcoin is realized by transaction orders. Similar to bank account statements, transaction orders serve as evidence of the amount of money a customer has by recording the arrival and leaving of currency instead of providing specific balance numbers. Transaction orders record detailed information of a transaction such as the payer, the payee and the payment amount.

Via P2P network, Bitcoin adds timestamp to a bunch of transaction information within certain period of time, and the information is then integrated into a block. Mutually verified blocks are connected to one another to form a blockchain. Each block keeps a record of the previous block's header which is generated by Hash function, meaning that sequence of the blocks cannot be changed once confirmed. At the same time, the digital signature in the transaction order adopts 256-bit elliptic curve digital signature algorithm (ECDSA) to ensure the integrity and undeniability of transaction data.

The blockchain ledger is the one and only definite ledger in the P2P network of Bitcoin. Every node in the network keeps the same ledger copy and any node can join or leave the blockchain network at any time. Any update of the blockchain would be broadcast to all nodes within the network and be recognized and stored to their own databases after consensus has been reached among all the nodes based on consensus algorithm, so as to ensure the consistency of data across the entire network.

Blockchain manages to eliminate the guarantee provided by the central intermediary with sophisticated algorithm and enables a peer-to-peer payment scenario where money in an online payment initiated by one party gets to be paid directly to the other party without the involvement of any financial institution or intermediary, thus realizing the online transfer of value. Therefore, the features of Bitcoin as a classic demonstration of decentralized digital currency are made possible due to a combination of "blockchain+cryptography".

Inspiration of Typical Systems

Drawing on the experience of typical electronic and digital currency systems such as E-Cash, M-PESA, GDM, game coin, third-party payment, Bitcoin and BitMint (some of them are just experimental systems but still have academic value), the design and construction of Chinese DFC should give careful thoughts on the following core issues.

Online and offline. Currently operating electronic currency systems are mostly online. The issuance and circulation of Chinese DFC should be able to support both online and offline operation, and the two should have different rules and processes to make the design concise.

Convenience and security. Convenience is important for DFC to achieve market recognition, and security is the foundation for the healthy operation of the entire system. A balance between the two is of critical importance. To enhance efficiency and convenience, high-value and small-value payments might be treated differently in terms of security mechanisms.

Real name and anonymity. Digital currency scheme can adopt either real-name system or anonymous system, or a combination of both. Chinese DFC might be designed to allow "anonymity at frontend and real-name at backend".

Transaction and data analysis. In the environment of big data and cloud computing, identification is no longer the sole measure to ensure transaction security. The role of client behavior analysis in assuring transaction security and risk prevention deserves great attention. Enhancing client behavior analysis is an important factor to consider for central banks that may issue DFC. Digital currency can be used to support big data analysis on a macro level, but on micro lever, privacy of legitimate users should not be violated.

Relevance to bank accounts. Current electronic currency systems are mostly based on bank accounts, which is not necessarily the case for pure digital currency systems.

Ecosystem construction. For the design of Chinese DFC, it is important to involve the financial and technological community and to conduct in-depth study on and reasonable application of all kinds of creative new technologies, so as to optimize the technical framework of digital currency issuance and circulation, hold sufficient expectation of technological advance and bring in a constantly evolving and improving development idea.

Expectation of blockchain technology. Blockchain technology has received great attention as a rudiment of the next generation of cloud computing, but cases of mature application by enterprises are rare. The ideas of "private cloud+high-performance database+mobile terminal" and "private cloud+blockchain+mobile terminal" might be two related but differentiated models. It will always be the goal of central bank-issued digital currency to make the center stronger, the data more secure, the terminal smarter and the payment action of individuals more independent. If blockchain is to be applied to the development of central bank-issued digital currency, is it okay to do some necessary modification to the technology? How should blockchain make substantial breakthrough to improve the speed and efficiency of large-denomination transactions?

In a word, it is the intention of digital currency issuers to make transactions more secure and convenient, to reduce clearing steps and to lower transaction costs.

Conceptual Prototype of Chinese Digital Currency

Chinese digital currency, as a DFC, must be assured by Chinese sovereignty and its design should comply with the preliminary idea that it should be a PBOC-led initiative where digital currency based on encryption algorithm be issued in parallel with physical cash, and the DFC would be part of M0. The issuer may use security chip to make secret key and algorithm process secure, so as to ensure the security of digital currency.

The master framework for the issuance of Chinese DFC can be described as follows—the PBOC digital currency is, in accordance with the current RMB administration principles, issued and withdrawn from circulation based on the "central bank-commercial bank" system where the central bank is responsible for the issuance, verification and monitoring of digital currency and commercial banks, having obtained digital currency from the central bank, provide circulation services directly to the public and build application ecosystem.

Core components of central bank digital currency system

The core components of central bank digital currency include the following: one type of currency, two currency repositories and three operation centers. More specifically, the system contains the following main components.

Private cloud of central bank digital currency, to support the fundamental infrastructures on which central bank digital currency operate.

Digital currency, an encrypted numerical string representing specific amounts that is guaranteed, signed and issued by central bank.

Digital currency issuance repository, the database on the private cloud of central bank digital currency that deposits digital currency issuance funds of PBOC.

Digital currency commercial bank repositories, the databases for commercial banks to deposit central bank digital currency, which can be stored either at local or on the central bank digital currency private cloud.

DFC digital wallet, the terminal APP for individuals or institutional clients to use central bank digital currency at the circulation market, and the wallet can be based on either hardware or software.

Certification center, to allow the central bank to manage the identity information of digital currency institutions and users in a centralized manner. It is not only the basic component to ensure system security but also an important step in controllable anonymous design.

Registration center, to record central bank digital currency and identities of corresponding users and conduct ownership registration; and to register the entire lifecycle of central bank digital currency from its creation and circulation to settlement and annulment.

Big data analysis center, to support anti money laundering, to analyze payment behavior and regulatory and policy indicators, etc.

Encrypted creation of digital currency

To explore the representation method of Chinese DFC is definitely necessary for further studies on the basic mathematic model of digital currency (including properties, issuer, owner, user permission, scope of use, digital signature, encryption, anti-counterfeit, etc.) and for the construction of recognition and description models.

In the central bank digital currency system, D-coin can be created based on either denomination unit or the amount of physical currency in circulation. The method to be applied can be configured in the initial process by adjusting the system parameter.

An encrypted text representing certain amount of central bank digital currency is shown as:

$D_{\#}$	From	To	Value	Time	E	TVM	...

Its structure can be designed to meet specific demands, and therefore generates different kinds of coins with different features such as account balance method, UTXO-like method, etc.

Issuance and circulation of digital currency

In the central bank digital currency system, there are central bank's digital currency issuance repository, commercial banks' digital currency repositories and users' digital wallets (e.g. those on mobile phones). The relationships among the three are as follows:

According to the total issuance amount the central bank generates digital currency (i.e. digital currency issuance fund) which is deposited in the central bank's digital currency issuance repository. Upon the application of commercial bank for digital currency, the central bank sends the needed amount of currency to the corresponding database of the applying commercial bank, thus completing the process of transferring digital currency from the issuance repository to the banking repository. Upon the application of user to withdraw digital currency, the currency is moved from the banking repository, enters into circulation and is put into the storage media of the user terminal (e.g. mobile phone). At the circulation stage, payment is realized by the transfer of digital currency between digital wallets of two users, and payment is categorized into online payment and offline payment.

Key design factors

First, compliance with the idea of traditional currency management ensures that digital currency is issued and withdrawn from circulation based on the current "central bank-commercial bank" system.

Second, cryptography is adopted in the design of DFC to ensure security.

Third, the creation, circulation, settlement and annulment of DFC are entirely registered. Experience can be drawn from blockchain technology for the establishment of a ledger registration center that keeps a balance between centralization and distribution.

Fourth, trusted computing and security chip technologies are fully used to ensure end-to-end security during digital currency transaction.

Fifth, big data analysis is applied to its fullest, which not only enhances transaction security but also meets needs of AML.

Sixth, the identity authentication of digital currency user follows the principle of "anonymity at frontend and real-name at backend", which manages to protect user privacy and at the same time prevents risks of illegal transactions.

Seventh, the design of digital currency should be as concise and efficient as possible while the commercial application based on digital currency should be left to the market as much as possible, and it is important to develop sound technology standards and application rules.

Eighth, it is important to build an integrated digital currency ecosystem involving various participants including the central bank, commercial banks, third party organizations and consumers, so as to ensure that the life cycle of digital currency (i.e. its issuance, circulation and recycle) is a closed-loop with high controllability. ■

YAO Qian

Dr. YAO Qian is the Chief Executive Officer of China Securities Depository and Clearing Corporation Limited (CSDC). He is also serving as the Research Fellow at the Financial Research Centre of the Counselors' Office of the State Council of the People's Republic of China and the Secretary General of China Financial Standardization Technical Committee.

Before joining CSDC, he served consecutive positions as the Deputy Director General and Counsel of the Technology Department of the People's Bank of China (PBoC), Director General of Institute of Digital Money of PBoC, and Deputy Director General of PBoC Credit Reference Centre.

He has published around 150 papers and 7 books and holds more than 100 patents. He has been awarded provincial and ministerial first prizes for his outstanding contribution in promoting new technology development and application in the banking sector.

YAO Qian holds a Doctor of Engineering degree. He is a professorate senior engineer and a Ph.D. supervisor.

MAKING TOKENS GOVERNABLE

Mirage Li, Founder, Bit Connections

INTRODUCTION

The rise of blockchain technologies has caused both challenges and opportunities to the global regulators. In this article, we point out that the blockchain technology can be a friend to regulators in the long run, and the primary regulation should be made in the chain-level instead of exchange level.

Tokens or cryptocurrencies play a key role in blockchain ecosystems. They are the programmable contracts and can have many functions. In the bitcoin system, the bitcoins, as the tokens, help to motivate miners taking the task of maintaining the chain. In some later blockchain systems with POS (Proof of Stake) type of consensus, tokens themselves are symbols of stakes in decision-making processes. The crypto communities have issued thousands of utility tokens with various functions in the hope of revolutionizing business.

A token's primary purpose can be of payment, financing or utilities, but they all have values, high or low, and can trade with other assets. Trading of financial assets has been traditionally overseen by regulators, to ensure the fairness and efficiency of markets and to ensure that proper tax related to trading activities is collected. Tokens, or at least some sorts of tokens, have been under the scope of global financial regulators. The classification of tokens varies across regions - for example, the bitcoin can be classified as a kind of commodity or a mere payment method. However, it has been a common understanding that those tokens with security features should be treated as securities and fall under governmental regulations. Tokens with equity features, debt features, or collective investment features are considered as a new means of security issuance and should be regulated as securities.

However, in comparison with traditional securities, the tokens are much more difficult to track. It is a temptation for the regulators of some regions to outlaw the issuing and trading of these tokens based on blockchains. For example, for a standard ERC20 token issued on the blockchain of Ethereum, the ownership is anonymous, and one can create any number of new addresses on the chain. Therefore one can freely transfer some these tokens to others without revealing his/her identity. From the regulators' point of view, it is hard to catch activities such as market manipulation and insider trading. The lack of trackability and missing of regulation are considered to be substantial reasons for the chaotic nature of the ICO token markets.

In order to comply with the regulation on securities, various modification on the trading of tokens had been made. Licenses for exchanges are issued in some countries so that only a certain number of crypto exchanges are considered "legal" in these countries. New protocols are created on Ethereum, and tokens issued based on these protocols cannot be transferred directly from one address to another. A certified broker has to be involved in completing a transaction. The idea behind these rules is to modify the token trading to fit the traditional regulatory framework – the regulation on banks, exchanges, and brokers. However, these approaches contradict the fundamental idea of blockchains – the removal of the intermediaries. If a token has to be traded through a broker, it does not need to be related to any blockchain. Moreover, this token doesn't share the liquidity of the other tokens in the blockchain world.

The efficiency of these rules is questionable. For example, after licenses are issued in Japan, the share of the trade volume in Japanese exchanges in the world has dropped more than one order of magnitude in a few months. It is not likely that most token holders in Japan stopped trading, and it is anticipated that most of the trading just moved to unlicensed exchanges offshore.

On the other hand, the blockchains, with all the transactions recorded on publicly accessible databases, have provided unprecedented transparencies. Tools had been developed for information query from blockchains such as the bitcoin. One type of query can be made to find out the whole transaction history of a specific address. The other kind of query focuses on a particular coin and obtain the transaction history since its creation. For a regulation purpose, the only missing piece is the user identity associated with addresses on the chain.

Therefore, we anticipate that the regulation in the token age is primarily on-chain. Such kind of regulation would require the information of associated identities of each address on the chain. The identity information is essential for the management of tokens with security features, at least for the period of immediate future, to aid the healthy growth of the blockchain ecosystem. The elimination of market manipulation and insider trading relies on the accessibility of all the trade information. Moreover, some tokens may be only eligible to a certain set of investors. The on-chain regulations can easily

ensure that only accredited investors can have corresponding wallets.

Therefore, a governable chain would be a permissioned blockchain, with a KYC process associated with each address and transparent to a governing body. The governing body might evolve to be decentralized in the future, while currently, but it should be considered as the government regulators initially to comply with the current laws globally.

The publicly available data on chains broadens the regulation spectrum to a whole new level. One could create algorithms to analyze crowd activities and identify highly suspicious trades. The collaboration between regulators and external analyzing contractors will be possible without sharing the private information to the contractors. The governing body can use a type of regulation tokens to incentivize the policing and analysis. This kind of partnership may eventually pave the way for the future decentralized governing.

Tokens are programmable contracts and expand the horizon of securities in the age of blockchains. Wallets are the gateways for individuals to access blockchains and represent users' identities in the world of blockchains. For an established blockchain ecosystem in the future, we expect many specialized chains to be in existence while various inter-chain services serve as communicators between chains. Therefore the inter-chain smart contracts can eventually help to integrate wallets of multiple chains. The unified wallet, with a trackable identity, can turn to be a governable unit. ■

Mirage Li

Mr. Mirage Li got his Ph.D. degree in Physics from Princeton University in 2007, and worked on Wall Street as a strategist and later as a trader.

In 2014, he founded FH Technologies, a firm focusing on High-Frequency Trading. From late 2017, Mirage started trading cryptocurrencies and developed a keen interest in the application of blockchain technologies. He then founded Bit Connection Company Limited in Hong Kong; a company focused on the technological service in Blockchain technologies.

CRYPTOCURRENCY AS DIRECTLY INVESTABLE PROTOCOL

Zhong Zhang, Editor in Chief of Crypto Review

SUMMARY

Cryptocurrencies are communication networks similar to the internet, but provide their own monetary tokens. This feature allows us to invest directly in the network protocol itself, instead of investing indirectly in businesses built on the network. It provides financing for projects, like open source software, that have difficulty in raising fund through the traditional financial market. It also creates problems as monetary tokens attract speculative trading to the project at very early stage.

The time is 1995. You are a nerd with deep understanding of TCP/IP, the communication protocol underpinning the internet. You know although this protocol is not well known beyond the field of computer science, it has great economic potential: once matured, it will change the way we do everything. Sending email is only the first step. We will watch movies, play games, shopping, dating, and do all kinds of crazy stuff on the Internet. So excited about it that you want to invest in this great protocol. You want to hold a piece of it. But how?

Unfortunately, TCP/IP and the Internet are public goods, like radio spectrum, you cannot claim a piece of it and hold for a higher resale value in the future. The best you can do is to invest your financial or human capital in an Internet related business, which is like a derivative instrument on top of TCP/IP. But investing in a business brings in additional risks beyond the fate of TCP/IP. Even if the Internet succeeds eventually, the business may fail due to many factors unrelated to the technology itself.

Cryptocurrencies, by design, are directly investable protocols. Bitcoin for example, provides the first functioning protocol for organizing a decentralized monetary network. Like TCP/IP, Bitcoin's protocol is developed as an open source software, so there is no private ownership of the code. Unlike TCP/IP, Bitcoin's protocol requires a built-in monetary token: Bitcoin, which serves as the incentive mechanism for itself to work. Miners who spend millions of dollars on hardware and electricity to provide computing power supporting Bitcoin's distributed ledger, do this because they can earn Bitcoin as reward for their "proof-of-work". The functionality of Bitcoin's network and the value of Bitcoin are tightly entangled.

If you are optimistic in Bitcoin's protocol but don't want to contribute to its code or start a related business, you can simply buy and hold Bitcoin. Your action will, other factors equal, marginally increase Bitcoin's value and incentivize others to contribute in a more fundamental way. If you can improve Bitcoin's code, or build a related startup, you may also want to hold some Bitcoin as your engineering or business skills may improve Bitcoin's functionality and thus its value. The same logic applies to other cryptocurrencies with their own monetary tokens.

Being a directly investable protocol allows Bitcoin to survive and to improve in its early years without funding from angel investors or other institutions. Most early developers/adaptors of Bitcoin also mined it when mining Bitcoin was almost costless. They accumulated great wealth when Bitcoin began to attract mainstream attention and increase in monetary value. Today many of those early developers/adaptors become angel investors and provide funding for other projects that further improve the Bitcoin protocol. In this way, cryptocurrency provides a new fundraising method for developing technologies, especially open sourced ones, without traditional venture capitalists who reply on the existing financial market to eventually cash out.

Being a directly investable protocol also creates troubles for cryptocurrency development. In many cases, having a publicly traded token at very early stage of development is a curse. Shares of traditional tech startup funded by venture capitalists do not have open market trading until a successful IPO, when its business model and value have already been understood by sophisticated investors. On one hand, this makes venture capital investment quite illiquid; on the other hand, it protects the project from excessive speculation and the associated legal and regulatory cost. Bitcoin has experienced three major boom-bust cycles during its first ten years, rising from nothing to over one hundred billion US dollar in circulating market capitalization, and have created too much drama for us to ignore. Put the market noise aside, development of Bitcoin's fundamental value progresses orderly on the nerd-populated GitHub.

Cryptocurrency, as "The Internet of Money", is creating a disrupting new financing model for technology development, and perhaps for everything else too. ■

Zhong Zhang

Dr. Zhang is currently a Senior Economist at Bates White Economic Consulting, a litigation consulting firm based in Washington, DC. He is an expert in the economic mechanism design, cryptocurrency and especially the blockchain technical features of Bitcoin's ecosystem.

Before he joined Bates Whites, he was an Assistant Professor of Finance at College of Business at City University of Hong Kong. He joined CityU in 2014 after receiving his Ph.D. from Kelley School of Business at Indiana University. His dissertation is about measuring informed trading in limit order markets. Before doctoral study, Dr. Zhang obtained his M.A. in Economics from Indiana University, and B.S. in Mathematics from Zhejiang University.

Dr. Zhang specializes in Financial Market Microstructure, Investment, and Derivatives. His current research focuses on informed trading, market liquidity, leverage, and their impact on security pricing and investment decisions.

Dr. Zhang has taught Algorithmic Trading and Option Pricing at CityU, and serves as faculty advisor of CityU's award winning delegation to Rotman International Trading Competition.

Disclaimer: Dr. Zhong Zhang's involvement in "Crypto Review" and all activities associated with "Crypto Review" are solely his own and do not reflect the views or opinions of Bates White or its clients. The opinions expressed represent only those of the author, and do not represent the views or opinions of Bates White, LLC or of other Bates White employees or affiliates.

GOSS INSTITUTE OF RESEARCH MANAGEMENT LIMITED

Penthouse 24C, Tai Yau Building,
181 Johnston Road, Wanchai,
Hong Kong

Tel : +852-28015500
Fax : +852-28017700
Website : www.goss.com.hk | www.cryptoreview.hk

CITY UNIVERSITY OF HONG KONG
COLLEGE OF BUSINESS

12-200 Lau Ming Wai,
Academic Building (LAU),
City University of Hong Kong,
Kowloon Tong, Hong Kong

Tel : +852-34428989
Fax : +852-34420151
Website : www.cb.cityu.edu.hk

B2 FINTECH SCHOOL

Shanghai Main Campus:
Suite 603, Floor 6,
Jin Ying Tower A,
Han Xiao Road,
Shanghai

Tel : :+86-21-68779982
Website : www.b2fintech.com