Going Beyond the Coinbase Transaction Fee: Alternative Reward Schemes for Miners in Blockchain Systems

Harald Gjermundrød
University of Nicosia
46 Makedonitissas Avenue
1700 Nicosia, Cyprus
gjermundrod.h@unic.ac.cy

Konstantinos Chalkias
Erybo Inc.
10 Dana Street, Suite 407
Cambridge, MA 02138, USA
kc@erybo.com

Ioanna Dionysiou
University of Nicosia
46 Makedonitissas Avenue
1700 Nicosia, Cyprus
dionysiou.i@unic.ac.cy

ABSTRACT

The blockchain technology has emerged as a disruptive technology in recent years. The open and transparent nature of the distributed ledger, as supported by the blockchain technology, is an appealing factor to push this technology in applications with strong accountability and audit requirements such as cryptocurrency systems (i.e. Bitcoin) and ecommerce (i.e OpenBazaar). In order to guarantee the integrity of the distributed ledger, a set of miner nodes is in place that uses computing power to prove the authenticity of the ledger, in exchange for a small compensation fee. In this paper, alternative reward schemes for the miners are presented.

Keywords

Cryptocurrency; Blockchain Technology; Miner Reward

1. INTRODUCTION

In the last couple of years, there is fast-growing interest on the technology underpinning the Bitcoin digital currency [7], namely the *blockchain* technology. The blockchain technology is a distributed ledger that permanently stores all transactions in the network, viewable by everyone, while at the same time providing cryptographically verifiable proof for any given transaction. Due to its open and transparent nature, along with the embedded nonrepudiation and integrity mechanisms, the blockchain technology acquired its own independent identity, leading into becoming the core fundamental data structure for a variety of applications, ranging from financial applications to smart contracts.

As a public blockchain, the need for central authorities and intermediaries is eliminated but instead a set of miner nodes provide the integrity of the ledger via computational-intensive proof-of-work tasks. Operating as a miner node requires the consumption of significant computational power (electricity, cooling) to carry out the proof-of-work, something that is compensated via a small fee. In the Bitcoin ecosystem, a miner that first verifies a block gets as a reward the *coinbase transaction* for that block along with any transaction fee that is present. However, the value of the coinbase transaction gets decreased as time goes by, eventually becoming a zero value and thus yielding a zero reward for the miners (except any transaction fee that may be present in the block). As the miners constitute the backbone of the blockchain, it is essential to devise alternative reward schemes that will act as the motivating power to continue providing the verification service for the ledger.

In this paper, four alternative miner reward schemes are presented that do not conflict with with the peer-to-peer, open, and transparent principles of the blockchain paradigm. The remainder of the paper is organized as follows. Section 2 presents technical details on the blockchain functionality. Section 3 addresses the problem of the decaying value of the coinbase transaction and introduces the alternative reward schemes. Section 4 concludes the paper.

2. CRYPTOCURRENCY SYSTEMS BASICS

Cryptocurrency systems like Bitcoin are distributed peer-to-peer systems that facilitate the exchange of value transactions by agreeing on a distributed ledger, referred to as blockchain [1, 9]. The decentralized nature of the blockchain eliminates the need of a central trusted entity or intermediary by establishing a network of miner nodes that safeguard the integrity of the transactions.

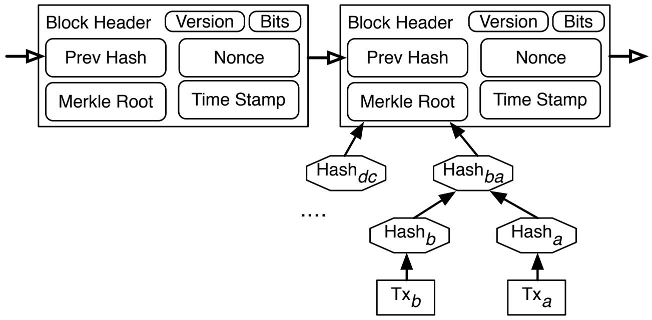

Figure 1: Bitcoin BlockChain

Figure 1 illustrates the Bitcoin blockchain, where all transactions in the network are permanently stored. Transactions reside in blocks, with a block being added to the blockchain only after being verified by a miner and *consensus* is reached among miners on its *validity*; this process is informally referred to as *mining*. As long as 51% of the miners are honest

PCI '16, November 10-12, 2016, Patras, Greece
© 2016 ACM. ISBN 978-1-4503-4789-1/16/11. . . $15.00
DOI: http://dx.doi.org/10.1145/3003733.3003773

miners (i.e. they will not claim as valid transactions those that have not taken place and vice-versa), then the integrity of the ledger is guaranteed. This concept is referred to as proof-of-work.

In a cryptocurrency system, that adheres to the original Nakamoto system principles, the value (amount of money) that is owned by an entity is *tied* in an *address*. An entity that wishes to join the cryptocurrency network, must first obtain an address. This is accomplished by first generating an ECDSA public-private key pair (*key =(key.sk, key.pk)*). The hash of the public key *key.pk* is generated and concatenated with the public key checksum, which are further encoded to create the address.

Once an entity is an owner of an address, it becomes eligible to use the digital currency system to transfer money via transactions. In a sense, a transaction involves the transfer of an amount from one address to another address. The transaction is broadcasted to the mining nodes and is added to a queue of pending (ready-to-be-processed) transactions. The miners will verify the transaction by adding it to the newest block (at that time) in the blockchain.

If the value of the current transaction is greater than the value specified to be moved to a new address (i.e the current value is 7 and the transfer value is 5), then the difference between the two values (2) is claimed by the miner as a transaction fee. In this sense the transactions are used to forward value from one address to another (similar to I owe you notes). One question remaining then is: When was the value first added to a transaction? The introduction of a value (i.e. minting new coins) into the cryptocurrency system is done in an intriguing way, that solves two problems:

1. The first problem deals with the problem of mining money and afterwards having to keep track of the valid mints, i.e. make sure that counterfeiting doesn't occur.

2. The second is that the miners will not want to work on the blockchain if there is no reward for doing it. In order to complete a block the miners must find a nonce such that when the whole block is hashed the resulting hash starts with a predefined number (the Bits field in the Block header) of zeros.

The miner that does find a nonce that satisfies the condition claims it as completed and introduces the next block in the block chain. As a reward for locating a valid nonce, a special transaction takes place into the new block, called a *coinbase transaction*. The coinbase transaction has no input address, but its destination address is specified by the miner that found the nonce of that block. The value (in Bitcoin this is currently 12.5 BTC, after the recent halvening) that is contained in a coinbase transaction will get decreased as time passes. In the Bitcoin system, the value will be halved about every 4 years, referred to as halvening.

3. ALTERNATIVE REWARD SCHEMES

The proof-of-work protocol, executed by the miners, is computationally intensive. The operator of a miner node needs to make significant investment in hardware (normally specialized hardware is used), physical space to host the computing infrastructure, and electricity for both the computing devices and the cooling system. In order to cover for the operational costs and be profitable, monetary compensation is expected from the Bitcoin community.

Currently, there are two reward mechanisms: the coinbase transaction value and any leftover *change* resulted from the transactions residing in the verified block. Due to the design principles of the Bitcoin system, the value affiliated with the coinbase transaction will eventually become zero. If no action is taken, there will be no incentives for the miners to be part of the Bitcoin ecosystem. In order to address this problem, we are proposing four alternative schemes.

3.1 Scheme A: Required Processing Fee

Even in the case of zero value in the coinbase transaction, still miners could benefit from a transaction's leftover *change*, something that is more attractive than the coinbase transaction value. However, not all transactions result in a profit but still miners have to process all transactions in the block. Having said that, introducing a required transaction fee for any processed transaction is a straightforward approach to provide compensation for a miner's work effort. Implementing a processing transaction fee requires the maintainers of the Bitcoin source code reach consensus on this matter, something that is not anticipated to be an easy decision to make for the reasons explained below.

Philosophy of the Community: Members of the Bitcoin community may advocate that charging for services that the system provides stands against the core foundation principles of Bitcoin itself. The nature of a peer-to-peer system is reflected in the collectiveness spirit to execute tasks, where members voluntarily contribute resources that could be shared among the community. The major weakness in practically implementing this notion is that the computing resources required to be a *successful* miner is out of the reach of normal users.

Amount of Processing Fee: Suppose that the community overcomes the first obstacle and decides to introduce a processing fee. The next difficult decision is the actual amount of the processing fee. Various *fee* schemes could be envisioned. A flat fixed fee could be set regardless of the value of the transaction. Thus, the same amount will be awarded for micropayments and large money transfers. Another approach is to set the fee as a percentage of the transferred value. A hybrid solution used by many electronic payment systems is also possible, where a fixed fee is applicable plus a percentage of the transferred value.

Differentiated Service Levels: Instead of charging a fee (regardless of the type), it might be possible to offer different service levels. This is a pricing model that is often used in the software industry, where you get a *free* basic version that could be upgraded with a paid version. In a sense, this is similar to how the Bitcoin system works today, where a transaction with a leftover change gets prioritized. What is proposed here is that this is formalized, with a pricing scheme, to make it deterministic what kind of service can be expected with a specific fee.

3.2 Scheme B: Minting New Coins

The reason for the decay of the coinbase transaction value lies on the fact that the number of Bitcoins that will ever be circulated is fixed. It is currently hardcoded in the source code that there should only ever be about 21 million bitcoins ever *minted*. The source code could be updated so that there will always be a positive and non zero value for the coinbase transaction. This approach does revert the founding principles set out by Nakamoto to have an inflation-proof monetary system with a fixed set of coins. There are no technical obstacles to implement this scheme, if more than 50% of the miners upgrade to a new version of the source code that supports the minting of new coins. In our opinion the introduction of this scheme is extremely unlikely, however it is important to consider what is technical possible compared to what is philosophically acceptable by the community.

3.3 Scheme C: Recirculating Lost Coins and Collecting Gold Dust

The need of recirculating *lost* Bitcoins was discussed in [6], with the primary goal being to combat deflation that could be experienced in the Bitcoin system as a result of the fixed amount of coins to be circulated. According to the authors in [6], there are three ways that could potentially lead to deflation. First, the ability to divide the value of coins into tiny amounts, referred to as *gold dust*, could contribute to the diminishing supply of coins. This is analogous to small-value coins of traditional currency systems. The difference is that in the cryptocurrency system there is no provision of issuing new coins, thus *gold dust* could have an impact over time. Second, the loss of cryptographic credentials (i.e. private key) prevents the further usage of money that are locked in transactions signed by those credentials. Last, coins are deliberately not circulated resulting in large amounts of coins held by hoarders [8].

The motivation behind the recirculation of *lost* Bitcoins is the community nature of the cryptocurrency system. It is argued that community members have privileges but also responsibilities. As a self-governing community it is essential to be active and it could be expected that the active status in the Bitcoin ecosystem is obtained by initiating money transfers from time-to-time, even self money transfers. If this requirement becomes a community policy, then the absence of transfer activities for a transaction during a specified time interval could be interpreted as dealing with a dormant transaction, thus the coins associated with the transaction could be *confiscated* and recirculated back into the system. It is important to note that the implementation of this policy could be transparent to the end user, especially if a hosting service is used for their wallet management. In this case, the hosting service will make sure that the coins are always in circulation.

Even though one may find the recirculation policy as a radical approach, consider the consequences from lack of action. Different polices (with their corresponding mechanisms) could be formulated to determine when a transaction should be considered for recirculation:

1. Interval of inactivity: The blockchain is a linked list of blocks, where a new block is added, on average, every 10 minutes. As the blockchain grows linearly that allows for a policy to be devised that would specify an dormant transaction, e.g. if at time t block x is preceded by y number of blocks, then any transaction within block x is blocked and recirculated. It is relatively easy to implement a mechanism to support this policy. Whenever a new block is mined, one block y number of blocks backward in the chain will enter *retirement*.

2. Proportional to the transaction fee: If a processing fee is supported, then the time interval before a transaction is considered dormant would be proportional to the processing fee given to the miner. The larger the processing fee, the longer a transaction could reside in the blockchain before being considered dormant. Compared to the previous policy, it is more complicated to implement the mechanism for this one as the level of granularity differs; in the current policy the granularity is per transaction as opposed to per block for the previous one.

3. Based on Value and Interval of inactivity: The aim of this policy is to collect gold dust as soon as possible, giving at the same time a longer lifetime for transactions containing large values. The lifetime of the transaction would be a function of its value. There are numerous benefits to the successful implementation of this policy. It will motive the users of the system to gather all their values together (collection of gold dust), hence reducing the number of active addresses in the system. The smaller size of active addresses will positively impact the scalability of the system. The complexity of implementing a mechanism for this policy is similar to the previous one, as the granularity of the recirculation is on the transaction level.

Once the conditions are set on which coins are to be recirculated in the system, the next step is to decide the scheme of reintroducing them into circulation. The main objective is to encourage the miners to continue their tasks by providing monetary incentives. Below are some proposed polices for distributing the reclaimed dormant coins:

1. Linearly distributed: This is the easiest policy to implement and it simply allocates the aggregated value of all transactions that will enter *retirement* (according to selected policy) to the miner that verifies the next block in the blockchain. The main drawback though is that the miners will be able to predict when a large reward will be given and may only be willing to mine for blocks that will yield a large reward.

2. Percentage of a common purse: In order to avoid the problem of instability that the previous policy may cause, the aggregated value of the recirculated transactions is to be added to a common *virtual* purse. A function will determine the value that will be given to the miner for each new mined block. It could be a percentage of the current amount available or a fixed value that would decrease/increase at deterministic intervals depending on the current total in the purse.

3. Lottery among miners: It could be that the value collected for recirculation is not very large. Hence, if part of this value will need to be allocated to the miners for each block that is mined it may not be enough to motivate the miners to continue to do their job. In this regard, it may be better to aggregate the values of recirculated transactions until it becomes substantial. A raffle could be held among the miners for the aggregated value. Motivation for this is similar to how the various lottery systems works. Even though the probability of winning the lottery is small, citizens still buys lottery tickets in the hope of striking it rich.

A prototype system has been implemented based on the work proposed in [6] (i.e. implementing Dormant Transaction Policy 1 - Interval of inactivity and Recirculation Policy 1 - Linearly distributed). The system was tested in a local deployment of the Bitcoin software and it stands as a proof that the schemes are technically feasible, in non-disruptive manner. Similarly, there is no technical limitation for implementing all the above policies, however there will be great resistance from the community where each member will have different motivations. In this paper we are only interested in presented various technical options that may be of interest to the community, and leave the politics for the discussion forums.

3.4 Scheme 4: Raffles

Unlike conventional lotteries using ping pong balls or electronic raffles where a randomization algorithm runs internally at a safe hardware infrastructure, public data that is very difficult to be a-priori predicted has been proposed as an undeniable source of randomness [3]. Some examples of open data sets that can be used as random beacons include:

1. The aggregated closing prices of the stocks that comprise an index in the stock market [5].
2. Weather conditions such as temperature, wind and humidity at a certain time in the major world capitals [4].
3. Official flight landing times at biggest airports [4].
4. The next block in a proof-of-work blockchain [2, 3].

It is a fact that currently at least 68 bits of min-entropy are produced every 10 minutes in the bitcoin protocol, thus the inherent unpredictability of each next block can be used as a source of public undeniable randomness [2]. Compared to the common national lotteries that rarely offer more than 30 bits of entropy, the aforementioned 68 bits are more than enough to conduct a raffle. Based on the above, three mining-rewarding policies, each one offering different properties, are presented below.

1. Random Reward per Block (RRB): Assuming there is a common purse for recirculated transactions, a function is required to define the exact amount of coins that will be given to the miner of each block. To provide a motivation mechanism and on the same time circumvent the practicality issues of the linear distribution and the fixed percentage policies presented in Section 3.3, the rewarded amount can be defined each time at random. This randomly selected amount must be bounded by a wisely selected lower and more importantly upper limit to avoid huge rewards that will minimize the available coins in the pool leaving no incentive for the upcoming miners.

Regarding the actual randomization protocol, the hash of each particular block is used as a seed to a function that outputs a value $r = Random(low, high)$ that will eventually define the rewarded coins. In this scenario, the miner is instantly aware of the amount won, but she cannot add this transaction to her block's Merkle tree, because the hash output will be altered. To avoid this, the next miner is responsible to include this winning transaction to her new mined block and so on.

2. One Lucky Miner (OLM): In another scenario, there is a draw every N blocks and the lucky miner wins a specified amount from the common purse. In this setting, each $N - th$ miner produces the random seed (the hash of the new mined block) and the last N miners participate on this raffle, following the raffle protocol of [4]. Unlike the RRB approach, in OLM not every miner is a winner and apparently participants have to wait for the "announcement" till the raffle takes place.

3. Native Bitcoin Raffle (NBR): By using the extended version of [4], the blockchain can be used for organizing an international lottery system where every user can participate by utilizing the OP_RETURN metadata of the bitcoin protocol. In this scheme, the miner of X block has actually produced the seed of this raffle and she will be rewarded for that contribution by an amount defined in the raffle's terms and conditions. This is very similar to conventional transaction fees and the amount won, which includes a percentage from the common purse plus coins from user bets, is actually shared between a lucky user and the lucky miner giving incentives to both users to make bitcoin transactions and miners to perform mining.

4. CONCLUSIONS

Cryptocurrency systems, like Bitcoin, rely on the blockchain technology to store and manage all transactions in the ecosystem. Miners are the system core entities that safeguard the integrity of the blockchain, in exchange for a fee. Due to the design principles of some cryptocurrency systems (like Bitcoin), this mining fee will eventually become zero as it gets decreased over time. In order to motivate the miners to continue their task, we present alternative reward schemes that act as monetary incentives. For each scheme, a detailed description is given we well as the anticipated reaction from the cryptocurrency community. The technical approaches are feasible to implement and could be introduced in an non-destructive way.

For future work we would like to implement all the policies that we have defined for recirculating coins and deploy them in a local testbed. In addition, we would like to to investigate the various ways that the blockchain technology could be used as a service for various applications (in order to generate some value for the miners), similar to the raffle service explained in this paper.

5. REFERENCES

[1] A. M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Crypto-Currencies.* O'Reilly Media, Inc., 2nd edition, 2015.

[2] J. Bonneau, J. Clark, and S. Goldfeder. On bitcoin as a public randomness source. Technical report, Cryptology ePrint Archive, http://eprint. iacr. org/2015/1015, 2015.

[3] K. Chalkias. Secure undeniable random numbers, 2011. Demo at http://saferandom.com.

[4] K. Chalkias, P. Chrysochoidis, A. Kichidis, and G. Siourounis. Saferandom - verifiable random generator from open data. In *NBG i-Bank #fintech Crowdhackathon.* National Bank of Greece and CrowdPolicy, 2016.

[5] J. Clark and U. Hengartner. On the use of financial data as a random beacon. In *USENIX EVT/WOTE.* USENIX Association, 2010.

[6] H. Gjermundrød and I. Dionysiou. *Recirculating Lost Coins in Cryptocurrency Systems*, pages 229–240. Springer International Publishing, Cham, 2014.

[7] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Available: http://www.bitcoin.org/ bitcoin.pdf, 2009.

[8] D. Ron and A. Shamir. *Quantitative Analysis of the Full Bitcoin Transaction Graph*, pages 6–24. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[9] M. Swan. *Blockchain: Blueprint for a New Economy.* O'Reilly Media, 2015.