UiT
THE ARCTIC UNIVERSITY OF NORWAY

Faculty of Science and Technology
Department of Computer Science

Trading Network Performance for Cash in the Bitcoin Blockchain

subtitle

—

Enrico Tedeschi
Master Thesis in Computer Science

Abstract

Nowadays blockchain systems are emerging and they are spreading each day more. Cryptocurrencies are the biggest example of a physical implementation of this protocol, having in 2012 more than 50 thousands transactions per day and reaching now in 2017 more than 350 thousands of transactions approved every day. In this thesis we evaluate the most famous blockchain system, the *Bitcoin blockchain*. Public blockchains have emerged as a plausible messaging substrate for applications that require highly reliable communication. However, sending messages over existing blockchains can be cumbersome and costly as miners require payment to establish consensus on the sequence of messages. The blockchain protocol requires an always growing size of the informations stored in it so its *scalability* is the biggest problem. For that reason we collected data to be analyzed and stored in our own dataframe, saving up to $x10$ space for the analysis.

This thesis will consider the network performance of the Bitcoin public ledger when used as a massaging substrate. From 2009 to 2017 a lot of analysis has been done on Bitcoin blockchain and meanwhile its block size limit changed multiple times, from 256 bytes up to 1 Mb, the Bitcoin price raised from ~ 0.7 \$ to more than 4.000 \$ and different papers were published discussing whether changing or not the block size limit or talking about the fees a miner could get from clients. We read and considered previous analysis on Bitcoin blockchain, we then present our own dataset, which contains a significant portion of the Bitcoin blockchain, updated at 09-2017, discuss our results and compare them with other evaluations from past years, then we also discuss how the fee paid to miners evolves during time and how much a client could pay for a faster approval time, plus we take into consideration transaction visibility, blockchain growth and fees paid to miners. From this we propose and evaluate, using machine learning techniques, three different cost prediction models for predicting bandwidth per Bitcoin cost of upcoming transaction. The models can be used by application to throttle network traffic to optimize message delivery. We also discuss and consider, according to the data obtained, whether the block size limit should be increased for an higher *throughput* or not.

People are using Bitcoin because it has a lower fee rate and no central authority, we aim to find any possible relation between the fee paid from a transaction to a miner and the approval time of this transaction, plus we also noticed that the bigger is the blockchain size the more the system become centralized, since only few members, or nodes, of the Peer to Peer network can support and use the full blockchain.

Bitcoin blockchain has been analyzed with a blockchain analytics system, developed using Bitcoin's API and data were collected both by using the API and parsing blockchain.info HTML pages. A total of # transactions has been evaluated, more transactions than ever were considered before and useful informations about the Bitcoin blockchain emerged. This thesis gives also a measurement about accuracy of data provided from blockchain.info.

Contents

List of Figures

My list of definitions

1

Introduction

In 1964, Paul Baran [22] represented a very clear topology describing the differences between a centralized, decentralized and distributed network (Figure 1.1). Since then, the attention in developing systems moved from a centralized scheme to a distributed one, leaving most of the computation to every single user in the network rather than a central coordinator. Such a change might be easy for systems that do not require much of security, where authentication or authorization is minimal. However, the more a system needs to be secure, the more the decentralization process might be tricky as it becomes very important to rely on some trusted central coordinator. Systems that more than others need to be secure are the one related to e-commerce, banking and trades, all systems that have to deal with money.

In 1983, a research paper by David Chaum introduced the idea of digital cash [25]. In 1990 he founded *DigiCash*, an electronic cash company that closed because of bankrupt in 1998. After that, other systems such as *e-gold* (1996) and *PayPal* (1998) emerged. However, these systems allowed digital money transfer while they were still relying on a central authority. In 2008 Satoshi Nakatomo has presented Bitcoin [43], the first decentralized digital currency. Until 2008 e-commerce used to rely exclusively on financial institutions serving as trusted third parties. Those are involved in the electronic payments process and they have to guarantee consistency of the transactions and security of data.

Decentralized digital currencies are not dependent on any trusted third parties and they are built over a Peer to Peer (P2P) network where every component

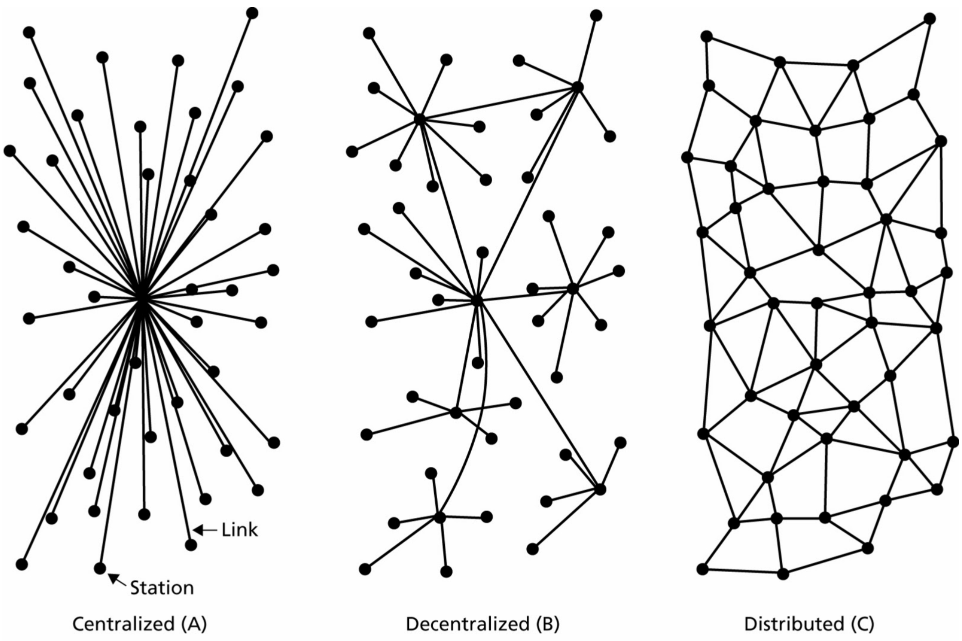

Figure 1.1: Differences between network topologies. Source: On Distributed Communication Networks, Paul Baran, 1964.

has the same privileges. These systems allow money exchange without a central authority, which means lower fees, no geographical separation and global trust among users. After Bitcoin, more decentralized digital currencies emerged, in 2011 *Litecoin*, originally based on the bitcoin protocol, then in 2013 Gavin Wood has presented *Ethereum* [51] and in 2014 *Monero* currency was released.

The order of transaction is essential in any cryptocurrency systems. However, establishing correct order can be problematic in decentralized cryptocurrency systems as they allow arbitrary nodes to join, including nodes that might be malicious. If arbitrary or Byzantine faults are allowed, the system might be left in an inconsistent or invalid state [37]. The ability to mask Byzantine faults has been implemented in various systems such as Byzantium [32], HRDB [49] and MITRA [39]. These protocol guarantees consistency of transactions having f faulty nodes, with a total of N nodes where $N = 2f + 1$ or $N = 3f + 1$, and a protocol like *Fireflies* [36] provides secure and scalable membership management and communication substrate in overlay network with Byzantine members. To guarantee an order of transaction all these cryptocurrencies rely on the *blockchain* protocol.

1.1 Blockchains

The need to tolerate malicious members was the reason for introducing the *blockchain* into cryptocurrency systems. The fundamental principle behind the blockchain is that consensus on transaction ordering is based on contributed computational power rather than number of participants. The blockchain works by appending transactions in blocks. Every block is generated after a relevant computation (*proof-of-work*), and each new block is appended to the public ledger of data, the blockchain, having in that way an ever growing chain of data containing every transaction ever happened.

Besides its use in cryptocurrency, this blockchain technology opens up to several usages in different sectors such as trading, file storage or identity management. Indeed it is already used by NASDAQ in its private socket market. If used in a P2P file sharing network, the blockchain removes the need of a centralized data base and heavy storage areas. Moreover it allows users to create tamper-proof digital identities for themselves. Blockchain technology opens up to usages in several important sectors such as trading, file storage, and identity management.

Blockchains essentially implements a distributed consensus protocols that enable a set of untrusted processes to agree on the content of an append only data structures. These ledgers are divided into blocks and linked together in sequence by hashes. They facilitate transactions between consenting individuals who would otherwise have no means to trust each other and deal with geographical separation and interfacing difficulties This technology promises a highly resilient and communication substrate where messages are kept potentially for a long time.

Nonetheless, decentralized digital currencies also have some side effects. The most relevant is *scalability*, due to the steady growth of the blockchain. It should be also considered that decentralized cryptocurrencies operate in open (or permissionless) networks in which the ledger of data could be manipulated from arbitrary adversaries and according also to the paper from University of Singapore [40] security of smart contracts has not received much attention yet. And since the only part not protected from cryptography is the *order of transactions* [10], an attacker would try to convince the network that a transaction occurred earlier than another one to gain money. The security bugs in smart contracts are classified as *Transaction-Ordering Dependence*, *Timestamp Dependence*, *Mishandled Exceptions* and *Reentrancy Vulnerability* [40].

1.2 Problem Statement

While doing research, studying and reading papers related to blockchains, it turned out that the most urgent concerns are related to its scalability and performance, but also to the fee a client has to pay to get better latency. In 2015, Möser and Böhme write [42]:

> *Bitcoin may not be as cheap for consumers as it appears.* [. . .] *Bitcoin users are encouraged to pay fees to miners, up to* 10 *cents (United States Dollar (USD)), per trnsaction, irrispective of the amount paid.*

Rizun writes in 2015 [44]:

> *The block size limit was set at one megabyte, corresponding roughly to three transactions per second.* [. . .] *The transaction rate is over three hundred times larger than when the block size limit was introduced, and rising the limit is now being seriously considered.*

Then Croman writes in 2016 [26]:

> *The current trend of increasing the block sizes on Bitcoin protends a potential problem where the system will reach its maximum capacity to clear transactions, probably by* 2017.

It is obvious then that these problems need to be taken into consideration. In this thesis we discuss the scalability of the blockchain, how it affects the throughput and we present performance observations of the Bitcoin blockchain, analyzed with a blcockhain analytic system developed for this purpose. We provide detailed insights and analysis on how Bitcoin's characteristics, such as fee, block size and reward to different miners involved have changed over time, and provide an updated model describing how the Bitcoin blockchain will grow. We analyzed the correlation between the fee paid from a transaction and its *latency*, or the time it takes to be visible in the whole network. Three different models are proposed to describe how applications best can spend money to improve network charactertics, this affects average bandwidth available to an application.

1.2.1 Scalability

Scalability and network performances are urgent concern in existing Blockchain-based cryptocurrencies [26]. According to Ethereum white paper [10], if Bitcoin would have the same amount of transactions of a VISA circuit, its blockchain would grow about 1 Mb every 3 seconds, $\sim$ 28GB per day, instead of the actual growth of ~ 0.12GB per day. In this thesis we discuss how much scalability affects centralization in Bitcoin network and how much it will impact in the next couple of years the blockchain growth.

1.2.2 Performance

Centralized schemes, like VISA are immediate, while having a throughput of 2000 transactions/sec up to 56 thousands transactions/sec [26]. It is true that Bitcoin has lower fees than centralized currency schemes, but these properties come at a performance and scalability cost. In the paper from Croman [26], they claim that Bitcoin achieve a throughput of 7 transactions/sec. In this thesis we also want to update at 2017 this statment and see how much a block size change might influence the whole network performance.

1.3 Method / Context

In this thesis we analyze a considerable part of the blockchain. In the paper from 2015 written by Möser and Böhme [42], they analyze tips and tolls in Bitcoin blockchain, they collected data until 2014 and they analyze more than 9 million of transactions. At that time there were a total of 100 thousands transactions per day, while today we count about 350 thousands txs/day, so the retrieving part turned out to be more time consuming than expected. Despite that, we aim to collect even a larger portion of the blockchain, storing data smartly in a *data frame*, which allows us to spare up to $10x$ of the space the blockchain actually requires. Then we analyze data and with *machine learning* techniques we define models, discuss about the results and how much they can be reliable in a future-wise implementation. In our data frame we store more than # transactions, with an analysis in between #date and #date. We used for the information retrieval Application Programming Interface (API) from Blockchain.info combined with a HyperText Markup Language (HTML) parsing on every "block-page" of the same website.

Our assumption is that we can get sufficient information about the blockchain growth, the block creation time, the time for a transaction to be visible in the public ledger of data and which miners are the more trendy and which usually requires more fee by retrieving and analyzing only a portion of the blockchain, but having in that way a finer granularity than the one represented in the Bitcoin website. In that way we hope to gain more informations out of it. Moreover, sampling data from a single node in the blockchain gives statistics representative of the whole system.

For the analysis, data are retrieved block per block and part of the blockchain is saved in a text file. This finer granularity allows us to have a lot of informations that may be hidden in the statistical analysis provided from Bitcoin. It is also possible to use the informations retrieved to make future predictions about how much the Bitcoin blockchain will grow, using polynomial interpolation on the data. According on how many blocks ago are fetched, it is possible to have an accurate prediction on the blockchain growth for the next few years.

We are going to compare more recent data, retrieved real time, with the Bitcoin one and see the differences of the blockchain growth. Moreover, In the Bitcoin website for blockchain analysis, `blockchain.info` [4], the finer granularity shows data for the last 7 days while we are collecting and monitoring data at every block creation ($\sim$ 8-10 min). In that way is easier for us to check if there are any abnormalities in the ledger of public data.

1.4 Outline

2

Related Works - SotA

As mentioned in Chapter 1, scalability and analysis on the blockchain has been taken into consideration by many researchers in the past years. This chapter summarizes the most relevant papers or works that talks about Bitcoin, blockchain and decentralized cryptocurrencies, it gives a short view of what has already been done and the reults obtained. In our previous paper [48], we enhance the importance of paying for having a certain bandwidth in the Bitcoin network. A paper from Peter R. Rizun [44], explains how a rational Bitcoin miner should select transactions from his node mempool, when creating a new block, in order to maximize his profit. We discuss that and apply new data from more recent sources to this idea of "selecting the right transaction" in a way that a miner could select the right transactions to earn more money out of the whole mining process. Scalability has taken into consideration in the Position Paper of Kyle Croman [26], they analyze how fundamental bottlenecks in Bitcoin limit the ability of its current peer-to-peer overlay network to support substantially higher throughputs and lower latencies. We are going to test the throughput as well, comparing it with the one showed in this paper. Regarding fees and tolls paid in the Bitcoin blockchain we refer to the study done in 2014 from Möser and Böhme [42]. They analyze the entire blockchain and make assumptions about that these "fees" are supposed to substitute miners' minting rewards in the long run. This paper contributes empirical evidence from a historical analysis of agents' revealed behavior concerning their payment of transaction fees. Furthermore, to fully understand how is possible to make money out of the blockchain and mining, in necessary to have a view of how *VISA* [11] makes money as well.

2.1 Rizun - A Transaction Fee Market Exists Without a Block Size Limit

2.1.1 Problems

A pressing concern exists over the ramifications of changing (or not) a Bitcoin protocol rule called *block size limit*. This rule sets an upper bound on the network's transactional capacity, or *throughput*. The limit was set at 1 Mb, corresponding roughly to three transactions per second. When this limit was set, it was over eight hundred times greater than what was required. However in 2015, blocks were filled near capacity and users experienced delays. In 2015 the transaction rate was over three hundred times larger than when the block size limit was introduced. One of the concerns is whether, in the absence of a limit or if the limit is far above the transactional demand, a healthy transaction fee market would develop which charges users the full cost to post transactions. The object of this paper is to consider whether or not such a fee market is likely to emerge if miners, rather than the protocol, limit the block size.

2.1.2 Methods

This paper shows how a Bitcoin miner should select transactions from his node's mempool when creating a new block in order to maximize his profit in the absence of a block size limit. *Block space supply curve* and *mempool demand curve* are explained, and the paper shows how the supply and demand curves from classical economics are related to the derivatives of these two curves. In the paper Rizun claims that the block-size limit determines the transaction throughput. In this paper he derives the *miner's profit equation* and then he introduces two novel concepts called the *mempool demand curve* and the *block space supply curve*.

Miner's Profit Equation

Every time a block is mined, the miner expects to generate a revenue $\langle V \rangle$ at hashing cost $\langle C \rangle$ to earn profit per block

$$\langle \Pi \rangle = \langle V \rangle - \langle C \rangle. \tag{2.1}$$

Miner's profit equation in 2.1 shows the gain of a miner $\langle \Pi \rangle$, where the hashing cost is represented as follows:

$$\langle C \rangle = \eta h T. \tag{2.2}$$

So the hashing cost $\langle C \rangle$ is directly dependent from the miner's individual hash rate, h, the cost per hash, η, and the creation time, T. Moreover, is important to consider the expectation value of a miner's revenue per block, this value is represented with $\langle V \rangle$ and is equal to the amount he would earn if he won the block multiplied by his probability of winning. So the expected revenue would be: $\langle V \rangle = (R + M)h/H$, where the amount he would earn is the sum of the block reward, R, and the transaction fees, M. His probability of winning, assuming all blocks propagating instantly, is equal to the ratio of his hash rate, h, to the total hash rate of the Bitcoin network, H. The problem with this equation is that it does not reflect the miner's diminished chances of winning if he chooses to publish a block that propagates slowly to the other miners. If a miner finds first a valid block, but his solution is received after most miners are working on another, then his block will likely be discarded. This effect is called *orphaning*. The equation, considering the orphaning factor, $\mathbb{P}_{orphan}$, is the following:

$$\langle V \rangle = (R + M)\,\frac{h}{H}\left(1 - \mathbb{P}_{orphan}\right). \tag{2.3}$$

Where P_{orphan} increases with the amount of time a block takes to propagate to other miners. Indeed, if τ is the block propagation time, the probability of orphaning is defined as:

$$\mathbb{P}_{orphan} = 1 - e^{-\frac{\tau}{T}}. \tag{2.4}$$

In conclusion the *miner's profit equation* is defined as:

$$\langle \Pi \rangle = (R + M)\frac{h}{H}e^{-\frac{\tau}{T}} - \eta h T \tag{2.5}$$

A *rational miner* selects which transactions to include in his block in a manner that maximizes the expectation value of his profit. This selection is explained with the *mempool demand curve* and the *block space supply curve*.

The Mempool Demand Curve

The set of transactions that still need to be approved and included in a block is called *mempool*. The mempool set is denoted with $\mathcal{N}$ and the number of transactions contained within it as n. According to the size limit, a block can select a $b \leq n$ transactions from $\mathcal{N}$ to create a new block $\mathcal{B} \subset \mathcal{N}$. A block first includes transactions with an higher *fee density*, ρ. This last, is a ratio between the *transaction fee*, t_f and the *transaction size*, t_q. To construct the mempool demand curve, is necessary first sorting the mempool from greatest fee density to least and then associating an index $\{i : 1, 2, \ldots, n-1, n\}$ with each transaction in the resulting list. The mempool demand curve will be then a graphical representation of the sum of the fees offered by each transaction in this sorted list:

$$M_{demand}(b) \equiv \sum_{i=1}^{b} fee_i, \tag{2.6}$$

and the sum of each transaction's size in bytes:

$$Q(b) \equiv \sum_{i=1}^{b} size_i. \tag{2.7}$$

The mempool demand curve represents then the maximum fee, $M_{demand}(b)$ a miner can claim by producing a given quantity $Q(b)$ of blockspace.

The Block Space Supply Curve

The size of the block a miner elects to produce controls the fees he attempts to claim, $M(Q)$, and the propagation time he chooses to risk, $\tau(Q)$. The block space supply curve represents the fees a miner requires to cover the additional cost of supplying block space Q. This cost grows exponentially with the propagation time. The equation which represents this curve is the following:

$$M_{supply}(Q) = R\left(e^{\frac{\Delta\tau(Q)}{T}} - 1\right), \tag{2.8}$$

where $\Delta\tau(Q) \equiv \tau(Q) - \tau(0)$. The propagation time ,$\tau$, is just an esteem from the propagation delay versus the block size.

Maximizing the Miner's Profit

To maximize his profit, the miner construct a mempool demand curve and a space supply curve. The block size Q^* where the miner's surplus, $M_{demand} - M_{supply}$, is largest represents the point of maximum profit. Considering this point Q^* of maximum profit, Rizun considers three market conditions for Bitcoin transaction fees: *healthy*, *unhealthy* and *non-existent*. In a healthy fee market, the miner's surplus is maximized at a finite quantity of block space, and thus a miner is incentivized to produce a finite block. In an unhealthy market, the miner's surplus continually increases with block space, and therefore a rational miner should produce an arbitrary large block. In a non-existent market, including *any* transactions results in a deficit to the miner, and so the miner is better off producing an empty block. A rational miner will produce a big block if his mempool is full of high fee density transactions, and will produce an empty block if no transactions pay a fee sufficient to offset the orphaning risk.

2.1.3 Results

In conclusion, they show that a transaction fee market should emerge without a block size limit if miners include transactions in a manner that maximizes the expectation value of their profit. A critical step in establishing this result was their calculation of the miner's cost to supply additional block space by accounting for orphaning risk.

2.2 Möser & Böhme - Trends, Tips, Tolls: A Longitudinal study of Bitcoin Transaction Fees

2.3 Croman - On Scaling Decentralized Blockchains

3

Technical Background

4

Blockchain Analytics System

5

Blockchain Observations

6

Conclusions

6.1 Discussion

6.2 Future Implementation

6.3 Comments

show bibliography [43], [51], [21], [30], [40], [28], [10], [15], [41], [45], [34], [36], [17], [32], [49], [39], [1], [6], [24], [7], [47], [22], [46], [4], [8], [9], [16], [19], [18], [38], [20], [12], [26], [31], [33], [13], [2], [3], [44] [5], [48], [29], [35], [11], [23], [42], [14], [50].

References

[1] Bitcoin api's, api-v1-client-python. https://github.com/blockchain/api-v1-client-python.

[2] Bitcoin mining hashing rate. https://blockchain.info/charts/hash-rate.

[3] Bitcoin nodes. https://bitnodes.21.co/.

[4] Bitocoin's blockchain website. https://blockchain.info.

[5] Construct a linear, no-fork, best version of the bitcoin blockchain. https://github.com/bitcoin/bitcoin/tree/master/contrib/linearize.

[6] Ethereum api's, pyethereum. https://github.com/ethereum/pyethereum.

[7] Ethereum wiki/patricia tree. https://github.com/ethereum/wiki/wiki/Patricia-Tree.

[8] Ethereum's blockchain analysis website. https://etherscan.io.

[9] Ethereum's blockchain website. https://etherchain.org/.

[10] Ethereum's white paper. https://github.com/ethereum/wiki/wiki/White-Paper.

[11] How visa make money. https://revenuesandprofits.com/how-visa-makes-money-understanding-visa-business-model/.

[12] Matplotlib for data plotting. https://matplotlib.org.

[13] Mining hardware comparison. https://en.bitcoin.it/wiki/Mining_hardware_comparison.

[14] pandas: Python Data Analysis Library. `http://pandas.pydata.org/`, 2012.

[15] Ethereum foundation - the solidity contract-oriented programming language. Technical report, https://solidity.readthedocs.io/en/develop/, 2014.

[16] Bitcoin mining process. `http://bitcoinminer.com/`, 2015.

[17] Bitcoin website – mining. `https://www.bitcoinmining.com`, 2016.

[18] Ethereum project – website. `https://www.ethereum.org`, 2016.

[19] tradeblock.com – analysis on the blockchain. `https://tradeblock.com`, 2016.

[20] Alfred V. Aho and Jeffrey D. Ullman. *Foundations of Computer Science*. Computer Science Press, Inc., New York, NY, USA, 1992.

[21] Adam Back. Hashcash - a denial of service counter-measure. Technical report, 2002.

[22] Paul Baran. *On Distributed Communications: Introduction to Distributed Communication Networks*. The Rand Corporation, 1964.

[23] Massimo Bartoletti, Andrea Bracciali, Stefano Lande, and Livio Pompianu. A general framework for bitcoin analytics. *CoRR*, abs/1707.01021, 2017.

[24] Georg Becker. *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*. 2008.

[25] David Chaum. Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, *Advances in Cryptology Proceedings of Crypto 82*, pages 199–203, 1983.

[26] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer. *On Scaling Decentralized Blockchains*, pages 106–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

[27] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings*, pages 1–10, Sept 2013.

[28] Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi. *Step by Step Towards Creating a Safe Smart Contract: Lessons and In-*

sights from a Cryptocurrency Lab, pages 79–94. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

[29] Jacob Donnelly. Bitcoin network still backlogged with tens of thousands of unconfirmed transactions, causing delays. *Bitcoin Magazine*, July 2015.

[30] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '92, pages 139–147, London, UK, UK, 1993. Springer-Verlag.

[31] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert van Renesse. Bitcoin-ng: A scalable blockchain protocol. *CoRR*, abs/1510.02037, 2015.

[32] Rui Garcia, Rodrigo Rodrigues, and Nuno Preguiça. Efficient middleware for byzantine fault tolerant database replication. In *Proceedings of the Sixth Conference on Computer Systems*, EuroSys '11, pages 107–122, New York, NY, USA, 2011. ACM.

[33] Begnaud Francis Hildebrand. *Introduction to Numerical Analysis: 2Nd Edition*. Dover Publications, Inc., New York, NY, USA, 1987.

[34] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation (3rd Edition)*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2006.

[35] Nicolas Houy. The economics of bitcoin transaction fees. Working Papers 1407, Groupe d'Analyse et de Théorie Economique (GATE), Centre national de la recherche scientifique (CNRS), Université Lyon 2, Ecole Normale Supérieure, 2014.

[36] Håvard D Johansen, Robbert van Renesse, Ymir Vigfusson, and Dag Johansen. Fireflies: A secure and scalable membership and gossip service. *ACM Transactions on Computer Systems (TOCS)*, 33(2):5:1–5:32, May 2015.

[37] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, July 1982.

[38] Craig Larman. *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd Edition)*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2004.

[39] Aldelir Fernando Luiz, Lau Cheuk Lung, and Miguel Correia. Mitra: Byzantine fault-tolerant middleware for transaction processing on replicated

databases. *SIGMOD Rec.*, 43(1):32–38, May 2014.

[40] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 254–269, New York, NY, USA, 2016. ACM.

[41] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. Demystifying incentives in the consensus computer. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 706–719, New York, NY, USA, 2015. ACM.

[42] Malte Möser and Rainer Böhme. *Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees*, pages 19–33. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[43] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf, 2008.

[44] Peter R. Rizun. A transaction fee market exists without a block size limit. Technical report, 2015.

[45] Chaitya B. Shah and Drashti R. Panchal. Secured hash algorithm-1: Review paper. Technical report, Indus Institute of Technology and Engineering, Gujarat Technological University, 2014.

[46] William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 3rd edition, 2002.

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

[48] Enrico Tedeschi. Paying for bandwidth in blockchain internet applications. Technical report, UiT Arctic University of Norway, 2016.

[49] Ben Vandiver, Hari Balakrishnan, Barbara Liskov, and Samuel Madden. Tolerating Byzantine Faults in Transaction Processing Systems Using Commit Barrier Scheduling. In *ACM SOSP*, Stevenson, WA, October 2007.

[50] Michael Waskom, Olga Botvinnik, drewokane, Paul Hobson, David, Yaroslav Halchenko, Saulius Lukauskas, John B. Cole, Jordi Warmenhoven, Julian de Ruiter, Stephan Hoyer, Jake Vanderplas, Santi Villalba, Gero Kunter, Eric Quintero, Marcel Martin, Alistair Miles, Kyle Meyer, Tom Augspurger, Tal Yarkoni, Pete Bachant, Mike Williams, Constantine Evans, Clark Fitzgerald, Brian, Daniel Wehner, Gregory Hitz, Erik Ziegler, Adel

Qalieh, and Antony Lee. seaborn: v0.7.1 (june 2016), June 2016.

[51] Dr. Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Technical report, 2014.

A

Terminology

RLP: Stands for recursive length prefix. It is a serialization method for encoding arbitrary structured binary data (byte arrays).

KEC-256: Another serialization method generating a 256-bit hash.

full node: A full node in a decentralized digital currency peer-2-peer network, is a node that stores and processes the entirety of every block, storing locally the entire size of the blockchain.

light node: A light node in a decentralized digital currency peer-2-peer network, is a node that only stores the part of the blockchain it needs.

satoshi: Unit of the Bitcoin currency. 100,000,000 satoshi are 1 BTC (Bitcoin).

B

List of Symbols

t_B	transaction approved in a block B.
t_{in}	transaction input in bitcoin (Ƀ). All the money sent.
t_{ou}	transaction output (Ƀ). All the money received.
t_f	transaction fee (Ƀ). $t_{in} - t_{ou}$.
t_q	transaction size, in bytes.
t_l	commit latency of a single transaction. $B_{epoch} - t_{epoch}$.
$\mathcal{T}$	expected block interval time ($\sim 10\,\text{min}$)
$\mathbb{P}_{orphan}$	probability that given a block is orphaned.
τ	block solution propagation time, we consider a $\tau = 10$ seconds

	according to Decker [27].
η	cost per hash.
$\langle \Pi \rangle$	expectation value of a miner's profit per block.
$\langle V \rangle$	expectation value of a miner's revenue per block.
$\langle C \rangle$	expectation value of a miner's hashing cost per block.
R	block reward, currently at 12.5 Ƀ.
h	miner's individual hash rate.
H	total hash rate of Bitcoin network.
Q	block size or block space in bytes.
Q^*	the block size that maximizes the miner's expected profit.
ρ	fee density, or the price per byte for block space.
M	money, bitcoin (Ƀ).
$M_{demand}(b)$	partial sum of the b transaction fees in mempool in order of descending fee density.
$M_{supply}(Q)$	miner's cost due to orphaning to produce a certain block size Q.
$\mathcal{N}$	the set of transactions in a miner's mempool.
n	number of transactions in a miner's mempool.

B single block.

B_t transaction root that links to every transaction in a block B.

/C

Listing