Security and Performance Issues Present in Cryptocurrencies and Trade-Off Analysis of Proposed Solutions

Mertcan Yasakçı   
Computer Engineering Department  
Faculty of Computer and InformaticsIstanbul, Turkey  
yasakci@itu.edu.tr

Muhammed Burak Buğrul  
Computer Engineering Department  
Faculty of Computer and InformaticsIstanbul, Turkey  
bugrul@itu.edu.tr

***Abstract*— This paper explains blockchain technology from foundations of data recordings such as first writing tablets to newest technology trends including technical base of the blockchains. It clarifies some known issues and problems present in are of security and performance of cryptocurrencies and gives some real life examples to them. Then it analyses suggested solutions to these issues. In the end, almost everything comes to a point that has trade-offs and decision making as in other fields of computing.**

***Keywords—blockchain, cryptocurrency, scalability, security, performance***

# Introduction

Computing and information technologies are developing exponentially from the beginning of humanity. There are many applications that humans used in past but not anymore thanks to improvements in field of computing and information. One of the latest innovation in the field is blockchain technology. Most popular applications of blockchain technologies is cryptocurrencies. In this paper, security and performance issues present in cryptocurrencies and trade-off analysis of proposed solutions to that problems will be investigated. Problems occurs continuously in this area due to increasing usage of this new technology. As the number of problems increased, number of proposed solutions to these problems are increased as well. These problems and proposed solutions analyzed in this paper.

# Foundation of Recording Systems and Early Examples of Ledgers

## First Recordings

As a result of human relations, recordings became a crucial topic in history due to need of barter, purchase, diplomacy savings, treaties etc. Without recording important events, there would be major security issues in every organization that base their current events to their(or another organizations’) past events. With invention of writings, all of these became possible. People used stone tablets as ledgers and books to record. “The cuneiform script, created in Mesopotamia, present-day Iraq, ca. 3200 BC, was first.”[6]. After that day, all institutions and organizations and even individuals are started to record their events in order to prevent future disputes and conflicts.

## Early Examples of Ledgers

In order to track prices and transaction details of transferring of goods, people used somewhat centralized books. These efforts take place in history before 5000 to 10000 years from today. Over time these books and ledgers are used to solve disputes occurred in transactions and trade between people. This usage proves the truthfulness property of these systems. This means in that time people used to trust these books and ledgers. They provide this records to public in order to maintain and protect trust to these records.

Over time, people adapted these early examples of ledgers to the time they are living. These derived examples of ledgers are used more differentiated purposes in order to meet people’s expectations. For example, in order to decide which people to trust while trading these derived examples of ledgers are used. This situation also proves that these ledgers are open to public and can be used and viewed by anyone who request. Although these ledgers are public, all control mechanism is centralized and uncontrollable by other people.

# Birth of Blockchain and Its Goals

Developing technology and advancing humanity replaced stone tablets with animal skins and papers over time. With the digitalization of world and humanity, ledgers and record books transformed into recording (databases, texts etc.) in computers and clouds. But monolithic architecture problems and uncontrollability still remained in these systems. In past years a new decentralized system suggested, blockchain. “In their simplest form, blockchains are the digital equivalent of the old stone ledgers.” [4]

Before defining blockchains, topic of linked lists and hashes should be covered.

1. Linked List: A simple structure where every element pointing the next one. It can be traversed via using these pointers until the end. Every item in the linked list called as nodes. Nodes contains data related to the system that use linked list and a pointer to the next node (sometimes they contain pointers to previous nodes, in this situation the structure named as ‘Doubly Linked List’). Pointer of the last node (named as tail node) is optional if it points to the first node (named as head node) the structure named as ‘Circular Linked List’. A linked list can be ‘Circular’ and ‘Doubly’ at the same time.
2. Hash: Hash functions can map a data that can be in different size to a new one that has a fixed size. Results of the hash functions (called as hash values) often stored in hash tables. Hash functions are useful in occurrence check, ciphers, equality check, data corruption control, data simplifications, data transforms etc.

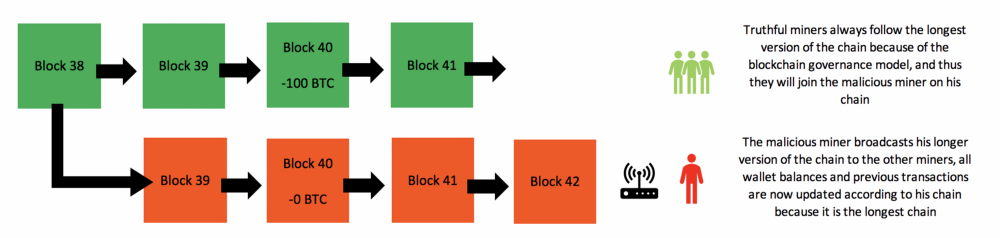
Blockchains are decentralized and controllable by other people. In technical aspect, a blockchain is a linked list. In every node of the linked list, a hash pointer to previous node can be found. By validating data flow and architecture of the linked list, everyone can see stability of data in the linked list. Anyone cannot change the data without broke the hash mechanism. This provides immutability on the linked list.[7]

When someone tries to change the data in some node of the linked list, he/she should change all hashes recursively. Due to impossibility of this action, it can be said that blockchains are immutable.

# Development of Cryptocurrencies and Achievements of Them

Technology, computing and their applications has progressed incredibly throughout the years, from punch-cards to the present supercomputers. These developments bring us these days where each gadget is associated with the web. As web turned out to be more accessible to individuals, they begun utilizing social organizes. Thus, the web turned into a piece of individuals' lives, in this way a virtual world developed which just exist on the web. The quantity of individuals utilizing the web increments quickly and online administrations are utilized more frequently than their genuine counterparts. This expansion required creation of the virtual economy. For this virtual economy to work, it must have a virtual cash to make exchanges.

In order to fill that virtual cash gap, cryptocurrencies are developed. Cryptocurrency technology, removed third parties in the middle of transactions. “The technology makes it possible to carry out reliable commercial transactions that do not go through third parties on the internet, which was difficult to realize before.” [3] Before cryptocurrency technology, international money transfer required so many third parties in the middle of a transaction. These third parties are increasing the transfer time. Faster applications like Western Union are faster than classical transfer, however, they are more expensive. “Until now, the costs of remittance were 5–20%. The blockchain reduces the costs to 2–3% of the total amount and provides guaranteed, real-time transactions across borders.” [2]

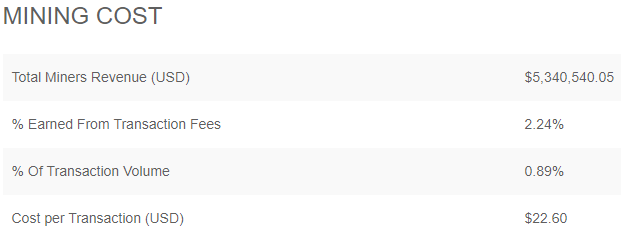
Cryptocurrencies utilizes digital money units called coins. These units are used to represent value and transferred between users. Coins have no physical representation, they exist only on the bitcoin network and users transfer money using this network. Cryptocurrencies can be used just like any other currency, to sell or buy goods or service. Cryptocurrencies uses a decentralized system; it runs on mathematical principles to verify transactions thus does not need a central bank or authority. The blockchain is the ledger where all transactions ever happened in the history and is publicly available. All information about cryptocurrency exists in its blockchain.

# Security and Performance Issues Present In Cryptocurrencies

Day by day, some problems and deficiencies occurs in are of cryptocurrencies and blockchains. For continuity and scalability of this technology, these problems should be solved or avoided. Some of known issues are:

## Scalability Problem

Bitcoin is most popular online cryptocurrency in our world now. These days, there are more than 200.000 transactions occur in every 24-hour period in BTC [8]. Validations of transactions can take minutes and in online digital world, this is a very slow case. Also there are general validations of whole system, length of these validations can take days (Bootstrap time). When costs of transactions and confirmations examined, it can be seen that miners take a crucial place in these costs. [9]



SS taken from [8]

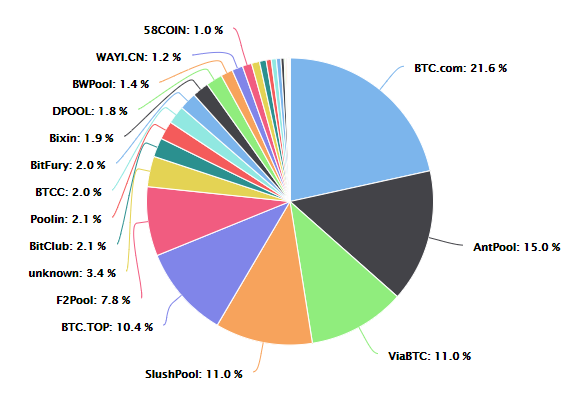
This scenario brings a lot of point that can be a bottleneck. Also people who delve into cryptocurrency area should note that 1MB block size limit of Bitcoin.

## The Majority

“A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system.” [11]

If someone has more than %50 of the miners, he/she can be the fastest node and can decide properness state of any block and control all of the blockchain.

Bitcoin has a wide usage in the world. People currently using Bitcoin in food, clothing, e-commerce industries etc. A successful majority attack can change the fate of millions of real money transactions. Mining pool distribution chart of last 1 year:



SS taken from [12]

## Regulatory Compliance

In systems that only have straight transactions like Bitcoin is suitable for blockchain usage. But not all system flows are as simple as Bitcoins’ flow. Applying blockchain innovation in intensely controlled businesses, for example, law or fund, with monetary forms other than Bitcoin will result in administrative issues and lawful inconveniences. Controls were intended for a framework altogether different from that of blockchain and the guidelines can't be effortlessly customized to fit blockchain activity, with the extreme transparency of having all records conveyed to all system individuals. Further, blockchains work online over purviews with various administrative principles, making it hard to guarantee consistence with all standards. [13]

Also there are different agreements between every company and different taxations for every system. It seems impossible to code every relation in control system of the blockchain. In addition, Changes in agreements, laws and creations of new laws will break the current control system of the blockchain

## Software Updates

Every software has a development cycle and versions. Some versions are for implementing new features, some for fixing bugs, some for both. In software world implementing new features/fixing bugs are done after forking a specific version. After finishing the task and tests new version can be released. But in blockchain this is difficult because the architecture is not monolithic. Every node should be updated in order to make the blockchain operate properly. But there are two problems:

* Updated and non-updated nodes can break the operations.
* As the number of nodes increase, the time required for update all of the nodes increase as well.

# Solutions Proposed for Security and Performance Issues Present In Cryptocurrencies

## Scalability Problem

There are various solutions proposed for this major problem of cryptocurrencies. First of them to increase block size. Increasing block size directly affects number of transactions per second. But this solution is like a double edged sword. Since blocks that are generated are sent to other nodes in the network, increasing block size creates a network stress and even if you can fit more transactions in a block, block transfer time will increase because of increased block size.

Another solution for this problem can be expressed as off-chain contracts. For a recurring transaction, sender and receiver can make an agreement to group those recurring transactions in a period. After this agreement, transaction is done for whole period for once. This system may lower the transactions in a network, however, it also contradicts with cryptocurrency principles.

A further solution is, instead of requesting a whole network to reach a consensus, waiting for only a fixed number of nodes to agree on a transaction. In other words, instead of whole network, only the selected number nodes are enough to validate a transaction.

## The Majority

Majority problem also expressed as 51% attack in the field. This attack compromises integrity and confidentiality of the blockchain. In order to prevent a malicious node to have more computing power than the rest of the network, different proof algorithms are implemented in cryptocurrencies. Such as proof-of-stake which is based on amount of total assets and proof-of-importance which is based of assets and transaction rates. Another solution for this problem is to introduce a penalty for each delayed block submission.

## Regulatory Compliance

Blockchains with their own money, for example Bitcoin, seems to exist against the law, as there is nothing that any administration specialist can do to influence or change their activity, and the Federal Reserve seat has said it has no specialist to control Bitcoin. Transactions will clear whether legitimate, and won't clear whether not substantial, and there is nothing that controllers can do to topple the agreement of the system handling power. [13]

It seems like a deadlock situation, because when laws and governments applies, more than simple validations and hash check occurs such as taxations, time checking, company and category specific laws, permissions, IDs (hardest part in blockchains) etc. So in some areas trade-off cannot be possible. There are only two cases, applicability and non-applicability of a blockchain system. Because there is no such system as “Perfect System”, so if it is not suitable, it shouldn’t be used.

## Software Updates

There are two concepts to solve this problem. One of them is hard fork. Hard fork basically introducing new rules to the system that are not backward-compatible. In this situation all of the nodes in the network have to be informed about this change in order to these nodes continue to produce valid blocks for the blockchain.

Another one is the soft fork. In soft fork changes introduced to the network are backward-compatible. In this situation majority of the network power should agree to update.

# Conclusion

From the first writing tablets to new blockchain systems there have been always management, security and performance problems. There have been always crisis situations and deadlocks. In an area of problem, there are generally bottleneck factors. Blockchains are used in different type in wide area, so they have their own bottlenecks and problems.

In scalability topic, there is a trade-off between decentralized and transparent architecture and performance. For the regularity there is a trade-off between simplicity and runnability of the system and lawful/agreemental correctness of the system. But for the software upgrade topic in one way or another updates should be done, it doesn’t matter the used in these updates.

Number of example scenarios can be increased, but almost all of them leads the solution to deciding the target and which place he/she want to be on the trade-off in order to satisfy his/her goals most.

##### References

1. E. Karaarslan ve E. Adiguzel, “Blockchain Based DNS and PKI Solutions”, IEEE Communications Standards Magazine, c. 2, sy 3, ss. 52-57, Eyl. 2018.
2. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, ve G. Das, “Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems”, IEEE Consumer Electronics Magazine, c. 7, sy 4, ss. 6-14, Tem. 2018.
3. Y. Kano ve T. Nakajima, “A novel approach to solve a mining work centralization problem in blockchain technologies”, Int J of Pervasive Comp & Comm, c. 14, sy 1, ss. 15-32, Nis. 2018.
4. T. Felin ve K. Lakhani, “What Problems Will You Solve with Blockchain?”, MIT Sloan Management Review; Cambridge, c. 60, sy 1, ss. 32-38, Fall 2018.
5. “The Evolution of Writing | Denise Schmandt-Besserat”. .
6. “The Evolution of Writing | Denise Schmandt-Besserat”. .
7. “Blockchain Applications for the Real World (Blockgeeks Guide)”, Blockgeeks. [Çevrimiçi]. Erişim adresi: https://blockgeeks.com/guides/blockchain-applications-real-world/. [Erişim: 26-Kas-2018].
8. “Bitcoin currency statistics”, Blockchain.com. [Çevrimiçi]. Erişim adresi: https://www.blockchain.com/stats. [Erişim: 26-Kas-2018].
9. K. Croman vd., “On Scaling Decentralized Blockchains”, içinde Financial Cryptography and Data Security, c. 9604, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, ve K. Rohloff, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, ss. 106-125.
10. I.-C. Lin ve T.-C. Liao, “A Survey of Blockchain Security Issues and Challenges”, International Journal of Network Security, c. 19, sy 5, ss. 653-659, Eyl. 2017.
11. “Proof of work”, bitcoin.it. [Çevrimiçi]. Erişim adresi: https://en.bitcoin.it/wiki/Proof\_of\_work. [Erişim: 26-Kas-2018].
12. “Bitcoin currency statistics”, btc.com. [Çevrimiçi]. Erişim adresi: https://btc.com/stats/pool?pool\_mode=year. [Erişim: 26-Kas-2018].
13. S. Ammous, “Blockchain Technology: What is it Good for?”, Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2832751, Ağu. 2016.
14. A. Castor, “A Short Guide to Bitcoin Forks”, CoinDesk, 27-Mar-2017. .