FINANCIAL INNOVATION SERIES

GLOBAL RISK INSTITUTE

FINANCIAL INNOVATION SERIES

BLOCKCHAIN AND ITS APPLICATIONS TO CRYPTOCURRENCIES

AUTHORS: **Alex LaPlante PhD,**
Managing Director of Research, Global Risk Institute

Alexey Rubtsov PhD,
Research Associate, Global Risk Institute

Abstract:

This paper provides a non-technical introduction to blockchain technology using cryptocurrencies as an illustrative example. We describe the mechanics of blockchain and outline some risks associated with the existing cryptocurrencies.

1. INTRODUCTION

Recent years have witnessed substantial innovation in the financial services sector with a wide range of new technologies coming to market. Highlighted by the 2016 World Economic Forum as one of the seven most world-changing technologies, blockchain is a technological innovation with the potential for broad applicability in finance.[1] Consequently, many financial experts have noted the potential implications of such a technology. At the Consensus 2016 event, former US Treasury Secretary Larry Summers stated:

> *"I'm reasonably confident…that the blockchain will change a great deal of financial practice and exchange."*

Blockchain is a type of distributed ledger: a database that exists across several locations, usually referred to as participants, nodes, or computing devices. The most important feature of distributed ledgers is that they are not maintained by any central authority, and all updates are made after consensus among participants has been reached; the latest, agreed-upon version of a ledger is saved separately by each participant. The absence of a trusted third party is perceived by many as a way to reduce the costs of maintaining the ledger and to make the ledger more secure. Distributed ledgers can have a variety of forms, and blockchain is a particular form in which all transactions are organized in blocks that are linked to one another and secured using cryptography. Its append-only structure makes it practically impossible to alter or delete previously entered data. Thus, blockchain technology is well-suited for recording events and managing records.

At present, cryptocurrencies are one of the most quickly developing applications of blockchain technology. Cryptocurrencies employ blockchain as a digital ledger on which all transactions are securely stored. While the ideas behind blockchain trace back to a series of papers by Haber and Stornetta published in the early 1990s, recent advances in computer science have used cryptography and clever incentive engineering to make a conceptual breakthrough: a pseudo-anonymous, fully decentralized blockchain.

This paper is organized as follows. Section 2 provides a non-technical introduction to blockchain technology using cryptocurrencies as an example. In Section 3 we list some of the flaws in the existing crytpocurrencies. Section 4 concludes.

---

1 See https://www.weforum.org/agenda/2016/01/a-brief-guide-to-the-technologies-changing-world/

2. BLOCKCHAIN AND CRYPTOCURRENCIES

In this section we describe the blockchain technology as applied to cryptocurrencies. Our intention is not to give a technical description, but rather to illustrate how the blockchain works and explain the system of incentives that underlies it.

Assume we have four individuals who do not want to rely on any third party to manage their transactions. The individuals only have details of each other's accounts and they might not know each other's identities in the sense that their account numbers are not linked to their names. For simplicity assume that our individuals' account numbers are #1, #2, #3, and #4 (see Figure 1).

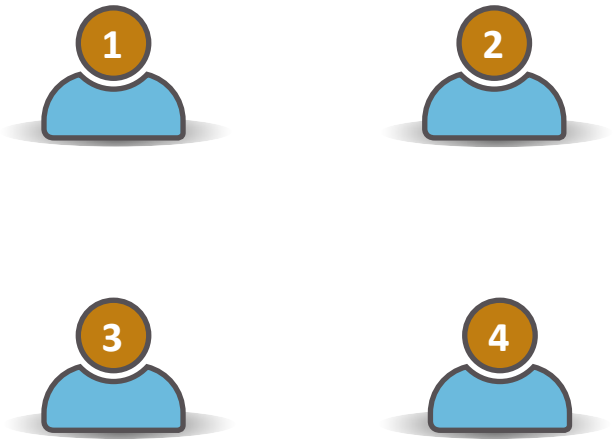


Figure 1. Only account numbers, not individuals' identities are available.

All individuals have an empty folder and they will keep adding pages to their folders as more and more transactions occur (all folders are identical). We will refer to each of the folders as a **ledger** which tracks the transactions.

2.1. A TRANSACTION HAPPENS

Assume that #1 wants to send $9 to #4. To make the transaction, #1 announces to all four individuals, "*I want to transfer $9 to #4. Add this transaction to your pages*." (see Figure 2).

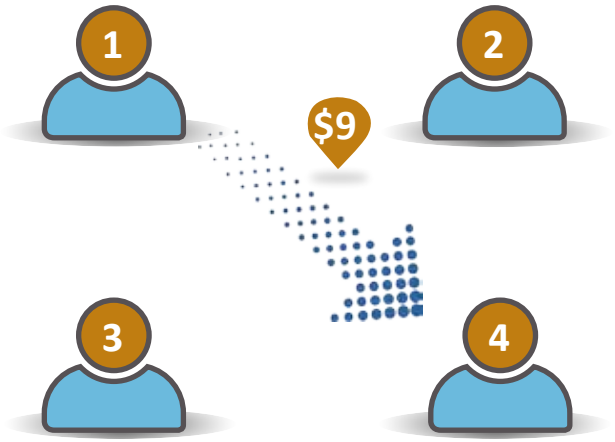


Figure 2. #1 wants to send $9 to #4.

All participants check whether #1 has enough balance to transfer $9 to #4. If #1 has enough balance, everyone makes a note of the transaction on their blank pages.

As the time passes, more transactions are made. This procedure of making notes about all occurring transactions continues until everyone runs out of space on the current page. For example, if a page has space to record 10 transactions, then everybody puts the page away as soon as the tenth transaction is made. It is time to put the page away in the ledger and get a new page to repeat the process.

2.2. SEALING THE PAGE

Before the page is put away, we have to make sure that the participants agree with all transactions written on the page and once the agreement is reached we seal the page. "Sealing the page" means that no one can make any changes to it once its copies have been put away in **everyone's** folder. Moreover, if all of the participants trust the seal that means that everyone trusts the contents of the page.

> *It is usually the third party that provides the trust that whatever they have written in the ledger will never be altered. In a distributed (that is, everyone has a copy of the ledger) and decentralized (that is, there is no third party) system, it is the seal that provides the trust.*

Before we construct the sealing mechanism and demonstrate how it ensures the validity of the transactions written on the page, we need to learn about hash functions that will play a central role in the sealing mechanism. As its name suggests cryptocurrencies make use of cryptography, and hash functions are one of cryptographic primitives used in building cryptocurrencies.[2]

A **hash function** is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values or simply hashes. Figure 3 demonstrates the hash function SHA-256 as an example.[3]

Figure 3 demonstrates that the hash function SHA-256 takes the phrase "Global Risk Institute" as its input and produces the corresponding output, that is, it maps "Global Risk Institute" to a certain hash value. Every time we feed "Global Risk Institute" to the hash function, it will always yield the same output.

Properties of the hash function ensure that this process is practically irreversible in the sense that given the output it is practically impossible to tell what the corresponding input was. The only way to figure out the input based on the hash value is to try all possible inputs. On the other hand, given the input and the output, it is easy to verify if the input leads to the output. A hash function is very easy to evaluate. Moreover, hash functions provide a very easy way to determine whether a given piece of information has been modified; one simply needs to compare the hashes of this information before and after some point in time. As we demonstrate below, this feature of hash functions is exploited in cryptocurrencies to protect past transaction records from being modified.

Figure 3. SHA-256 hash function value (output) for the phrase "Global Risk Institute" (input)

2 *In simple words, cryptography is the study of techniques for secure communication in the presence of third parties called adversaries.*

3 *The hash for "Global Risk Institute" was obtained from Xorbin online SHA256 Hash Calculator, which evaluates hash values based on Secure Hash Algorithm (SHA-256)*

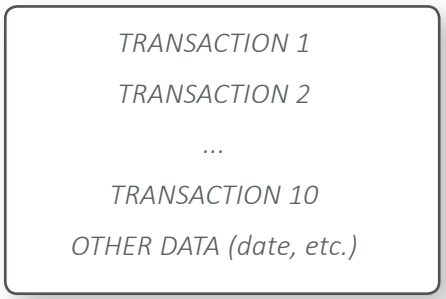
2.3. USE OF HASH FUNCTIONS IN SEALING A PAGE

Now we assume that everyone has a page with 10 transactions (see Figure 4). Next, we need a mechanism to seal the page and put it away in the ledger.

The purpose of the seal is to ensure that the content of the page was not changed.

Since the system is assumed to be decentralized, it must be somehow determined who will verify the validity of transactions and add the next block to the chain. Although there exist several schemes that determine how the next validator is chosen, we describe a widely known approach which is called Proof-Of-Work.

Figure 4. Page with transactions



According to the Proof-Of-Work scheme, all participants compete with one another in trying to solve the following puzzle:

What number should be added to the content of the page, so that the hash value of this new page content has five leading zeros?

That number, called **nonce**, is taken as the seal for the page. Figure 5 illustrates the procedure.

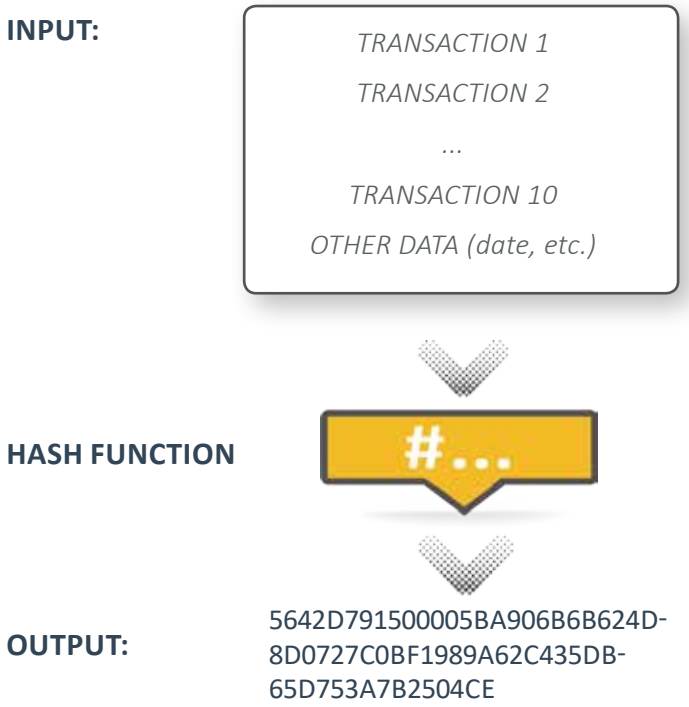
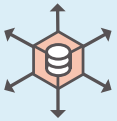


Figure 5. To seal the page, participants try to find the nonce ("solve the puzzle") that once added to the page, produces the hash value with a certain number of leading zeros.

At this point one may wonder why we cannot simply choose participants randomly instead of making them compete with each other. The problem with such a naïve approach is that the system is supposed to be pseudo-anonymous in the sense that we see only account numbers, not the identities of their holders. As a consequence, an adversary can simply create a lot of accounts to increase the chances of being chosen, thereby becoming the third party who decides what transactions are included in the ledger.



By requiring the account holders to compete with each other, we are solving the problem of randomly choosing the account holders (not account numbers) while keeping the system decentralized and pseudo-anonymous.

The only way to solve the puzzle is through trial-and-error approach: one should keep trying different nonces until the puzzle is solved. Computational resources available to each participant are critical here in the sense that the larger the computational resources, the faster one can solve the puzzle. As a result, the designed puzzle-solving mechanism comes at a cost to the participants (cost of electricity and equipment).

A very important consequence of the described sealing mechanism is that it becomes very easy to verify whether the transactions on the page have been tampered: one only needs to feed the contents of the page to the hash function and check if the output solves the puzzle. If the resulting hash does not solve the puzzle, then the transactions were altered.

To make the ledger more secure, the hash of each page is included in the next page that participants start using to record new transactions. Thus, all pages become linked and can be thought of as blocks linked in a chain, blockchain (see Figure 6).

From this point on we will use the words "page" and "block" interchangeably.

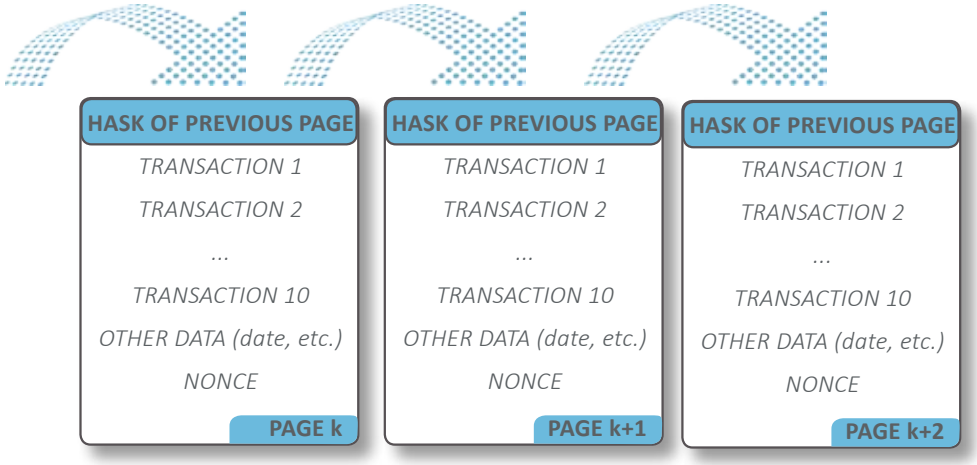


Figure 6. Blockchain (or the ledger).

How does this additional feature make the ledger more secure? Assume that an adversary changes some data in page k and obtains a new nonce that solves the puzzle for page k. The hash value of page k changes and becomes different from the hash value previously written in page k+1. To remove this inconsistency, the adversary now has to solve the puzzle for page k+1. As a result, the adversary has to solve the puzzles for all pages in the blockchain starting from page k and this presents an enormous computational challenge.

2.4. PUTTING THE PAGE AWAY INTO THE LEDGER: CONSENSUS MECHANISM

The next important question is how the participants reach consensus regarding the transactions in the blockchain. Below we describe one of the approaches.

The first one in the network who solves the puzzle announces the nonce to all participants, who then verify that all transactions in the page are valid and the nonce is indeed a solution. Assume that in our example, it is #1 who first solves the puzzle (see Figure 7).

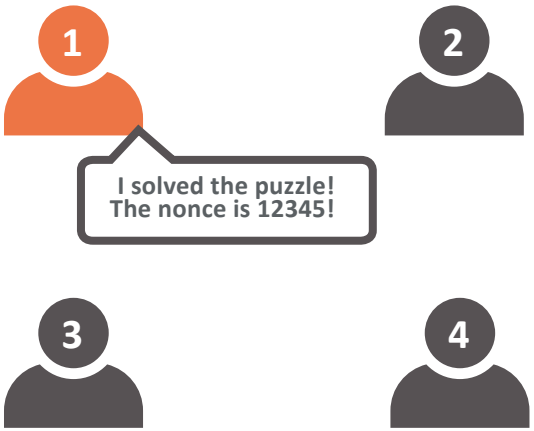


Figure 7.
#1 is the first who solves the puzzle

Once the nonce is verified by all participants, the page is considered to be sealed and everyone puts it away in their own ledger. However, what if the proposed nonce does not yield the required output for some of the participants? This could happen for a number of reasons, for instance, it could be a miswritten transaction or, perhaps, some of the participants are malicious. In such case, the following rule holds:

It is the consensus among the participants that determines what page is included in the ledger.

For the sake of illustration, assume that #1 solved the puzzle for the page with the wrong transaction. For example, #1 does not have the $9 that was announced to be transferred to #4 and therefore, the transaction is impossible. Other participants reject the page with invalid transactions by not extending the chain from that wrong page, or technically speaking, by not including the hash value of the wrong page in the next page that they are working on. And this is exactly how the consensus is reached:

Participants express their agreement with the page by including its hash value in the next proposed page. (See Figure 8)

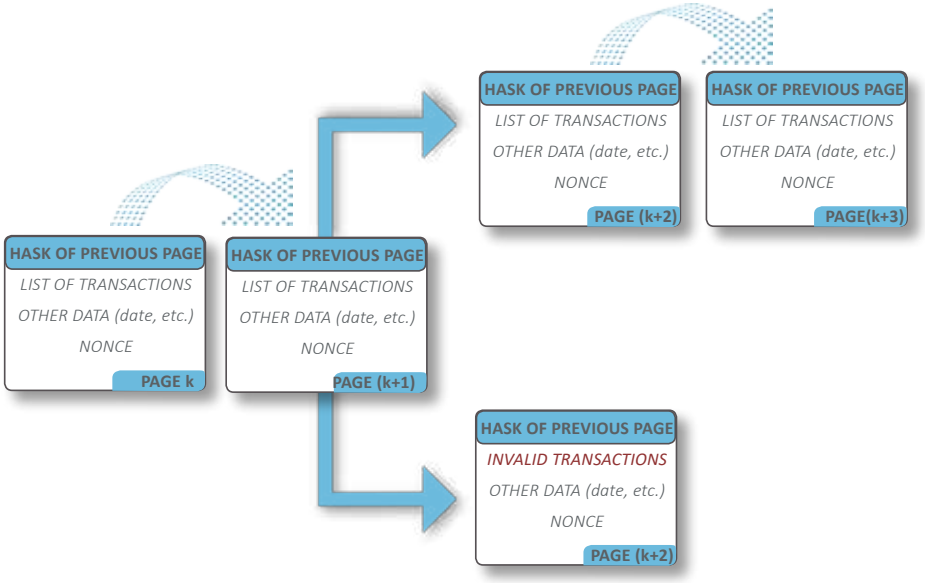


Figure 8. Participants reject the page with invalid transactions by not extending the chain from that page (the rejected page is called "orphan block" and its transactions are considered to be unconfirmed).

2.5. CONSENSUS MECHANISM AND SOLUTION TO DOUBLE-SPENDING PROBLEM

How can the described consensus mechanism prevent double-spending? First, we illustrate the double-spending problem. Assume that #1 wants to buy a book from #4 for $9. Thus, as we discussed before, he announces that he pays $9 to #4 and this transaction is included in the block k+2. When #4 notices that the transaction is in the chain, he/she delivers the book. Now assume that #1 happens to win the next block (solves the puzzle first) and instead of continuing from the block k+2, he/she continues from the block k+1, thereby rejecting the block where he pays to #4. This would imply that #1 still has $9 and #4 does not have it. However, now there are two branches in the blockchain with all blocks having valid transactions (see Figure 9).

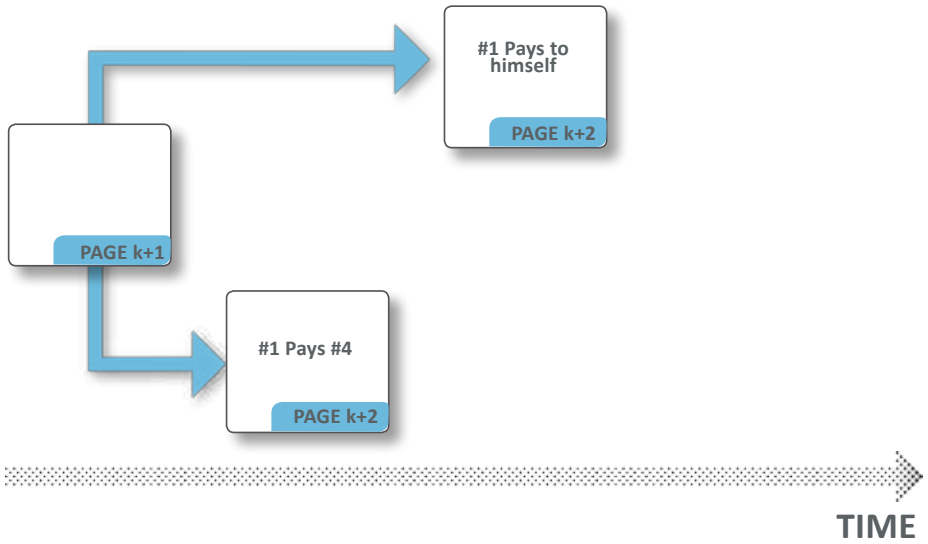


Figure 9. Double-spending attempt in the blockchain: #4 delivers the book to #1 as soon as the transaction is in the blockchain (page k+2); #1 is the first who solves the puzzle for the next block and decides to ignore the block where he pays to #4 by continuing the blockchain from block k+1.

The question becomes: from which block will the blockchain continue? There is no clear answer to this question! Of course, if #1 happens to win the next block again, then he would certainly continue from the block that allows him to double-spend $9. Otherwise, the chances are rather equal. To prevent this from happening, #4 will have to wait until the block with the transaction where he receives the payment gets enough confirmations, that is, enough blocks, say 4, built on it ensuring that the block will not end up being an orphan block. Only after this should #4 ship the book to #1 (see Figure 10).

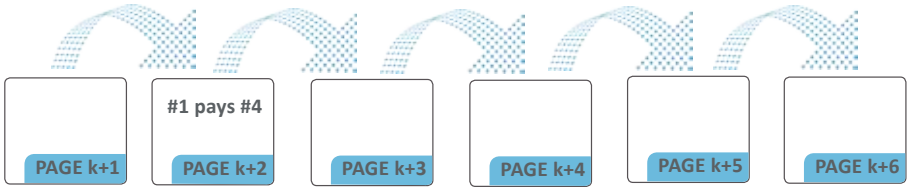


Figure 10. The transaction where #1 pays #4 gets four confirmations, that is, four blocks are built on it.

Since there could be different branches in a given blockchain, the participants need a protocol that would stipulate what chain should be considered as the main chain:

Participants always extend the longest valid branch of the blockchain.

With this rule, it can be shown that the probability that #1 is successful in building a longer parallel chain that starts from block k+1 decreases exponentially with the number of blocks that already confirmed the transaction. Thus, to be successful in its double-spending attempt, #1 will have to be the first to

solve puzzles several times in a row to be able to construct a longer branch that ignores the block where he sends $9 to #4. And this is the point where we make an assumption about the number of malicious nodes in the system:

The majority of the nodes (51%) in the network must be honest.

In summary, cryptography provides the protection against invalid transactions, whereas it is the consensus mechanism that provides the protection against double-spending.

The next question is why would the participants behave the way that we just described? We answer this question in the next section.

2.6. INCENTIVE ENGINEERING

Incentive engineering plays an important role in most cryptocurrency systems. To put it simply, a cryptocurrency should be designed in such a way that would discourage dishonest behaviour. For the Proof-Of-Work scheme, the participant that creates a block (that is, solves the puzzle first) is allowed to include a special transaction in that block. This transaction is a coin-creation transaction and the participant can also choose the recipient address of this transaction (reward for creating the block). At this point one may wonder why the block reward mechanism incentivizes honest behavior. It may appear that the participant who wins the block gets his reward regardless of whether it proposes a valid block or behaves maliciously. However, this is not true. The participant will collect the reward only if the proposed block ends up being on the consensus branch; just like every other transaction, the coin-creation transaction will only be accepted by other participants if it happens to be on this branch. This mechanism incentivises the participants to behave in whatever way they believe will get other participants to extend their blocks. Thus, if most of the network is following the protocol (extending the longest-valid-branch), it incentivises all participants to follow the protocol.

An additional incentive to behave honestly is the transaction fee that may be paid for including a transaction in a block. A participant who wants to make a transaction may be willing to pay a fee for that transaction. This fee would get paid to the participant who includes the transaction in a block. Generally, the higher the fee the faster that transaction will be included. Of course, the only way to collect the fees from all transactions in the block is when the block ends up being on the consensus branch.

Another example of incentive engineering is the Proof-Of-Stake scheme that can complement and even replace the Proof-Of-Work scheme. In simple terms, the Proof-Of-Stake scheme does away with the puzzle-solving competition. Instead, the participant who will validate the next block (add the next block to the blockchain) is chosen randomly based on the share of cryptocurrency that he/she holds. For example, a participant who owns 5% of the currency can potentially verify 5% of the blocks. Proponents of this scheme argue that undermining the currency becomes less attractive when one is holding a large stake in that currency.

3. CRYPTOCURRENCIES: *RISKS AND FLAWS*

In this section we discuss some of the flaws inherent in many existing cryptocurrencies as well as the risks that these flaws may pose if these cryptocurrencies become widely adopted.

As was mentioned in the previous section, some cryptocurrencies require participants to compete with each other. Such competitions usually require a substantial investment in hardware, for example, Application Specific Integrated Circuit (ASIC) machines designed to focus on solving puzzles. Because of these expenses, many participants decide not to participate in the puzzle-solving competition. Those who can afford the investment and decide to participate are called miners. The competition also requires considerable amounts of energy, which is why miners often locate in places where the cost of electricity is low, like Iceland, for example. Another way miners have been offsetting their costs is by spreading malware that hijacks unsuspecting internet users' computers to mine cryptocurrencies.

The arms race among miners incents them to form mining pools where the rewards are spread across the pools' members. The reason that miners form these pools is that they prefer a steady stream of smaller rewards the possibility of large but infrequent rewards that they could obtain by mining alone. The mining arms race, combined with this pooling tendency, makes the organization of a dominant mining group more likely. In fact, in 2014 the mining pool Ghash.io accounted for 50% of global computing power used for cryptocurrency mining. In this case, however, there was no damage to the system as the Ghash.io pool had benign, rather than malicious, intent.

Transaction validation time may also be an issue. For many cryptocurrencies, it can take hours, or even days, for transactions to be added to the blockchain. Transaction fees play a critical role in ensuring reasonable execution times, and as block rewards begin to run out these fees will become increasingly important.

Beyond these potential efficiency and cost-related design flaws, blockchain-based cryptocurrencies, like any internet-based technology, are also susceptible to various forms of hacking. For one, one of the most common avenues for malicious attacks is not on the blockchain itself but on centralized websites and cryptocurrency exchanges. There are now numerous examples where millions of dollars of cryptocurrencies have been stolen from these sites. In other cases, cryptocurrency websites and trading platforms themselves have been set up with the explicit intent of defrauding their customers. Even wallets, files where cryptocurrency owners store their accounts, can be compromised, manipulated, and/or stolen. Users should also be aware that there is an increasing number of cryptocurrency Trojans that hijack transactions. For example, if a user is transferring coins from one account to another account, the Trojan will replace the destination account number with its own. If the user does not catch the mistake, the coins will be transferred to the Trojan's account and cannot be recovered.

More generally, as with any cryptographic solution, the blockchain is susceptible to programming bugs and poor private key security, both of which can compromise the whole system. There are several instances, in fact, in which hackers manipulated cryptocurrency mining and trading software to steal coins from users. Moreover, the consistent, predictable format of the blockchain may make it more susceptible to crypto-attacks. Consequently, cryptocurrency users should always use the latest, most secure ciphers to encrypt their wallets and other data.

Each cryptocurrency has its own set of inherent risks and flaws. There is still a high degree of competition between cryptocurrencies and a high amount of uncertainty around which, if any, cryptocurrency has the potential for long term viability.

4. CONCLUSION

In this paper we provided a non-technical description of blockchain technology using cryptocurrencies as an example. Despite the enthusiasm for blockchain's potential, one should also understand this technology's weaknesses when applied to cryptocurrencies. Ongoing vigorous competition among existing cryptocurrencies indicates that a viable cryptocurrency has yet to appear, so consumers and financial institutions should be wary of investing heavily in one cryptocurrency over another.

5. REFERENCES:

1. *Halaburda, H., Sarvary, M.: Beyond Bitcoin: The Economics of Digital Currencies. Palgrave Macmillan, 2016.*

2. *Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016.*