Vulnerabilities and Security Breaches in Cryptocurrencies

Sigurdsson, Gudmundur; Giaretta, Alberto; Dragoni, Nicola

Published in:
Proceedings of 6th International Conference in Software Engineering for Defence Applications - SEDA 2018

Link to article, DOI:
10.1007/978-3-030-14687-0_26

Publication date:
2020

Document Version
Peer reviewed version

Vulnerabilities and Security Breaches in Cryptocurrencies

Gudmundur Sigurdsson[1], Alberto Giaretta[2], and Nicola Dragoni[1,2]

[1] DTU Compute, Technical University of Denmark, Denmark
s172168@student.dtu.dk, ndra@dtu.dk,
[2] Centre for Applied Autonomous Sensor Systems (AASS), Örebro University, Sweden, alberto.giaretta@oru.se

Abstract. Nowadays, 1375 different cryptocurrencies exist, and their market value totals up to $444.8 billion, at the time of writing. The interest revolving around cryptocurrencies is constantly growing, and this hype caused an increase of criminal attacks on various cryptocurrencies. In this paper, we cover the main aspects that concern cryptocurrencies vulnerabilities and related security breaches. Then, we propose possible solutions to prevent them, or to decrease the attackers' profit margins by increasing the costs they have to face, in order to strike some of these attacks. Alongside, we briefly describe a few attacks that have occurred in the past.

1 Introduction

In 2009, Satoshi Nakamoto introduced on the market the first cryptocurrency in history, Bitcoin [4]. Even though Bitcoin is still the most popular cryptocurrency, with a trading volume of $ 7.1 billion a day and 39.8% market share [7], at time of writing more than 1500 different cryptocurrencies have been created. One of the main alternatives is Ethereum, which holds a daily trading volume of $ 2 billion.

Thanks to its peer-to-peer protocol, Bitcoin is a fully distributed and decentralized currency that achieves trust without relying upon a trusted third party. Blockchain is the fundamental underlying technology, a linked list of information stored in blocks that, combined with a peer-to-peer (P2P) protocol, ensures distribution and decentralization. In the case of cryptocurrencies, currency transactions are the stored information. Apart from data, each block holds a hash of the previous one, as well as a timestamp, in order to enforce the chain validity. Indeed, any attempt to edit one of the blocks would invalidate hashes validity and, consequently, the whole blockchain [21].

It is possible to separate Bitcoin users into two different groups, regular users and miners. We describe hereby the two roles as separate entities, but a user can equally perform both of them. Firstly, regular users manage their bitcoins through a digital wallet, as like as they were using a traditional electronic home banking. In order to access the data, each user holds a private key, which ensures that no third party can access users' money. As we previously said, no central

authority has power over Bitcoin, which means that if the private key is lost (and no backup was done) the bitcoins are lost forever. No third party can re-issue a password, reset an account or operate in any way over others' wallets.

Secondly, mining is the process where blockchain progresses and network generates new units of Bitcoin. Miners compete to solve complex mathematical problems by dedicating their computational power to this purpose. By solving these problems, they confirm the validity of Bitcoin transactions and they are rewarded with a fixed number of bitcoins [22], plus all the fees that users attached to their issued transactions as an incentive to choose their transaction. Whenever the amount of mined blocks reaches half of the number of the remaining minable blocks, the reward decreases by half. In the beginning, the fixed reward was 50 BTC (bitcoins) for each new block created, and the current reward equals 12.5 BTC per block. This halving mechanism will keep going on, until the upper limit of 21 million BTC is reached [18]. At that point, the whole Bitcoin network will rely exclusively upon the transaction fees.

When trying to mine a block, a miner must begin with collecting new transactions into the block. One the block has been created, a nonce is chosen and a pre-defined hash algorithm is applied to the block. The goal is to obtain a hash with a targeted number of zeros, so the miner keeps on increasing the nonce and performing the hashing over the block, until they hopefully find a good hash. In case this happens, the miner broadcasts the solution, which is checked by the other participants. In case the solution is correct and the block correctly formed, the miner receives the reward and the block is appended to the blockchain. Difficulty is adjusted automatically by the system, in order to achieve a ratio of 1 new block per 10 minutes, on average [22].

Blockchain is believed to be immutable and tamper-proof by design but, even though it is strongly resilient, this claim were proved to be incorrect. In this paper, we aim to explain the vulnerabilities that can be found in cryptocurrencies and propose solutions to prevent them from happening, along with some of the biggest security breaches that have occurred in the past. This paper revolves around Bitcoin, since it is the first cryptocurrency that appeared on the market, and even the most popular one.

2 Related Work

Bucko et al. [21] enlist various issues that can affect cryptocurrency trust. They suggest that cryptocurrencies would become more secure, if businesses that utilize this technology would follow the standards drafted by the CryptoCurrency Certification Consortium.

Latif et al. [30] state that the online environment could cause a security breach in cryptocurrencies. There is no security for the users' savings, since there is no third party to which users can turn to, in case problems with their money arise. They also state that cryptocurrencies depend on the power of speculations, investors can therefore over- or under- value the cryptocurrencies, which affects

the market price. They also claim that the public nature of transaction records exposes users to de-anonymizing techniques.

Kaushal [29] talks about how selfish mining and malleability vulnerabilities affect Bitcoin. The author addresses the selfish mining problem and shows how a backward compatible approach was introduced, in order to solve it. Feder et al. [26] measured the impact of Distributed Denial of Service (DDoS) attacks on Bitcoin exchanges. They chose to use kurtosis (which measures whether the data is light- or heavy-tailed, with respect to a regular distribution) and skewness (which measures eventual lack of symmetry) for day-to-day transactions. They found out that when DDoS attacks occurred both kurtosis and skewness decreased. Therefore, the volume of day-to-day transactions changes and this means that less large transactions occur during such attacks.

Vasek et al. [31] studied 142 different DDoS attacks, mentioned on the website bitcointalk.org. The chosen timeline went from February 2011 to October 2013. From 2940 different pages, the team found out that 142 different DDoS attacks were performed on Bitcoin, during the chosen period. Vyas and Lunagaria [32] claim that storage, mining and transaction processes are the main vulnerable phases of Bitcoin. They state that, in order to increase security during the mining process, Bitcoin protocols need to change their framework. To operate this modification, roughly 80% of Bitcoin users need to agree on the change.

Conti et al. [22] thoroughly evaluated Bitcoin, with regards of both security and privacy issues. They give a detailed overview about the protocol, as well all the documented vulnerabilities together with possible countermeasures. Furthermore, the authors summarize the open challenges and suggest the aspects future work should focus on, in order to solve the current issues.

3 Vulnerabilities and Attacks

The heaviest loss in Bitcoin history happened in February 2014, when MT. Gox, a Bitcoin market in Tokyo, lost 850.000 BTC that totalled $474 million at that time. At the time of writing, taken into consideration the current market price, the losses would have totalled more than $7 billion. Later on, MT. Gox stated that the incident was caused by a transaction malleability, a known security issue [5] that we describe later in this section.

Another example is the attack performed on the Decentralized Autonomous Organization (DAO), a venture capital fund that enabled investors to directly fund proposals through smart contracts, based on the Ethereum platform. The attack led to a theft of 3.6 million ether coins, worth $3.1 billion accordingly to the current market price. The attackers exploited a loophole, which enabled them to recursively transfer funds from a parent account to a child, without updating the parent balance [2].

Apart from these two examples, there are many other vulnerabilities in cryptocurrencies. In this section, we describe the most important ones.

3.1 Selfish Mining

There are two types of miners: the honest ones, and the selfish ones. It does not matter if an honest miner works as an individual, in a single group or in a number of different groups. The main goal of selfish miners is to force the honest ones to waste their computational power on the stale public branch. Due to design reasons, it is possible (even though unlikely) that a blockchain splits in two concurrent branches. To solve this paradox, Bitcoin and other blockchain protocols enforce the longest chain as the correct one, thus invalidating all the blocks mined in the shortest parallel chain. The selfish miners leverage this characteristic, they keep private all the blocks and work on their secret branch. As soon as the honest miners are about to catch up, in terms of blockchain length, with the selfish miners, the latter group releases the secret chain. By doing so, the selfish miners nullify all the honest blocks and reclaim all the reward for themselves [25].

Not all cryptocurrencies are prone to selfish mining attacks. As an example, Ripple was created from the beginning with 100 billion XRP (the Ripple currency), which are not minable and are also wasted after the first usage. The company idea is to have possession of half of it and let the other half into circulation [1]. The only way to acquire this cryptocurrency is through exchange with other currencies, therefore Ripple is free from all attacks relating to the mining process.

3.2 Wallet

In order to manage their currency, whether it is to store it or issue transactions, users need a wallet. There are five different types of wallets, divided into three main categories: hardware, software (web, desktop, mobile), and paper wallet. Wallets need to be encrypted and an offline back-up is highly desirable: in case something happens, the facility that keeps the back-up can help its users to restore their wallets.

When it comes to choose a wallet solution, it is good to follow some criteria: the interface should to be user-friendly, backups have to be easy to create, security has to be taken into account, development team should actively support the wallet, and so on. As an example, if users want to be completely safe from attacks while the currency is in storage, they should get a paper wallet, which is also the cheapest wallet to choose [32]. Furthermore, the hardware wallet is a better choice than the software one, since it does not require to be continuously connected to the Internet. It does not matter what kind of cryptocurrency you are going to store in a wallet, wallets are all similar. Therefore, a user should always follow the same criteria when choosing their wallet [3].

Recently, a hacker stole 153.000 Ether (the Ethereum currency), worth almost $131.8 million dollars at the current price, by manipulating a vulnerability in Ethereum wallet. The attacker exploited a bug in Parity Ethereum client to withdraw currency from multi-signature wallets. Multi-signature wallets, also known as multi-sig, are accounts where numerous individuals democratically

control the currency flow. A transaction is issued if, and only if, a pre-defined number of users sign it with their own private key [9]. Considering the cryptocurrencies value, alongside the general robustness of blockchains, hackers are focusing more and more on attacking directly users' wallets. As an example, as shown in Section 3.12, attackers use social engineering techniques to gain victims' trust and steal their wallets [12].

3.3 Distributed Denial of Service (DDoS) Attack

DDoS attacks aim to make a device (or a network) unreachable to users, for example through packet flooding techniques. These attacks are among the most common ones that affect cryptocurrencies, mainly because they are highly disruptive and relatively cheap to perform. The main targets of DDoS attacks, with respect to cryptocurrencies, are the currency exchange platforms and the mining pools.

As mentioned earlier, researchers [31] enlisted 142 different attacks in their 33 months timeline. Most attacks target mining pools, currency exchanges, electronic wallets, and financial services, but the most popular ones are performed on large mining pools and currency exchanges. These are more popular than others, since the attacker is likely to earn a larger amount of money than attacking small mining pools, or individuals. As an example, a trading and exchange platform called BTC-e experienced reiterated DDoS attack, during 2016 and 2017. These attacks overloaded the whole system, at such a point that it was offline for hours [6].

Moreover, mining pools are often target of DDoS attacks performed by other mining pools, which try to impede competitors from succeeding. Anti-DDoS services popularity varies between categories, but overall are only used by roughly 20% of Bitcoin pools. As expected, these protections are more popular among larger mining pools, which are more likely to experience attacks [31]. Another study [28] explored the trade-off between two different strategies to create bitcoins. These strategies are called construction and destruction. The construction paradigm is when mining pools devote more resources to increase their computing power, thus their chances of mining the next blocks. The destruction paradigm is when a mining pool chooses to invest resources into a DDoS attack, in order decrease the success of competing mining pools.

3.4 Malleability Attack

In malleability attacks, the attacker tries to modify the hash of transactions and pretend he never received the money, in order to deceive his victims and lead them to issue the same transaction a second time. First of all, the victim issues a legitimate transaction to the attacker (e.g., for a purchase). As soon as the attacker detects the transaction in the network, he modifies its signature, which creates a different transaction hash ID. After this, the attacker issues the altered transaction in the network. In this moment, both the legitimate transaction and the forged one are waiting for confirmation. If the forged transaction is confirmed,

the legitimate is not acceptable anymore (therefore, it is discarded) and the attacker can try to persuade the victim to issue the transaction again [24]. The malleability attack should not be confused with the double spending attack. In the latter case, the coins are automatically double spent, whereas the former one can lead to a second spending phase if, and only if, the attacker succeeds in tricking the victim.

Malleability attacks can also lead to DoS attacks. If the attacker issues many forged transactions in the transaction pool, the miners have to spend a lot of time in verifying (and discarding) all these false transactions [22]. Bitcoin is prone to such attacks, which can be eliminated by slightly modifying the protocol [20]. Indeed, in 2015 Bitcoin experienced a malleability attack that succeeded in changing the hash of many transactions. The sums and the related recipients were not affected, but it took a long time before all the transactions were finally confirmed [13].

3.5 Double Spending Attack

Double spending happens when a malicious entity spends the same currency more than once. In a typical cryptocurrency like Bitcoin, when a transaction is issued, it goes in the transaction pool waiting to be confirmed as part of a block. As an example, if a merchant does not wait for the final confirmation of the incoming transaction, a malicious customer can try to spend the same coins by issuing another transaction to another merchant. When the confirmation happens, one of the two conflicting transactions is cancelled, since a coin can be spent only one time, but the attacker would have actually got more goods than he paid for.

Merchants are recommended to wait that, at least, six more blocks are mined after the block containing their transaction, before processing the order they were paid for. This time slot is enough to avoid the risk of a cancelled transaction [22].

3.6 Dropping Transactions

Transactions can be dropped when a miner deliberately does not pick up some transactions from the transaction pool. Someone suggested that this might become a problem, since that a miner, aiming to speedup its mining processes, could deliberately choose to drop all the transactions and mine empty blocks. As aforementioned in Section 1, in order to increase the chances that a miner picks up a transaction, the issuer attaches a fee. These fees seem profitable enough to avoid deliberate dropping.

Obviously, the higher the fee, the more probable a transaction is chosen. It is clear to see that a transaction has higher chances to be dropped if the attached fee is not profitable enough for the miner. As long as the transaction is not picked up from the transaction pool, it remains unconfirmed until a miner eventually chooses it [17].

3.7 51% Attack

The idea behind a decentralized cryptocurrency such as Bitcoin, is that no entity should have the power to take non-democratic decisions. A PoW protocol is perfect, under the initial assumption that miners work on they own, but mining pool can endanger this system. The more a mining pool grows, the more decisional weight it has over the blockchain it is mining. If, at any point, a pool achieves the 51% of the total computational power working on the blockchain, it can effectively take full control. The pool can allow its members to double spend their coins, prevent competing pools to mine the blockchain, and even impede the confirmation of transactions. Even without achieving the 51% of computational power, an important mining pool can still damage a cryptocurrency network. As an example, a mining pool that controls around 30% of computational power can still perform some of the aforementioned attacks [32].

The Proof of Stake (PoS) protocol makes these attacks more difficult than PoW-based cryptocurrencies. The core point of PoS is the coin age, measured by multiplying the number of coins per holding days. In PoW solutions, it is sufficient for the attacker to gain the 51% of resources, in order to control the network. Instead, with PoS ownership is not enough, as the attacker needs to hold the resources for a considerable amount of time. Furthermore, to avoid the selfish mining incentive in PoS networks, researchers [27] proposed to set an upper limit on coins age, after which the coin age is reset.

3.8 Timejacking Attack

Timestamps are essential to validate blocks in the Bitcoin protocol and, through this multi-step sophisticated attack, an attacker can increase the chances of performing a double spend attack [18]. First of all, an attacker can slow down the median time of its target by sending it wrong timestamps. The time can be skewed up to 70 minutes, accordingly to the protocol; over this threshold, the time reverts to system time. This can easily be done, since a few Tor nodes that wrongly report the time are enough to succeed in altering the victim time. On the other hand, to perform a timejacking attack the majority of the network has to be speeded up 70 minutes, which requires far greater resources than simply altering the time for a single node. At this point, if the attacker succeeds, the difference between the victim and the rest of the network is 140 minutes.

Keeping in mind that Bitcoin nodes are designed to reject blocks which differ more than 120 minutes from the local time, the attacker aims to create a "poison pill" block, with a timestamp 190 minutes ahead of the real time. By doing so, the block will be accepted from the speeded up network (since it is exactly within the 120 minutes threshold) but the victim will reject it, since the block time is 260 minutes far ahead the node time. At this point, the chains fork and the target is isolated from the normal Bitcoin network operations. Since the time difference between the new blocks and the local time is 140 minutes, all the legitimate blocks are automatically rejected without checking the contents.

Until the victim eventually catches up with the rest of the network (e.g., after a clock reset, an operation intervention or an unaffected node that pushes a correct timestamped block), the attacker can feed the node fake confirmations and double spend its own coins with the victim. If the victim is a miner, this results in a DoS attack, since it is unknowingly wasting computational power on a stale fork of the chain, while the majority of the network is normally progressing on another chain.

One of the possible solutions to this vulnerability, is to use the system time both when a new block is created and when the timestamps are compared. To further mitigate it, the acceptable time range could be tightened up from 70 minutes to 30 minutes leading to a restricted attack window, but this exposes the network to problems in case some nodes do not correctly handle daylight savings. Another suggestion would be to use the median blockchain time when validating blocks, as it already happens for the lower bound of the protocol. Indeed, Bitcoin protocol forces a node to reject any block which timestamp is earlier than the median of the previous 11 blocks. Adopting a similar strategy for the upper bound might resolve the timejacking vulnerability.

3.9 Sybil Attack

In a sybil attack, a malicious attacker fills the network with fake entities, and attempts to take over the regular network activities. Without adequate countermeasures, an attacker could try to confirm fake transactions or disconnect the victim from the network by not forwarding transactions and blocks. A malicious adversary could also forward only fake blocks, in order to attempt to double spend coins on the victim.

One of the main characteristics of cryptocurrencies is anonymity, therefore it is mandatory that anonymous validation algorithms are used (i.e., enforcing to link a miner to a physical person or organization is not an option). The Bitcoin Proof of Work (PoW) algorithm prevents the sybil attack for the mining processes. No matter how many virtual miners an attacker creates, the physical computational resources cannot be virtually multiplied, which entails that creating dozens of fake miners does not increase the chances to mine new blocks. PoW has some severe drawbacks, though, such as inefficiency and expensiveness [33].

To prevent sybil attacks and solve the Know-Your-Customer (KYC) problem, the Proof of Individuality (PoI) algorithm was proposed [14]. Based on Ethereum, the assumption is that a person can attend only one meeting at a time. PoI pairs users in random small groups of 5 people and a 10 minutes video conference starts for all the groups, at the same time. During this time the users have to actively engage, in order to prove they are attending to only one conference. After the, call the users within the same groups validate (or not) the others and each validated user receives an anonymous unique token. This proposal seems particular useful for voting scenarios. The operations happen at a specific time and, after the vote is cast, the token is destroyed [8].

3.10 Spam Transactions

In some cryptocurrencies, such as Bitcoin and Litecoin, the blocks have an upper size limit of 1MB [23] but it is not a rule for all cryptocurrencies. As an example, Ethereum do not have block size limits but a limit to the number of transactions [16], called gas limit. That being said, the results in both cases is that the number of maximum transactions per block is limited.

This inherent limit exposes the blockchain to DoS attacks, in the form of various flooding attacks. A malicious attacker can send multiple (and economically non-relevant) transactions, aiming to fill up the transactions pool and delay the legitimate transactions. In 2015, a set of unknown actors allegedly performed a flood attack on Bitcoin network [23], in order to convince the community that the 1MB size limit should be raised.

One way to counter flood attacks is to force a monetary commitment on the payer, whenever a transaction is issued. By doing so, the attacker eventually runs out of currency and resources to buy new coins. Bitcoin, Ripple, and many other cryptocurrencies, charge network transactions fees on their users [10, 19], which protects the network from this issue.

3.11 Segmentation

Segmented networks should perfectly work even if the connection between them is poor. If no means of communication exits, the network segments and the blockchain forks. When the connection is restored, accordingly to the Bitcoin protocol, the longest chain is automatically chosen as the correct one and all the transactions in the shortest chain are put back into the transaction pool. As long as a chain does not fork more than 120 blocks, all the transactions are still valid, even though they start again with a 0\unconfirmed status. If the fork is longer, such transactions are definitively invalid and unrecoverable.

A malicious attacker could take advantage of a segmented network to double spend coins on both blockchains, however if the attacker is able to connect to both blockchains, almost certainly even legitimate users can do the same. Even though it is unlikely that someone can leverage this characteristic to double spend coins [15], keeping track and evaluating a sudden drop, in numbers, of legitimate peers might help an honest user to avoid frauds.

3.12 Social Engineering

Social engineering attacks leverage the weaknesses of human psychology, which makes hard to counteract them through software and hardware solutions. This is the reason why social engineering attacks rank high, amongst the types of security issues. The only weapon against social engineering attacks is to educate the users to recognize and avoid attacks attempts. Social engineering techniques take advantage of human greed and curiosity, as well as many other emotions, which entails a wide diversity of possible attacks and related countermeasures.

Attackers can aim to steal login credentials of users' wallets, as well as infect third-party systems and use their resources for mining purposes.

As an example, in early December 2017 the Bitcoin mining marketplace NiceHash, accordingly to their head of marketing, experienced a sophisticated social engineering attack to their systems that led to 4700 BTC stolen (worth roughly $49.28 million) [12]. In another case, a malware called RETADUP infected a number of Israeli hospitals, aiming to spread a cryptocurrency mining software [11] and directly monetize from the infections.

4 Conclusion

The interest for cryptocurrencies, and consequently their economic value, has risen above all expectations in a few years. Bitcoin was the first cryptocurrency on the market and is still the most popular one, but many others have been proposed, with different degrees of success. It is clear to see that higher economic value, combined with the anonymous nature of the currency, entails higher interest from criminal parties. Cryptocurrencies are not only fertile soil for buying and selling illegal goods, but also an attractive target for currency thieves. In this paper, as shown in Table 1, we presented a number of different cryptocurrencies vulnerabilities, as well as some solutions and countermeasures. Moreover, we presented actual attacks perpetrated on different entities, and the severe economic impact that such attacks had on their victims.

New and intriguing ideas emerge every day from the cryptocurrency field, but hackers are quick to respond and adapt to new technology. On the one hand, cryptocurrencies foundations lay on the Internet and this makes them naturally prone to different vulnerabilities. On the other hand, blockchain is the promising core technology that could help to solve multiple trust problems in the present Internet architecture. One thing is sure, though: the exciting battle between attackers and defenders is unlikely to finish anytime soon.

References

1. 10 things you need to know about ripple. https://www.coindesk.com/10-things-you-need-to-know-about-ripple/
2. $55 million in digital currency stolen from investment fund. https://www.bankinfosecurity.com/55-million-in-digital-currency-stolen-from-investment-fund-a-9214
3. Best ethereum wallets 2017: Hardware vs software vs paper. https://blockonomi.com/best-ethereum-wallets/
4. Bitcoin: A peer-to-peer electronic cash system. https://coinmarketcap.com/all/views/all/
5. Bitcoin hack highlights cryptocurrency challenges. https://www.bankinfosecurity.com/bitcoin-hack-highlights-cryptocurrency-challenges-a-9305
6. Bitcoin, litecoin exchange platform under ddos attack, security inadequate. https://cointelegraph.com/news/bitcoin-litecoin-exchange-platform-under-ddos-attack-security-inadequate

Table 1. Comparison of Cryptocurrencies Attacks

Type of attack	Targets	Description	Effects	Solutions
Selfish Mining	Mining process	Takes advantage of honest miners	Honest miners waste their resources on a stale chain	Backwards compatible modification [25]
Wallet	Businesses and regular users	Private key is lost or deleted	Loss of every content in the wallet	Have a backup of the wallet
DDoS Attack	Miners, users, network and services	Makes devices or networks unreachable to their users	Isolate targets	Proof of activity (PoA)
Malleability Attack	Transaction process	Forge transactions, almost identical to the original copy	DDoS. Users can be tricked into re-issuing transactions	Modify the vulnerable protocols
Double Spending Attack	Transaction process	Spend the same currency on different transactions	Buying multiple things with the same coins	Confirm a transaction only after 6 valid blocks
Dropping Transactions	Transaction process	Miners might never choose some transactions	Transactions are never issued	Attach reasonable fees for the miners
51% Attack	Mining and currency exchange process	Mining pools have more than 50% of the power	Double spending and denial of service	Proof of Stake (PoS)
Timejacking Attack	Mining and transaction process	Change the blocks timestamps	Miners work on a stale chain, users prone to fake transaction confirms	Use system time, and narrow time ranges
Sybil Attack	Mining process	Fill the network with fake miners	DoS, double spending, and selfish mining	Adopt a resource-bound protocol (such as PoW, or PoI)
Spam Transactions	Mining and transaction process	Flood the pool with multiple transactions	Delays and backlogs	Charge a fee for every transaction
Segmentation	Mining and transaction process	Segment the network and prevent communications	Double spending	Evaluate abrupt loss of peers
Social Engineering	Miners, businesses, and regular users	Steal sensitive information	Money and identity theft	Educate users to identify potential frauds

7. Cryptocurrency market capitalizations. https://coinmarketcap.com/all/views/all/
8. Ethereum based proof-of-individuality prevents sybil attacks. https://decentralize.today/ethereum-based-proof-of-individuality-prevents-sybil-attacks-9757864bbf61
9. Hacker uses parity wallet vulnerability to steal $30 million worth of ethereum. https://www.bleepingcomputer.com/news/security/hacker-uses-parity-wallet-vulnerability-to-steal-30-million-worth-of-ethereum/
10. Introducing ripple. https://bitcoinmagazine.com/articles/introducing-ripple/
11. New RETADUP variants hit south america, turn to cryptocurrency mining. https://blog.trendmicro.com/trendlabs-security-intelligence/new-retadup-variants-hit-south-america-turn-cryptocurrency-mining/
12. Nicehash hacked at peak btc prices, loses $64 million's worth of bitcoin. https://cryptovest.com/news/nicehash-hacked-at-peak-btc-prices-loses-64-millions-worth-of-bitcoin/
13. The ongoing bitcoin malleability attack. https://cointelegraph.com/news/the-ongoing-bitcoin-malleability-attack
14. Proof of identity on ethereum (or the kyc problem). https://blog.oraclize.it/proof-of-identity-on-ethereum-or-the-kyc-problem-f4a9ee40af21
15. Re: Anonymity. bitcoin forum. https://bitcointalk.org/index.php?topic=241.msg2071\#msg2071
16. Re: Maximum block size? - ethereum community forum. https://forum.ethereum.org/discussion/1757/maximum-block-size
17. Re: What is the incentive to collect transactions. bitcoin forum thread. https://bitcointalk.org/index.php?topic=165.msg1595\#msg1595, accessed: 2018-02-26
18. Timejacking & bitcoin. http://culubas.blogspot.dk/
19. Transaction fee historical chart. https://bitinfocharts.com/comparison/transactionfees-btc-eth-bch-ltc-dash-xmr-vtc-aur.html

20. Andrychowicz, M., Dziembowski, S., Malinowski, D., Mazurek, Ł.: On the malleability of bitcoin transactions. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) Financial Cryptography and Data Security. pp. 1–18. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
21. Bucko, J., Palova, D., Vejacka, M.: Security and trust in cryptocurrencies (2015)
22. Conti, M., E, S.K., Lal, C., Ruj, S.: A Survey on Security and Privacy Issues of Bitcoin. ArXiv e-prints (Jun 2017)
23. Dan, M., David, B., David, A., Miguel, M.S., Yike, G., J., K.W.: Visualizing dynamic bitcoin transaction patterns. Big Data 4(2), 109–119 (2016), https://doi.org/10.1089/big.2015.0056, pMID: 27441715
24. Decker, C., Wattenhofer, R.: Bitcoin transaction malleability and mtgox. In: Kutyłowski, M., Vaidya, J. (eds.) Computer Security - ESORICS 2014. pp. 313–326. Springer International Publishing, Cham (2014)
25. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) Financial Cryptography and Data Security. pp. 436–454. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
26. Feder, A., Gandal, N., Hamrick, J.T., Moore, T.: The impact of ddos and other security shocks on bitcoin currency exchanges: evidence from mt. gox. Journal of Cybersecurity 3(2), 137–144 (2017), +http://dx.doi.org/10.1093/cybsec/tyx012
27. Gao, Y., Nobuhara, H.: A proof of stake sharding protocol for scalable blockchains. In: Proceedings of the 14th APAN Research Workshop 2017 (2017)
28. Johnson, B., Laszka, A., Grossklags, J., Vasek, M., Moore, T.: Game-theoretic analysis of ddos attacks against bitcoin mining pools. In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) Financial Cryptography and Data Security. pp. 72–86. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
29. Kaushal, R.: Bitcoin: Vulnerabilities and attacks. Imperial Journal of Interdisciplinary Research 2(7) (2016), http://www.imperialjournals.com/index.php/IJIR/article/view/1238
30. Latif, S., Mohd, M., Mohd Amin, M., Mohamad, A.: Testing the weak form of efficient market in cryptocurrency. Journal of Engineering and Applied Sciences 12(9), 2285–2288 (2017)
31. Vasek, M., Thornton, M., Moore, T.: Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) Financial Cryptography and Data Security. pp. 57–71. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
32. Vyas, C.A., Lunagaria, M.: Article: Security concerns and issues for bitcoin. IJCA Proceedings on National Conference cum Workshop on Bioinformatics and Computational Biology NCWBCB(2), 10–12 (May 2014), full text available
33. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A.B., Chen, S.: The blockchain as a software connector. In: 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA). vol. 00, pp. 182–191 (April 2016), doi.ieeecomputersociety.org/10.1109/WICSA.2016.21