IFERP
connecting engineers... developing research

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

Strategic Quality Management – An Annotated Review

Gaurav Sharma
Rayat Bahra University

***Abstract:* - Few people in the blockchain industry have marked the blockchain has become over popular but in reality the technology has limitations and also is inappropriate for many digital communications. Blockchain requires a large network of users to maintain it’s ecosystem, however It becomes more difficult to reap the full benefit if a blockchain is not a robust network with a widely distributed grid of nodes. The blockchain can only executes about seven transactions per second. The biggest security flaw in blockchains is if more than half of the computers executing as nodes to instruct and service the network tell a lie, the lie will become the truth in just a blink of eye. This is marked as ‘51% attack’ and was highlighted by Satoshi Nakamoto when he inaugurated the bitcoin. This is the reason the bitcoin mining pools are monitored closely by the community and ensuring no one unknowingly gains such network influence. Politics has been a biggest restriction in the avoidance of blockchain as the protocols offer an opportunity to digitize governance models, and the miners are essentially forming another type of incentivised governance model, so there have been tremendous opportunities for public disagreements between different community sectors.**

Key words: Cryptocurrency, Blockchain, Mining, Privacy, Security

1. INTRODUCTION

Since the entry of Bitcoin in 2009, its underlyingtechnique, blockchain, has looks promising application prospects and attracted lots of attention from industry and academia. Being the first cryptocurrency, Bitcoin was rated as the top performing cur- rency in 2015 and the best performing commodity in 2016, and has more than 300K confirmed transactions daily in May, 2017. At the same time, the blockchain technique has been applied to many fields, including medicine, economics, Internet of things, software engineering and so on. The introduction of Turing complete programming languages to activate users to develop smart contracts running on the blockchain marks the start of blockchain 2.0 era. With the decentralized con- sensus mechanism of blockchain, smart contracts allow mutually distrusted users to complete data exchange or transaction without the need of any third-party trusted authority. Ethereum is now (May of 2017) the most widely used blockchain supporting smart contracts, where there are already 317,506 smart contracts and more than 75,000 transactions happened daily. Since blockchain is one of the core technology in FinTech (Fi- nancial Technology) industry, users are very concerned about its security. Some security vulnerabilities and attacks have been re- cently reported. Loi et al. invents that 8,833 out of 19,366 existing Ethereum contracts are vulnerable. Note that smart contracts with security vulnerabilities may lead to financial losses. For in- stance, in June 2016, the criminals attacked the smart contract DAO by exploiting a recursive calling vulnerability, and stole around 60 million dollars. As another example, in March 2014, the criminals exploited transaction mutability in Bitcoin to attack MtGox , the largest Bitcoin trading platform. It caused the collapse of MtGox , with a value of 450 million dollars Bitcoin stolen. Although there are some recent studies on the security of blockchain, none of them performs a systematic examination on the risks to blockchain systems, the corresponding real attacks, and security enhancements. The closest research work to ours is that only focuses on Ethereum smart contracts, rather than popular blockchain systems. From security programming perspec- tive, their work analyzes the security vulnerabilities of Ethereum smart contracts, and provides a taxonomy of common program- ming pitfalls that may lead to vulnerabilities. Although a series.

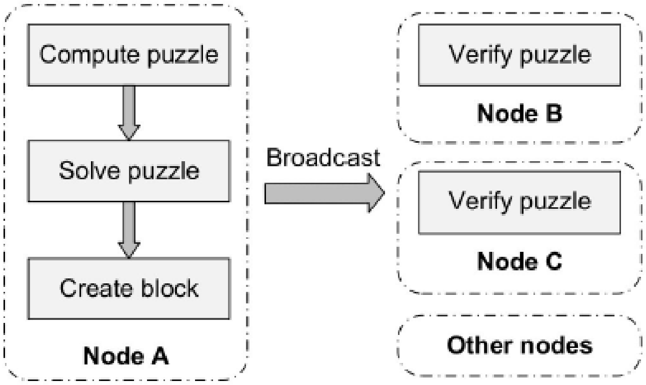


Fig. 1. PoW consensus mechanism.

of related attacks on smart contracts are listed in, there lacks a discussion on security enhancement. This paper focuses on the security of blockchain from more comprehensive perspectives. The main contributions of this paper are as follows: (1) To the best of our knowledge, we conduct the first systematic examination on security risks to popular blockchain systems. (2) We survey the real attacks on popular blockchain systems from 2009 to the present (May of 2017) and analyze the vulnerabilities exploited in these cases. (3) We summarize practical academic achievements for enhancing the security of blockchain, and suggest a few future directions in this area. The remainder of this paper is organized as follows. Section 2 introduces the main technologies used in blockchain systems. Section 3 systematically examines the security risks to blockchain.

2. OVERVIEW OF BLOCKCHAIN TECHNOLOGIES

This section introduces the main technologies employed in blockchain. We first present the fundamental trust mechanism (i.e., the consensus mechanism) used in blockchain, and then explain the synchronization process between nodes. After that, we introduce the two development stages of blockchain.

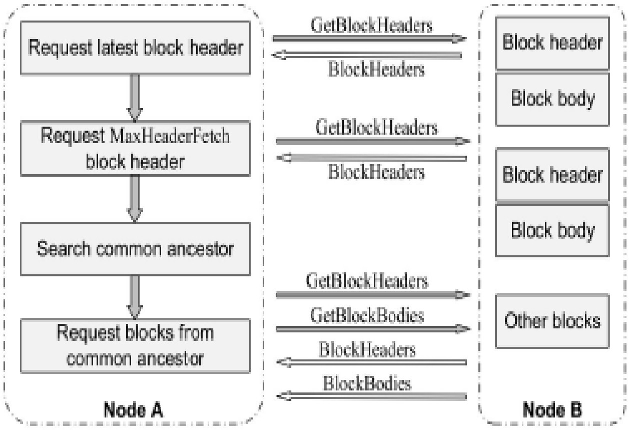
2.1. Consensus mechanism

Being a decentralized system, blockchain systems do not need a third-party trusted authority. Instead, to guarantee the reliability and consistency of the data and transactions, blockchain adopts the decentralized consensus mechanism. In the existing blockchain systems, there are four major consensus mechanisms: PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), and DPoS (Delegated Proof of Stake). Other consensus mechanisms, such as PoB (Proof of Bandwidth), PoET (Proof of Elapsed Time), PoA(Proof of Authority) and so on, are also used in some blockchain systems. The two most popular blockchain systems (i.e., Bitcoin and Ethereum) use the PoW mechanism. Ethereum also incorporates the PoA mechanism (i.e., Kovan public test chain), and some other cryptocurrencies also use the PoS mechanism, such as PeerCoin, ShadowCash and so on. PoW mechanism uses the solution of puzzles to prove the credibility of the data. The puzzle is usually a computationally hard but easily verifiable problem. When a node creates a block, it must resolve a PoW puzzle. After the PoW puzzle is resolved, it will be broadcasted to other nodes, so as to achieve the purpose of consensus, as shown in Fig. 1. In different blockchain systems, the block structure may vary in detail. Typically in Bitcoin, each block contains PrevHash, nonce, and Tx. In particular, PrevHash indicates the hash value of the last generated block, and Txs denote the transactions included in this block. The value of nonce is obtained by solving the PoW puzzle. A correct nonce should satisfy that the hash value shown in Eq. (1) is less than a target value, which could be adjusted to tune the difficulty of PoW puzzle. SHA256(PrevHash || Tx1 || Tx2 || . . . || nonce) < Target PoS mechanism uses the proof of ownership of cryptocurrency to prove the credibility of the data. In PoS-based blockchain, during the process of creating block or transaction, users are required to pay a certain amount of cryptocurrency. If the block or transaction created can eventually be validated, the cryptocurrency will be returned to the original node as a bonus. Otherwise, it will be fined.

In the PoW mechanism, it needs a lot of calculations, resulting in a waste of computing power. On the contrary, PoS mechanism can greatly reduce the amount of computation, thereby increasing the throughput of the entire blockchain system.

2.2. Block propagation and synchronization

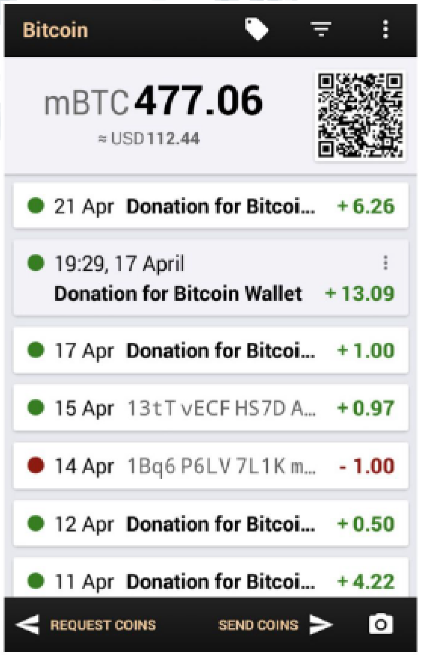
In the blockchain, each full node stores the information of all blocks. Being the foundation to building consensus and trust for blockchain, the block propagation mechanisms can be divided into the following categories: (1) Advertisement-based propagation. This propagation mechanism is originated from Bitcoin. When node A receives the information of a block, A will send an inv message (a message type in Bitcoin) to its connected peers. When node B receives the inv message from A, it will do as follows. If node B already has the information of this block, it will do nothing. If node B does not have the information, it will reply to node A. When node A receives the reply message from node B, node A will send the complete information of this block to node B. (2) Sendheaders propagation. This propagation mechanism is an improvement to the advertisement-based propagation mechanism. In the sendheaders propagation mechanism, node B will send a sendheaders message (a message type in Bitcoin) to node A. When node A receives the information of a block, it will send the block header information directly to node B. Compared with the advertisement-based propagation mechanism, node A does not need to send inv messages, and hence it speeds up the block propagation. (3) Unsolicited push propagation. In the unsolicited push mechanism, after one block is mined, the miner will directly broadcast the block to other nodes. In this propagation mechanism, there is no inv message and sendheaders message. Compared with the previous two propagation mechanisms, unsolicited push mechanism can further improve the speed of block propagation. (4) Relay network propagation. This propagation mechanism is an improvement to the unsolicited push mechanism. In this mechanism, all the miners share a transaction pool. Each transaction is replaced by a global ID, which will greatly reduce the broadcasted block size, thereby further reducing the network load and improving the propagation speed. (5) Push/Advertisement hybrid propagation. This hybrid propagation mechanism is used in Ethereum. We assume that node A has n connected peers. In this mechanism, node A will push the block to √ n peers directly. For the other n − √ n connected peers, node A will advertise the block hash to them.



Different blockchain systems may use diverse block synchronization processes. In Ethereum, node A can request block synchronization from node B with more total difficulty. The specific process is as follows (shown in Fig. 2) (1) Node A requests the header of the latest block from node B. This action is implemented by sending a GetBlockHeaders message. Node B will reply to node A a BlockHeaders message that contains the block header requested by A. (2) Node A requests MaxHeaderFetch blocks to find common ancestor from node B. The default value of MaxHeaderFetch is 256, but the number of block headers sent by node B to A can be less than this value. (3) If A has not found common ancestor after the above two steps, node A will continue to send GetBlockHeaders message, requesting one block header each time. Moreover, A repeats in binary search to find the common ancestor in its local blockchain. (4) After node A discovers a common ancestor, A will request block synchronization from the common ancestor. In this process, A requests MaxHeaderFetch blocks per request, but the actual number of nodes sent from B to A can be less than this value.

2.3. Technology development

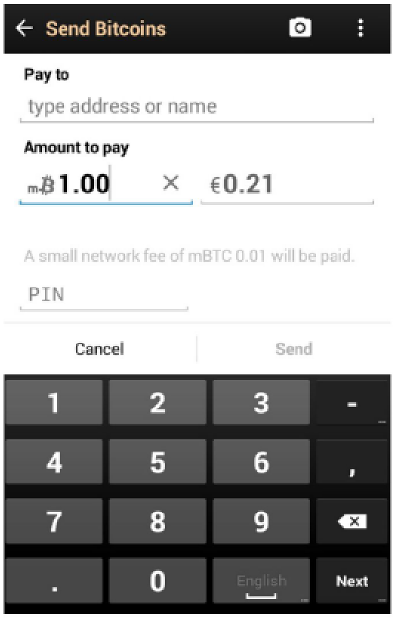
From the birth of the first blockchain system Bitcoin, the blockchain technology has experienced two stages of development: blockchain 1.0 and blockchain 2.0. In the blockchain 1.0 stage, the blockchain technology is mainly used for cryptocurrency. In addition to Bitcoin, there are many other types of cryptocurrencies, such as Litecoin, Dogecoin and so on. There are currently over 700 types of cryptocurrencies, and the total market capitalizations of them are over 26 billion US$ [30]. The technology stack of cryptocurrency could be divided into two layers: the underlying decentralized ledger layer and protocol layer [31]. Cryptocurrency client, such as Bitcoin Wallet, runs in the protocol layer to conduct transactions, as shown in Figs. 3–5. Compared with traditional currency, cryptocurrency has the following characteristics and advantages: (1) Irreversible and traceable. Transfer and payment operations are irreversible using cryptocurrency. Once the behavior is completed, it is impossible to withdraw. In addition, all user behaviors are traceable, and these behaviors are permanently saved in the blockchain. (2) Decentralized and anonymous. There is no third-party organization involved in the entire structure of cryptocurrency, nor does it has central management like banks. In addition, all user behaviors are anonymous. Hence, according to the transaction information, we cannot obtain the user's real identity. (3) Secure and permissionless. The security of the cryptocurrency is ensured by the public key cryptography and the blockchain



mBTC 477.06
≈ USD 112.44

● 21 Apr Donation for Bitcoi... +6.26
● 19:29, 17 April Donation for Bitcoin Wallet +13.09
● 17 Apr Donation for Bitcoi... +1.00
● 15 Apr 13tT vECF HS7D A... +0.97
● 14 Apr 1Bq6 P6LV 7L1K m... -1.00
● 12 Apr Donation for Bitcoi... +0.50
● 11 Apr Donation for Bitcoi... +4.22

Fig. 3. Query Bitcoin transaction history.



Send Bitcoins

Pay to

type address or name

Amount to pay

m฿1.00 × €0.21

A small network fee of mBTC 0.01 will be paid.

PIN

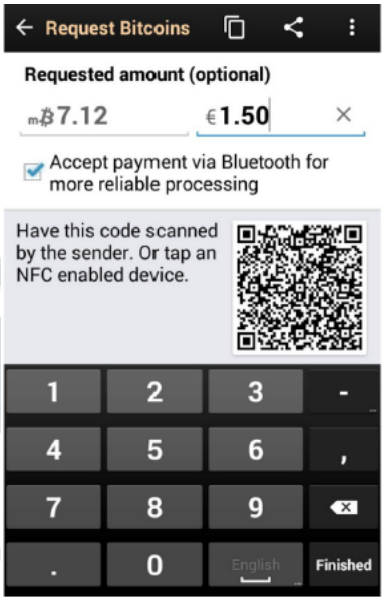
Cancel Send

Fig. 4. Pay with Bitcoin.

consensus mechanism, which are hard to be broken by the criminal. Moreover, there is no need to apply for any authority or permission to use cryptocurrency. Users can simply use the cryptocurrency through the relevant clients. (4) Fast and global. Transactions can be completed in only several minutes using cryptocurrency. Since cryptocurrencies are mostly based on public chains, anyone in the world can use them. Therefore, the user's geographical location has little impact on the transaction speed. In blockchain 2.0 stage, smart contract is introduced so that developers can create various applications through smart contracts. A smart contract can be considered as a lightweight dAPP (decentralized application). Ethereum is a typical system of blockchain 2.0. Each Ethereum node runs an EVM (Ethereum Virtual Machine) that executes smart contracts. Besides Ethereum, several other blockchain systems also support smart contracts, whose information is listed in Table 1. In Ethereum, developers can use a variety of programming languages to develop smart contracts, such as Solidity (the recommended language), Serpent, and LLL. Since these languages are Turing-complete, smart contracts can achieve rich functions. Fig. 6 shows the process of smart contracts' development, deployment and interaction. Each deployed smart contract corresponds to a unique address, through which users can interact with the smart contract through transactions by different clients (e.g., Parity, Geth, etc.). Since smart contracts can call each other through messages, developers can develop more featurerich dAPPs based on available smart contracts. Compared with the traditional

Table 1
Statistics of blockchain systems supporting smart contracts (until May of 2017)

System	Contract language	Total TXs	Market capitalization /M US$
Ethereum	EVM bytecode	23,102,544	8,468
RSK	Solidity	Unknown	N/A
Counterparty	EVM bytecode	12,170,386	15
Stellar	Transaction chains	Unknown	139
Monax	EVM bytecode	Unknown	N/A
Lisk	JavaScript	Unknown	71



Request Bitcoins

Requested amount (optional)

m฿7.12 €1.50 ×

☑ Accept payment via Bluetooth for more reliable processing

Have this code scanned by the sender. Or tap an NFC enabled device.

Fig. 5. Collect payments with Bitcoin.

that executes smart contracts. Besides Ethereum, several other blockchain systems also support smart contracts, whose information is listed in Table 1. In Ethereum, developers can use a variety of programming languages to develop smart contracts, such as Solidity (the recommended language), Serpent, and LLL. Since these languages are Turing-complete, smart contracts can achieve rich functions. Fig. 6 shows the process of smart contracts' development, deployment and interaction. Each deployed smart contract corresponds to a unique address, through which users can interact with the smart contract through transactions by

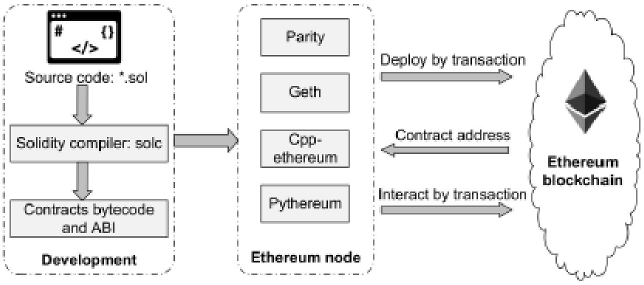


Fig. 6. The process of smart contract's development, deployment, and interaction.

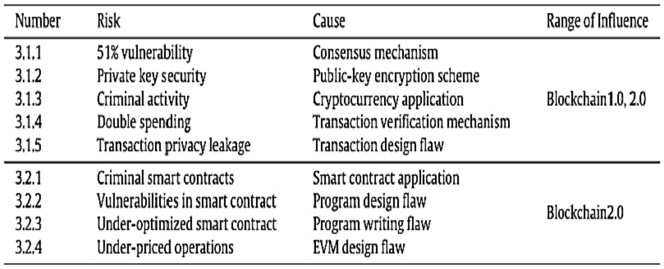
different clients (e.g., Parity, Geth, etc.). Since smart contracts can call each other through messages, developers can develop more featurerich dAPPs based on available smart contracts. Compared with the traditional application, a dAPP has the following characteristics and advantages (1) Autonomy. dAPPs are developed on the basis of smart contracts, and smart contracts are deployed and run on the blockchain. Hence, dAPPs can run autonomically without the need of any third party's assistance and participation. (2) Stable. The bytecodes of smart contracts are stored in the state tree of blockchain. Each full node saves the information of all

blocks and stateDB, including the bytecodes of smart contracts. Hence, the failure of some nodes will not affect its operation. This mechanism ensures that dAPPs can run stably. (3) Traceable. Since the invocation information of smart contracts is stored in the blockchain as transactions, all the behaviors of dAPPs are recorded and traceable. (4) Secure. The public key cryptography and the blockchain consensus mechanism can ensure the security and correct operations of smart contracts, so as to maximize the security of dAPPs.

3. RISKS TO BLOCKCHAIN

We divide the common blockchain risks into nine categories, as shown in Table 2, and detail the causes and possible consequences of each risk. The risks described in Section 3.1 exist in blockchain 1.0 and 2.0, and their causes are mostly related to the blockchain operation mechanism. By contrast, the risks introduced in Section 3.2 are unique to blockchain 2.0, and are usually resulted from the development, deployment, and execution of smart contracts.

Table 2
Taxonomy of blockchain's risks.



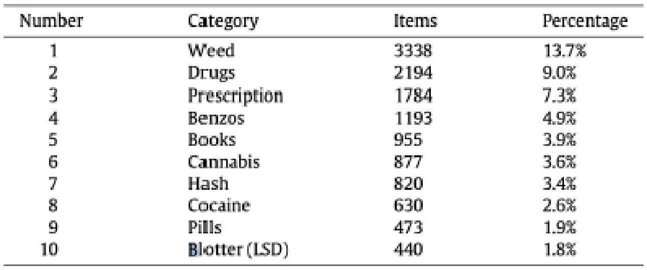
Number	Risk	Cause	Range of Influence
3.1.1	51% vulnerability	Consensus mechanism	Blockchain1.0, 2.0
3.1.2	Private key security	Public-key encryption scheme	
3.1.3	Criminal activity	Cryptocurrency application	
3.1.4	Double spending	Transaction verification mechanism	
3.1.5	Transaction privacy leakage	Transaction design flaw	
3.2.1	Criminal smart contracts	Smart contract application	Blockchain2.0
3.2.2	Vulnerabilities in smart contract	Program design flaw	
3.2.3	Under-optimized smart contract	Program writing flaw	
3.2.4	Under-priced operations	EVM design flaw	

3.1. Common risks to blockchain 1.0 and 2.0

3.1.1. 51% vulnerability

The blockchain relies on the distributed consensus mechanism to establish mutual trust. However, the consensus mechanism itself has 51% vulnerability, which can be exploited by attackers to control the entire blockchain. More precisely, in PoW-based blockchains, if a single miner's hashing power accounts for more than 50% of the total hashing power of the entire blockchain, then the 51% attack may be launched. Hence, the mining power concentrating in a few mining pools may result in the fears of an inadvertent situation, such as a single pool controls more than half of all computing power.

Table 3
Top 10 categories of items available in Silk Road.



Number	Category	Items	Percentage
1	Weed	3338	13.7%
2	Drugs	2194	9.0%
3	Prescription	1784	7.3%
4	Benzos	1193	4.9%
5	Books	955	3.9%
6	Cannabis	877	3.6%
7	Hash	820	3.4%
8	Cocaine	630	2.6%
9	Pills	473	1.9%
10	Blotter (LSD)	440	1.8%

In Jan. 2014, after the mining pool ghash.io reached 42% of the total Bitcoin computing power, a number of miners voluntarily dropped out of the pool, and ghash.io issued a press statement to reassure the Bitcoin community that it would avoid reaching the 51% threshold. In PoS-based blockchains, 51% attack may also occur if the number of coins owned by a single miner is more than 50% of the total blockchain. By launching the 51% attack, an attacker can arbitrarily manipulate and modify the blockchain information. Specifically, an attacker can exploit this vulnerability to conduct the following attacks. (1) Reverse transactions and initiate double spending attack (the same coins are spent multiple times). (2) Exclude and modify the ordering of transactions. (3) Hamper normal mining operations of other miners. (4) Impede the confirmation operation of normal transactions.

3.1.2. Private key security

When using blockchain, the user's private key is regarded as the identity and security credential, which is generated and maintained by the user instead of third-party agencies. For example, when creating a cold storage wallet in Bitcoin blockchain, the user must import his/her private key. Hartwig et al. [38] discover a vulnerability in ECDSA (Elliptic Curve Digital Signature Algorithm) scheme.

4. FUTURE DIRECTIONS

Based on the above systematic examination on the security of current blockchain systems, we list a few future directions to stir up research efforts into this area. First, nowadays the most popular consensus mechanism used in blockchain is PoW. However, a major disadvantage of PoW is a waste of computing resources. To solve this problem, Ethereum is trying to develop a hybrid consensus mechanism of PoW and

PoS. Conducting research and developing more efficient consensus mechanisms will make a significant contribution to the development of blockchain. Second, with the growth of the number of feature-rich dAPPs, the privacy leakage risk of blockchain will be more serious. A dAPP itself, as well as the process of communication between the dAPP and Internet, are both faced with privacy leakage risks. There are some interesting techniques that can be applied in this problem: code obfuscation, application hardening, execution trusted computing (e.g., Intel SGX), etc. Third, the blockchain will produce a lot of data, including block information, transaction data, contract bytecode, etc. However, not all of the data stored in blockchain is valid. For example, a smart contract can erase its code by SUICIDE or SELFDESTRUCT, but the address of the contract will not be erased. In addition, there are a lot of smart contracts containing no code or totally the same code in Ethereum, and many smart contracts are never be executed after its deployment. An efficient data cleanup and detection mechanism is desired to improve the execution efficiency of blockchain systems.

5. CONCLUSION

In this paper, we focus on the security issues of blockchain technology. By studying the popular blockchain systems (e.g., Ethereum, Bitcoin, Monero, etc.), we conduct a systematic examination on the security risks to blockchain. For each risk or vulnerability, we analyze its causes and possible consequence. Furthermore, we survey the real attacks on the blockchain systems, and analyze the vulnerabilities exploited in these attacks. Finally, we summarize blockchain security enhancements and suggest a few future directions in this area.

6. REFERENCES

[1] J. DESJARDINS, It's official: Bitcoin was the top performing currency of 2015, 2016. URL http://money.visualcapitalist.com/its-official-bitcoin-wasthetop- performing-currency-of-2015/ .

[2] J. Adinolfi, And 2016's best-performing commodity is ...bitcoin? 2016. URL http://www.marketwatch.com/story/and-2016s-best-performing-commodit y-is-bitcoin-2016-12-22.

[3] blockchain.info, Confirmed transactions per day, 2017. URL https://blockchain.info/charts/n-transactions?timespan=all/#.

[4] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: medrec prototype for electronic health records and medical research data,2016. URLhttps://www.media.mit.edu/publications/medrecwhitepaper/ .

[5] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: International Conference on Open and Big Data, OBD, 2016, pp. 25–30.

[6] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. (2016) 218.

[7] S. Huckle, R. Bhattacharya, M. White, N. Beloff, Internet of things, blockchain and shared economy applications, Proc. Comput. Sci. 98 (2016) 461–466.

[8] P. Bylica, Ł. Gleń, P. Janiuk, A. Skrzypczak, A. Zawłocki, A probabilistic nanopayment scheme for golem, 2015. URL http://golemproject.net/doc/ GolemNanopayments.pdf.

[9]P. Hurich, The virtual is real: An argument for characterizing bitcoins as private property, in: Banking & Finance Law Review, Vol. 31, Carswell Publishing, 2016, p. 573.

[10]A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing, 2017.

[11]Y. Zhang, J. Wen, The IoT electric business model: Using blockchain technology for the internet of things, Peer-to-Peer Netw. Appl. (2016) 1–12.

[12]J. Sun, J. Yan, K.Z. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities, Financ. Innov. (2016) 26.

[13] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The blockchain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 2016.

[14] E. Nordström, Personal Clouds: Concedo (Master's thesis), Lulea University of Technology, 2015.

[15] J.S. Czepluch, N.Z. Lollike, S.O. Malone, The use of block chain technology in different application domains, in: The IT University of Copenhagen, 2015, Copenhagen. Ethereum, Etherscan: The ethereum block explorer, 2017. URL https://www. ethereum.org/.

[16]L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.

[17] V. Buterin, Critical update re: Dao vulnerability, 2016. URL https://blog ethereum.org/2016/06/17/critical-update-re-dao-vulnerabilit y/.

[18] J. Adelstein, Behind the biggest bitcoin heist in history: Inside the implosion of mt.gox, 2016. URL http://www.thedailybeast.com/articles/2016/05/19/behin d-

the-biggest-bitcoin-heist-in-history-inside-the-implosion-o f-mt-gox.html.

[19] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017, pp. 164–186.

[20] Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, Internat. J. Web Grid Serv. (2016).

[21] M. Ghosh, M. Richardson, B. Ford, R. Jansen, A torpath to torcoin, proof-ofbandwidth altcoins for compensating relays, 2014. URL https://www.smithandcrown.com/open-research/a-torpath-to-torcoin-proof-of-bandwidth-altco ins-for-compensating-relays/. Intel, Proof of elapsed time (poet), 2017. URL http://intelledger.github.io/ .

IFERP connecting engineers... developing research