Open access • Proceedings Article • DOI:10.1109/COMNET.2018.8621944

Blockchain Challenges and Security Schemes: A Survey — Source link

Sirine Sayadi, Sonia Ben Rejeb, Zied Choukair

Institutions: Higher School of Communication of Tunis

Published on: 01 Nov 2018 - International Conference on Communications

Topics: Network security, Cloud computing, Server and Blockchain

Blockchain Challenges and Security Schemes: A Survey

Sirine Sayadi, Sonia Ben Rejeb, Zièd Choukair

Blockchain Challenges and Security Schemes: A Survey

Sirine SAYADI
MEDIATRON Laboratory
Higher School of Communication of Tunis, Sup'Com, Tunisia
Sirine.sayadi@supcom.tn

Sonia BEN REJEB
MEDIATRON Laboratory
Higher School of Communication of Tunis, Sup'Com, Tunisia
sonia.benrejeb@supcom.tn

Ziéd CHOUKAIR
MEDIATRON Laboratory
Higher School of Communication of Tunis, Sup'Com, Tunisia
Z.choukair@supcom.tn

***Abstract*— With the increasing number of connected devices and the number of online transactions today, managing all these transactions and devices and maintaining network security is a research issue. Current solutions are mainly based on cloud computing infrastructures, which require servers high-end and broadband networks to provide data storage and computing services. These solutions have a number of significant disadvantages, such as high maintenance costs of centralized servers, critical weakness of Internet Of Things applications, security and trust issues, etc. The blockchain is seen as a promising technique for addressing the mentioned security issues and design new decentralization frameworks. However, this new technology has a great potential in the most diverse technological fields. In this paper, we focus on presenting an overview of blockchain technology, highlighting its advantages, limitations and areas of application.**

The originality of this work resides in the comparison between the different blockchain systems and their security schemes and the perspective of integrating this technology into secured systems models for our comfort and our private life.

Keywords—Blockchain, Security, Technology, Smart Contracts, Consensus

I. INTRODUCTION

The current network model connects multiple computing devices and will continue to support small-scale Internet of Things networks that will not be able to meet the growing needs of tomorrow's large ecosystems. Centralized cloud servers will remain a bottleneck. throttling and a point of failure that can disrupt the network.

In this context, Blockchain technology appeared in 2009 by Nakamoto [1] "Bitcoin Developers" as a storage technology serving decentralized large registers and as a security technique for authenticating, authorizing and verifying data generated.

With blockchain technology the concept of consensus has emerged as a mechanism that ensures trust in communication between two entities without the intervention of an intermediary. We can use blockchain in cryptocurrency, smart contracts, digital identity management, internet of things, access control applications, automated peer-to-peer insurance, in banks and in many other applications [2].

Since its inception, from the initial cryptocurrency to the current smart contract, blockchain technology has shown promising prospects in many areas of application.

This proposed paper will be a state-of-the-art study on blockchain technology. Section 2 will present an overview of blockchain technology. Section 3 will describe a semantic study of the potential of blockchain technology. We present in Section 4 some cases of use of this technology. Then we will examine the security threats, some real attacks for this technology, and its security enhancement solutions in Section 5 and finally we will conclude our paper by suggesting future directions.

II. OVERVIEW OF BLOCKCHAIN TECHNOLOGIES

This section presents a complete visualization of blockchain technology, how it works, its structure and existing types.

A. Blockchain Process

The Blockchain process is described as a transaction between users on the network that are grouped into blocks. The block is validated and saved on the network by a «minor » according to cryptographic techniques that depend on the rules of the type of blockchain used.

In the bitcoin blockchain this technique is called the "Proof-of-Work", (POW), and "proof-of-stake" (POS) in the blockchain ethereum. If the block is validated, it is time stamped and added to the block chain. The transaction is then visible to the receiver as well as the entire network. This process takes some time depending on the blockchain (about 10 minutes for bitcoin, 15 seconds for Ethereum) [8].

Each blockchain is identified by its cryptographic hash and carries a list of transactions and a hash to the previous block.

The exception to this is the first block in the chain, called "genesis", which is common to all clients in a blockchain network and has no parent. This establishes a link between the blocks, thus creating a chain of blocks, or blockchain. Any node having access to this ordered and back-linked block list can read it and understand what is the current global state of the data exchange on the network.

978-1-5386-5651-8/18/$31.00 ©2018 IEEE

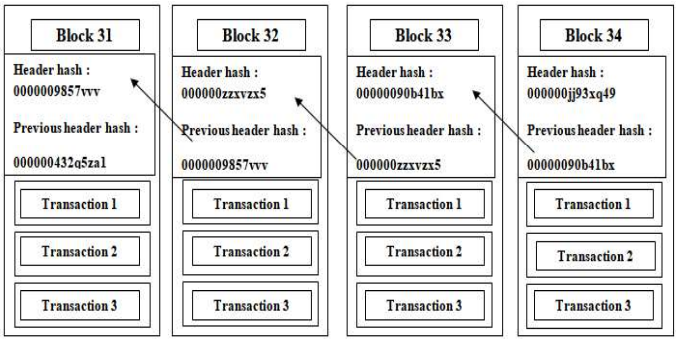

Figure 1: Blockchain Process

B. *Blockchain Structure*

A block is composed of two main parts which are the Block Header and the transactions (see Figure 1). The Block header contains several fields, the most important among them are the block version, the Merkle tree Root Hash, time stamp, nBits, Nonce and parent block hash. Transactions are the data saved in the block [46].

These fields will be detailed below (see figure 2):

- **Block Version**: Specifies the set of block validation rules to follow [46].
- **Merkle tree Root Hash :** is a condensed digital fingerprint of all transactions in the block. The slightest modification of a transaction in the block modifies this root. Its principle is to calculate the hash of a node from a hash of his sons [3].
- **Timestamp**: current time in seconds in universal time since January 1, 1970 [46].
- **nBits**: target threshold of a valid block hash.
- **Nonce**: A 4-byte field, which usually starts with 0 and increases for each hash calculation. On receipt of the new block, the complete nodes compute the header hash only once, to see if the Nonce is valid [37].
- **Parent block hash**: The nodes save the data of the block's. Thus, all the nodes have the hash of the block 31, if the block 32 is received by a node, it will determine that the block 32 is the child of 31 by checking this field [37].

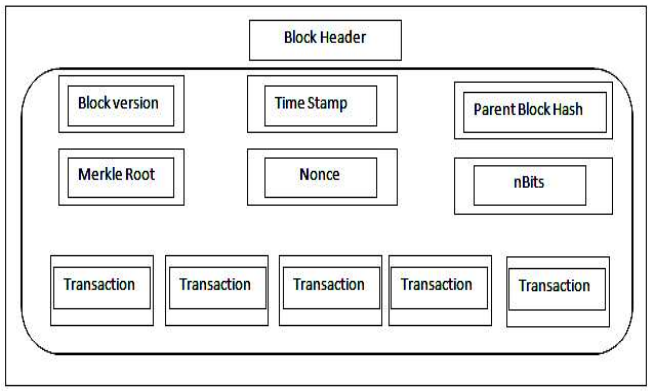

Figure 2: Simplified Block Structure

C. *Type of Blockchain*

There are three types of Blockchain technologies presented in the following table :

- **Public blockchain** from which everyone can participate in the process of reaching consensus and verifying the transaction. Like Bitcoin [4] and Ethereum [5].
- **Consortium blockchains**: In this type, the node can be chosen in advance if the data in blockchain can be public or private. They can be considered as partially decentralized like Hyperledger [6].
- **Private blockchain** has strict management authority over access to data. Nodes are restricted, not all nodes can participate in this blockchain like Ripple [7].

Table 1: Comparative table of blockchain types [46]

Property	Public Blockchain	Consortium Blockchain	Private Blockchain
Determination of consensus	all minors	Selected node	An organization
Read permission	public	Public or private	Public or private
Immutability	impossible to handle	can be altered	can be altered
Efficiency	Low	high	high
centralized	No	Partial	Yes
Consensus process	Without permission	With permission	With permission
Example	Bitcoin	Hyperledger	Ripple

All types of blockchain have advantages. The choice of blockchain type depends on our needs and our proposed services.

III. Potentiels of Blockchain

Blockchain technology is not only a technique, but it is a technological revolution with very important security features, its operating model using consensus and its shared ledger to solve the problems of traditional centralized models.

A. *Basic Security Techniques*

We detail in this section the different basic security principle by specifying how Blockchain technology can perfectly guarantee them.

- **Integrity:** it to ensure that the information has not been changed, only by those authorized to make changes. Blockchain uses cryptographic mechanisms to guarantee that operations are immutable with the purpose of verifying integrity.
- **Availability:** it ensures the availability of data for every need. the service is always active at the request of a legitimate users. Blockchain allows users to maintain blocks in a decentralized manner with various copies on the blockchain.

- **Pivacy:** is the guarantee that only authorized persons can access to the information. The Blockchain uses a pseudo-anonymization mechanism (hash functions) to hide user identities to ensure confidentiality.
- **Authentication:** a procedure by which a computer system certifies the identity of a person or a computer to allow that person to access certain secure resources. The Blockchain technology provides this function by providing private keys for users who are authorized to carry out transactions.
- **Non-repudiation:** Is the impossibility, for a person or any other entity engaged in a communication, to deny having received or sent a message, and this is ensured by blockchain technology.

B. Shared Ledger

This is the basic feature of blockchain technology, it means that blockchain does not have a centralized node, data is processed, stored and updated in a decentralized way. This avoids the problems of single deffain point and offers a peer to peer communication such that all nodes are interconnected and all participants in the network are equal without a central node.

C. Smart Contract

The smart contract is autonomous computer programs that once started, automatically execute pre-defined conditions with conditional statements of the type « if .... Then .... » Using the information available on the blockchain.

These contracts must be able to reduce audit costs, execution, arbitration and fraud. They may have to manage funds or authenticate external entities [8].

D. Consensus

A consensus is a secure fundamental trust mechanism. It characterizes a general agreement of existence of the members of a group. It allows you to make a decision without the need of an intermediary or a trusted authority.

In the existing blockchain system, there are several consensus mechanisms. We will quote the best known below:

- PoW (Proof of Work) :

Method used to validate Blockchain network blocks. This method requires users to use their computing power to validate a block. Minors compete against each other. As a result, the higher the computational power (combining several computers, to increase computing power), the more likely they are to find the result of a "Hash" function and thus validate the block. In the Bitcoin blockchain it is necessary to count a validation every 10 minutes approximately [9].

- PoS (Proof of Stake):

A chance to validate a block is based on how much of a stake (or cryptocurrency) the miners have. For example, if you had 5% of the cryptocurrency, you could extract 5% of all its transactions. People with more currency are thought to be less likely to attack the network. Its operating principle based on the richest person has more power in the network is unfair because the power here depends on the balance held in the account [46]. The PoS save more energy (reduces the amount of calculation) but increases the flow. Unfortunately, if the operating cost is close to zero, attacks could result.

- PBFT (Practical Byzantine Fault Tolerance) :

The problem of Byzantine generals is a metaphor that deals with questioning the reliability of transmissions and the integrity of the interlocutors. A Byzantine fault is therefore a failure that consists of the presentation of erroneous or inconsistent information. The consensus "Practical Bizantine Fault Tolerance" (PBFT) is a state machine replication protocol that tolerates arbitrary, or "Byzantine" faults. It is fault-resistant, fast, long-lived and an attack does not impact its performance too much. This protocol consists of three phases: pre-preparation, preparation & validation, it requires $3f + 1$ replicates to tolerate f simultaneous Byzantine faults. When a message is sent on the platform, the nodes retransmit the transaction to all peers. If at least 2/3 of the nodes confirm the validity of the transaction it is confirmed. The platform allows users to transfer peer-to-peer ownership regardless [46].

Many other consensus mechanisms can be found , such as DPoS (Delegated Proof of Stake), PoB (Proof of Bandwidth) [10], PoEt (Proof of Elapsed Time) [11], PoA (Proof of Authority) [12], Ripple [48], Tendermint[49] etc. that are used in some blockchain systems.

A comparison between some of the most used consensus algorithms is presented in table 2 [46].

With these advantages presented in this section from the basic security techniques, smart contracts, shared ledger and the consesus, blockchain technology has attracted attention in several areas..

In the next section, we will introduce some areas of use of blockchain technology as a solution concept.

Table 2: Comparison between some consensus algorithms

Property	**POW**	**POS**	**PBFT**
Identity management of nodes	**Without permission**	**Without permission**	**With permission**
Energy saving	**No**	**partial**	**yes**
Power tolerated	**<25% computing power**	**<51% stake**	**<33,3% Defective replicas**
Example	**Bitcoin**	**Ethereum**	**Hyperledger**

IV. CASES USE OF BLOCKCHAIN AND APPLICATIONS

In our days, Blockchain technology is used in many areas, not only in the financial application, but also in other areas such as supply chain traceability, identity certification, insurance, International payments, the Internet Of Things and the protection of privacy etc [25, 26, 31, 32, 33,34].

We detail in this section some uses of blockchain technology:

1) Digital Currency :

Several transaction systems have been built recently by blockchain technology, which makes a revolution in digital currency and online payment system. With these digital currencies and the crypthography technique, transfers can be made without the need of the central bank.

For example, we can send and receive bitcoins using public keys, with all anonymity we can record transactions.

Several other cryptocurrency like ethereurm, ripple, litecoin and etc [27].

2) Smart Contract:

Smart Contract is a digital contract that runs automatically through a computer system. It controls the digital assets of the user, by formulating a set of rules containing the rights and obligations of the users. Smart Contract is like an automatic trusting authority among participants [28]. Ethereum is an open source blockchain platform offering a decentralized virtual machine based on the Smart Contract. To manage these contracts Ethereum uses its digital currency called ETH, users can create many applications, services or different contracts on this platform [29].

3) Hyperledger :

Hyperledger is an open source blockchain platform, launched by the Linux Foundation in December 2015 with the aim of improving reliability and performance. It aims to support global business transactions of large technology, financial and supply chain companies etc [30].

4) Blockhcain To Ensure privacy, Access control and Integrity

Protecting our personal information and our private life is a challenge in our day. [35][36] uses blockchain technology based POW in IOT applications to ensure integrity and confidentiality. Blockchain can also be used for access control. Just save the history daily in blockchain as a signed transaction specifying public keys with access rights. Only minors authetified with his private keys can include this transactions in their blocks [37].

Based on blockchain technology, Ouaddah and al. [36] presented the FaiAccess framework with its different parts to allow users to control their data. Zyskind et al. [34] exploited the access control option provided by the blockchain with storage in a distributed hash table of several selected nodes. The Blockchain is used here for data location management and their access.

Ali and al. [33] used blockchain to build "Blockstack ID" which is an identity system and a decentralized PKI. This system consists of a control plane that is a name registration protocol and links and a data plan that is responsible for storing the data that must be signed by the name owner's key.

5) Blockchain For Eletronic Transactions

The Blockchain can be used as a base that will support the shared economy, based on machine-to-machine (M2M) communication. Several propositions in the theme [38, 39, 40, 41, 42]. Blockchain technology allows agents to autonomously perform a variety of transactions and to store the history of each transaction with transaparance and no deffiliation.

Sun et al. [41] specifies that Blockchain technology leads to the Internet of decentralized and autonomous objects. The blockchain supports all processing transactions between devices and each device can manage its behaviors and roles in an autonomous way.

Using the Bitcoin network, [40] described a model of data exchange by electronic money, between a sensor and a client. [38] described a Bitcoin-based e-commerce model for IOT devices. This composite model consists of 4 layers (the technical layer for the management of the Blockchain module, the infrastructure layer containing the smart contract platforms and IoT services, the content layer containing the participants and the IOT products and the layer exchange that contains the P2P transaction system).

We can find many other proposals that use Blockchain technology for economic transactions for IoT like ADEPT [43], Filament [39], Waston IoT platform [44], IOTA [42] etc.

6) Blockchain To Secure Smart Home :

Dorri et al. [45, 50] proposed a lightweight blockchain solution adopted for IoT without cryptocurrency to illustrate a smart home containing a power computer that is responsible to control and audit communications and provide access control between devices. It maintains a private blockchain and is considered minor without the need for the proof of work concept because only this computer is responsible for managing the blockchain. Other devices receive a private key and a public key to perform transactions. For example, if a sensor wants to open the faucet, it will send a transaction to the faucet, which will check in Blockchain if that sensor is allowed to open it.

A smart home is the best example for IoT Blockchain combination. The services offered by blockchain technology can be contribute to shared economies and to the smart cities where objects connect seamlessly and anonymously to exchange and share data.

V. SECURITY ISSUES OF A BLOCKCHAIN TECHNOLOGIE

We describe in this section some recently encountered limitations that can affect the good functioning of blockchain technology by presenting some models in the form of the proposed improvement solutions to limit these risks.

A. Risks to Blockchain

1) 51% Vulnerability:

The consensus mechanism has a vulnerability of 51%, which can be exploited by attackers to manipulate the blockchain.

In PoW, if the hash power of a minor> 50% of the blockchain's total hash power, the 51% attack can be initiated. As a result, mining resources concentrated in a few mining pools can cause fears, as a single pool controls more than half of all computing power [13].

In the PoS, if the number of cryptocurrencies owned by a single by a single miner is greater than 50% of the total blockchain. A 51% attack can occur which an attacker can arbitrarily manipulate information from the blockchain [47].

An attacker can exploit this vulnerability to carry out attacks; we will mention some of each after following [15]:

- Run a double spending by modifying the transaction data (same coins are spent multiples times).
- Change the order of transactions.
- Prevent normal mining operations of other miners (Denial of service attack).

2) Double Spending attack:

A customer provides a seller with a signed transaction; the seller verifies the validity with a peer who confirms the transaction. If the client is malicious, it can create a conflicting transaction by generating a double spend (the same crypto currency spent twice) and having it validated by another peer before the first transaction has spread across the network. Both transactions are therefore proposed for mining. Depending on which will be treated first, it is this truth that will be imposed on the entire network by registration in one block and invalidate the other. In this case, if the seller had delivered before validation by the minor, he was robbed ... resulting in a double spending [14] [47].

3) Smart Contracts Risks

- Dependency of the transaction order:

In order to update the blockchain, in each era, each miner will propose his own block. Since a block can contain multiple transactions, the state of the blockchain can change several times during an epoch.

This attack can be triggered if two successive transactions of the same block invoke the same smart contract. The order of execution of these two successive transactions affects the final state because the execution of the smart contract is associated with a single state [47].

- The time stamp dependency:

Each block in the blockchain contains a timestamp field. Some conditions for triggering smart contracts depend on the timestamp, which is defined by the minor according to the time of his local system. Smart contracts depend on time stamp fields are vulnerable, if they can be changed by attackers [47].

- Under-Optimized Smart Contract :

The gas value corresponds to the computing resources exploited by the bandwidth operation, memory occupancy and many other parameters used in Ethereum as a function of time.

We can find some resource-intensive operations such as dead code operations and the use of loops by exchanging the gas value according to the cryptocurrency. [47].

4) Denial Of Service Attack

An attacker can launch a DoS (Denial of Service) attack by exploiting a set of operations executed in a single transaction. This is because some heavy operations require too low gas values. This can cause a waste of resources [16].

5) Selfish Mining Attack:

This attack is conducted by mining in order to obtain undue rewards or to waste the computing power of honest minors [18]. The attacker holds the blocks discovered in private and then tries to forge a private channel. The authors in [19] proposed a Selfish-Mining attack, which attract other honest miners to dispel their computing resources unnecessarily to keep working on blocks that lead to a stalemate instead of attaching them to the longest chain.

6) Reentrancy Attack:

It is the fact of exploiting a recursive sending for example the biggest flight about 60 million US dollar of the contract CAO by this attack just after its deployment of 20 days [17].

7) Liveness Attack

In [20] the authors proposed this attack to exploit the dilation of the confirmation duration in order to obtain a target transaction.

8) The Balance Attack

Christopher and al. [21] proposed this attack based on PoW blockchain, which consists of identifying subgroups of miners with similar mining power and delaying messages passed between them in order to mine blocks before them.

B. Security Improvements

1) Smart Pool

L. Luu et al [22] proposed a new Smart Poll mining pool system, implemented as a smart contract. It is a decentralized mining protocol that replaces the centralized pool operator.

It retrieves client transactions that contain information about mining tasks. Then the miner performs a hash calculation and returns the completed shares to the smartpool. A threshold sets an amount, if the shadow of actions made reaches this threshold, the miners will be committed to a smartpool contract that verifies the actions and delivers rewards to the customer [47].

2) Quantitative Framework

In [23] the authors proposed a quantitative framework is used to analyze the performance and security provisions of the blockchain. it is a blockchain simulator and a security model that mimics its execution to evaluate basic security and performance.

This model specifically focuses on the attacks of selfish and double-spending mining by taking into consideration the consensus protocol used and network parameters such as block propagation delays, block sizes, delays network, block rate and the mechanism of propagation of information etc.

3) Oyente

Loi and al. [24] proposed a new program called Oyente that tracks errors in smart contracts. This tool can also detect bugs and injection attacks in smart contracts.

Oyente analyzes the bytecode of smart contracts and follows the EVM execution model [47].

VI. Conclusion and Perspectives

In this paper, we presented an overview of Blokchain technology. We have described its different security potentials by specifying a comparison between some of the most widely used consensus algorithms in different blockchain systems. We have also clarified the fields of use of this technology because in recent years, it has shown its potential in several applications and this is due to the advantages of this technology and its decentralized nature. These applications permeate everyday life, business and society as a whole, transforming the world into a more efficient world. And finally, we indicated that many maneuvers of this technology, then specifying the improvement solutions proposed to defend them.

Blockchain then presents many promising opportunities that open up many paths for the future and for a connected world in complete security. However, the challenges remain in the resources and consensus models used.

That's why, we aims in future work to leverage the benefits, limitations of blockcahin technology, and enhancement solutions to produce a new secure system model that integrates this technology with the Internet Of Things technology for a connected and secure world.

References

[1] S.Nakamoto, Bitcoin,Apeer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf.

[2] M. Pilkington, Blockchain technology: principles and applications. research handbook on digital transformations, F. X. Olleros andM. Zhegu, Eds., 2016.

[3] R. C. Merkle, “A digital signature based on a conventional encryption function,” in Proceedings of the Conference on the Theory and Application of Cryptographic Techniques.

[4] https://www.bitcoin.com/.

[5] G.Wood, “Ethereum, A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, 2014.

[6] C. Cachin, “Architecture of the hyperledger blockchain fabric,” in In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.

[7] M. Pilkington, “Blockchain technology: Principles and applications,” Browser DownloadThis Paper, 2015.

[8] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, \Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE Symposium on Security and Privacy (SP'16), pp. 839-858, May 2016.

[9] Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, in: International Journal of Web and Grid Services, 2016.

[10] M. Ghosh, M. Richardson, B. Ford, R. Jansen, A torpath to torcoin, proof-of-bandwidth altcoins for compensating relays (2014). https://www.smithandcrown.com/open-research/a-torpath-to-torcoin-proof-of-bandwidth-altcoins-for-compensating-relays/.

[11] Intel, Proof of elapsed time (poet) (2017). http://intelledger.github.io/.

[12] P. technologies, Proof of authority chains (2017).

[13] N. Hajdarbegovic, Bitcoin miners ditch ghash.io pool over fears of 51% attack (2014). http://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

[14] M. Rosenfeld, \Analysis of hashrate-based double spending," CoRR, vol. abs/1402.2009, 2014.

[15] Dean, 51% attack (2015). http://cryptorials.io/glossary/51-attack/

[16] B. Rivlin, Vitalik buterin on empty accounts and the ethereum state (2016). https://www.ethnews.com/vitalik-buterin-on-empty-accounts-and-the-ethereum-state.

[17] 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.

[18] S. Solat, M. Potop-Butucaru, Zeroblock: Preventing selsh mining in bitcoin, Ph.D. thesis, University of Paris (2016)

[19] I. Eyal, E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, in: Financial Cryptography and Data Security - 18th International Conference, Lecture Notes in Computer Science, 2014, pp. 436-454.

[20] A. Kiayias, G. Panagiotakos, On trees, chains and fast transactions in the blockchain, 2016. https://eprint.iacr.org/2016/545.pdf.

[21] C. Natoli, V. Gramoli, The balance attack against proof-of-work blockchains: The r3 testbed as an example, in: arXiv preprint:1612.09426, 2016.

[22] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smart pool: Practical decentralized pooled mining, USENIX Security Symposium, 2017.

[23] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: The ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3-16.

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

[25] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, \A secure sharding protocol for open blockchains," in

Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 17-30, New York, NY, USA, 2016.

[26] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, \A system view of financial blockchains," in IEEE Symposium on Service-Oriented System Engineering (SOSE'16), pp. 450-457, Mar. 2016.

[27] https://fr.investing.com/crypto/

[28] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, \Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE Symposium on Security and Privacy (SP'16), pp. 839-858, May 2016.

[29] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, \Blockchain contract: Securing a blockchain applied to smart contracts," in IEEE International Conference on Consumer Electronics (ICCE'16), pp. 467-468, Jan. 2016.

[30] I. Lin1 and T. Liao, "A Survey of Blockchain Security Issues and Challenges, " in International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017.

[31] D. W¨orner and T. Von Bomhard, “When your sensor earns money: Exchanging data for cash with Bitcoin,” in Proceedings of the 2014 ACMInternational Joint Conference on Pervasive and Ubiquitous Computing, UbiComp 2014, pp. 295–298, September 2014.

[32] K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” Ad Hoc Networks, vol. 32, article no. 1181, pp. 17–31, 2015.

[33] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in Proceedings of the USENIX Annual Technical Conference, pp. 181–194, 2016.

[34] G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in Proceedings of the IEEE Security and PrivacyWorkshops, SPW2015, pp. 180– 184, IEEE, May 2015.

[35] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2016, IEEE, Agadir, Morocco, December 2016.

[36] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things,” Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2017.

[37] E. F. Jesus , V. R. L. Chicarino, C. V. N. Albuquerque, and A. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," in Security and Communication Networks,vol.27, April 2018.

[38] Y. Zhang and J. Wen, “An IoT electric business model based on the protocol of bitcoin,” in Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015, pp. 184–191, IEEE, France, February 2015.

[39] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” Applied Innovation, vol. 2, pp. 6–10, 2016.

[40] D. W¨orner and T. Von Bomhard, “When your sensor earns money: Exchanging data for cash with Bitcoin,” in Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp 2014, pp. 295–298, ACM, September 2014.

[41] Y. Sun, H. Song, A. J. Jara, and R. Bie, “Internet of things and big data analytics for smart and connected communities,” IEEE Access, vol. 4, pp. 766–773, 2016.

[42] S. Popov, “The tangle, 2016,” https://iota.org/IOTA Whitepaper.pdf.

[43] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, “Adept: An iot practitioner perspective,” IBMInstitute for Business Value, 2014.

[44] N. Kshetri, “Can Blockchain Strengthen the Internet ofThings?” IT Professional, vol. 19, no. 4, Article ID8012302, pp. 68–72, 2017.

[45] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internetof things: Challenges and Solutions, 2016,” https://arxiv.org/abs/1608.05187.

[46] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.

[47] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, 2017.

[48] D. Schwartz, N. Youngs, and A. Britto, “The ripple protocol consensusalgorithm,” Ripple Labs Inc White Paper, vol. 5, 2014.

[49] J. Kwon, “Tendermint: Consensus without mining,” URLhttp://tendermint. com/docs/tendermint {}v04. pdf, 2014.

[50] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623, Kona, Big Island, HI, USA, March 2017.