Blockchain and IoT: Mind the Gap

Anass Sedrati[1,2], Mohamed Ahmed Abdelraheem[2], and Shahid Raza[2(✉)]

[1] INPT, Rabat, Morocco
sedrati@inpt.ac.ma
[2] RISE SICS, Stockholm, Sweden
{mohamed.abdelraheem,shahid.raza}@ri.se

Abstract. Blockchain, the core technology behind the first decentralized cryptocurrency, Bitcoin, has been recently proposed as a promising solution to create a viable decentralized network of Internet of Things (IoT) with good security and privacy properties. This survey investigates the currently proposed Blockchain-IoT solutions and examines their suitability for IoT devices.

1 Introduction

Blockchain is the core technology behind the decentralized Bitcoin cryptocurrency which operates in a trustless peertopeer network without the need to a centralized trusted party dictating the operations executed in the network. However, as indicated in many reports such as the UK government [1], Blockchain applications go far beyond Bitcoin as it can be used to turn a centralized application running by a trusted party to a decentralized application where the trust is distributed across the entire peer-to-peer network. The security behind the bitcoin blockchain relies on incentivising the participants in its peer-to-peer network who successfully accomplish specific assigned tasks by performing a certain amount of work.

Based on the Bitcoin blockchain concept, many alternative cryptocurrencies have been proposed by tweaking some parameters and/or adding new functionalities such as programs that execute autonomously on blockchains which are called smart contracts. An important new cryptocurrency that added new functionality represented in executing smart contracts is the Ethereum cryptocurrency. Anyone can participate in the trading of these alternative cryptocurrencies without any prior registration or permission and therefore are called public blockchains. When the participants of a blockchain are known, a so-called private or permissioned blockchain are more suitable and efficient choice. A private blockchain inherits the public blockchain features such as consensus-based transactions and creation of smart contract. However, private blockchains lose the true notion of distributed trust as it requires a single or group of entities to grant permissions to participate in the blockchain operations.

Internet of Things (IoT), a network of globally identifiable heterogeneous physical objects or things, are by nature a distributed network with very loose

G. Fortino et al. (Eds.): InterIoT 2017/SaSeIoT 2017, LNICST 242, pp. 113–122, 2018.
https://doi.org/10.1007/978-3-319-93797-7_13

or no centralized control. Therefore, blockchain could be a most suitable choice to perform secure and privacy-preserved device-to-device or device to back-end (cloud) transactions. In general, blockchain technology can be used to create decentralized applications where the trust is distributed across a peer-to-peer networks. However, this capability comes with increased and redundant use of resources. Most IoT devices, on the other hand, have limited processing, storage and communication capabilities. Also, most IoT deployments are within or close to human surroundings and sense physical environments; therefore, IoT have more stringent privacy requirements. Furthermore, compared with traditional Internet hosts, IoT devices are more vulnerable to unforeseen attacks. In this paper, we review different blockchain-based solutions proposed or claimed for IoT and investigate their suitability for different classes of IoT devices. We also discuss different blockchain technologies and IoT use cases where these technologies could be used.

The paper is organized as follows. In Sect. 2, we discuss IoT networks and their security challenges. In Sect. 3, we review blockchain technologies. In Sect. 4, we survey current blockchain technologies proposed or claimed for IoT. Section 5 concludes the paper.

2 IoT Devices and Networks

IoT Security: Providing security is challenging in the Internet, but even more challenging in the IoT as the devices are expected to have IPv6 and web support, globally accessible, heterogeneous (consisting of things, smartphones, standard computers, clouds), often deployed in unguarded environments, and most of them lack conventional user interface (keyboard, display, etc.). In addition, constrained environments in the IoT inherit the constraints of conventional Wireless Sensor Networks (WSNs) such as limited energy and processing resources, lossy wireless links, and multi-hop communication. A number of security solutions are proposed for these low-power and lossy IoT networks [2,3]. IoT deployments that deal with personal or sensitive data have the following security challenges.

- *Confidentiality and Integrity*: End-to-End encryption and unnoticed modification protection, while IoT data is in transit through a wireless multi-hop networks and at rest (stored in an IoT), is hard but necessary.
- *Availability*: Compared with traditional Internet hosts, due to unattended IoT deployments it is easier to compromised IoT devices, and due to low-power wireless connectivity it easier to interfere with or jam IoT networks.
- *Authenticity*: Source authentication is important but challenging because the limited IoT resources may not always permit digital signatures.
- *Compliance*: It is very challenging to ensure new EU GDPR compliance when ubiquitous environment-sensing IoT devices sense personal data.
- *Freshness*: Often connection-less data transfer protocols are used in IoT; it is therefore necessary that old packets are not replayed.

IoT Devices: IoT devices have heterogeneous capabilities in terms of processing power, storage, and energy; therefore, the definition of an IoT device varies across different sectors and use cases. However, there are two general categories of IoT devices: (i) long-lasting battery-powered and (ii) continuously powered or frequently chargeable. IETF, the organization who standardizes the base Internet protocols (IP, TCP, UDP, TLS/SSL, etc.), has also classified different IoT devices [4] and has standardized different novel protocols for these devices namely 6LoWPAN, CoAP, and RPL. In the current classification, IETF only considers battery-powered IoT devices and divides them into three classes. *Class 0* includes highly constrained devices with RAM size *less* than 10 KiB and ROM size *less* than 100 KiB. These devices will probably not be able to establish a secure global communication channel using sophisticated security protocols such as Datagram TLS (DTLS) [5]. They typically join the Internet through a more powerful device (e.g., a gateway). *Class 1* includes devices with RAM size close to 10 KiB and ROM size close to 100 KiB. These devices can use strong Internet security protocols such as DTLS but only with pre-shared keys and cannot have digital signature processing capabilities. *Class 3* includes devices with RAM close to 50 KiB and ROM close to 250 KiB. These devices can use fully-fledged DTLS with digital signature. We have recently shown the feasibility of DTLS in battery-powered IoT devices with digital signatures [6].

It is evident that the IETF classified IoT device categories cannot themselves run blockchain mining or even digital signatures for each transaction. On the other hand, these devices may rely on a third party for blockchain operations; however, this is against the philosophy of distributed blockchain where no trusted third party exists. Even when IoT devices are continuously powered and have more resources (such as a TV, refrigerator, and an ECU in a vehicle) they are not general-purpose computers and it will be insane to use them as blockchain minors. They can however create a blockchain transaction and can themselves perform digital signatures, ensuring end-to-end security.

Centralized vs Decentralized IoT: IoT architectures can be classified into two categories: centralized and decentralized. In most centralized architectures, IoT devices are passive and sense and send raw data to trusted cloud backends. Such an architecture requires a protected communication channel between an IoT device and cloud where the actual processing (or integration with for example blockchain) happens in a powerful machine. On the other hand, fully distributed IoT devices retrieve, process, combine and provide data and services to other entities, enabling direct device-to-device communication. When device resources permit, blockchain would be suitable choose to establish trust in distributed IoT.

3 Blockchain Technologies

Blockchain is a distributed authenticated data structure in a peer-to-peer network where blocks of data are added according to a consensus protocol. The blocks of data are interlinked with each other through the use of cryptographic

hash functions in way that creates a hash chain in order to make it difficult to modify by adversaries. Two main blockchain-based distributed ledgers are Bitcoin and Ethereum.

Bitcoin. Blockchain is the core technology behind the Bitcoin cryptocurrency and it was introduced in 2008 [7]. Bitcoin runs a consensus a protocol where any participant node that is able to solve a proof-of-work (POW) hash puzzle is allowed to add new blocks containing new transactions to the blockchain. A distributed consensus protocol must satisfy: *Agreement* all honest nodes decide for the same value; *Termination* all honest nodes must terminate in finite time; and *Validity* a decision value must be the input value of an honest node.

Bitcoin's consensus protocol is secure under the assumption that 51% of the participants are honest. While being secured and decentralized via a proof-of-work hash puzzle, Bitcoin's proof-of-work system has led it to become a centralized system as currently few miners have the privilege to add more blocks thanks to their huge investment in sophisticated and powerful hardware equipments to "mine" new bitcoins. Moreover, the proof-of-work system is estimated to require as much electricity as all of Denmark by 2020 [8]. This has led to many proposals other than the proof-of-work system such as proof-of-stake where a user's mining power depends on the amount of Bitcoin owned by the user. Also many alternative coins have been created by forking Bitcoin's source code and changing the cryptographic hash function under use (i.e. SHA256) to another hash function that is difficult to optimize in hardware such as scrypt. For example, Zerocash [9], a new promising cryptocurrency with strong privacy guarantees uses Equihash [10] proof-of-work algorithm to prevent any possible centralization of the mining process. Another concern regarding Bitcoin's scalability is the growing size of its blockchain and the few number of transactions (maximum 7 transactions/sec [11]) being processed in one second compared to standard credit card payment through the internet.

Ethereum. Besides the financial sector, blockchain can have different applications. One attempt to generalize the use of blockchains into different domains is Ethereum. It is a blockchain technology proposed by Vitalik Buterin where a transaction-based state machine is built [12]. Ethereum views smart contract as their first-class element. A smart contract is the transaction-based state machine generalization of the blockchain. Each node in the network is considered to be a singleton state machine that can switch between different states. Each state transition can be seen as a transaction and is added to a block that will be in the blockchain. In a smart contract context The machine updates then the states in the network depending on the current information in the blocks. Ethereum builds into the blockchain a Turing-complete instruction set to allow smart-contract programming and a storage capability to accommodate on-chain state [13].

Blockchain's Privacy. In Bitcoin's paper, it is mentioned that privacy can be maintained by keeping the public key (Bitcoin addresses) anonymous which would not enable linking a transaction to anyone. However, several papers [14–16] have investigated the anonymity of Bitcoin and the conclusion is that

Bitcoin is only pseudonymous. Obviously if anyone can link the different public key addresses to the real world identity of their owner, then all your transaction history is linked to your identity. In fact, many companies are offering de-anonymization services to financial and law enforcement agencies. Two main directions to achieve anonymity in cryptocurrencies. The first direction is using mixing/tumbler services which is specific for anonymizing Bitcoin. Many solutions exist such Coinshuffle [17], Mixcoin [18] and Blindcoin [19], to name a few. The second direction is to build "Anonymous Decentralized Cryptocurrencies". Recently two such cryptocurrencies have been proposed Zerocoin [20] and Zerocash [9]. Zerocoin [20] was originally proposed for providing anonymity in Bitcoin but it can be used in any cryptocurrency. However, it does not hide the meta data about the transactions. It uses cryptographic accumulators, commitment schemes and zero knowledge proofs to achieve anonymity. It is a semi-decentralized cryptocurrency as it requires a trusted setup to generate large prime numbers used in its scheme. Zerocash [9] is an independent cryptocurrency with strong privacy properties. It can also be integrated with Bitcoin or any other altcoins. It uses zk-SNARKS (Zero Knowledge Succinct Non Interactive Arguments of Knowledge) [21] a special kind of zero knowledge proof. It can also be considered as a semi-decentralized cryptocurrency as it also needs a trusted setup to generate its public parameters which was done recently in a ceremony where the random numbers involved in the setup procedure had been destroyed in order to prevent counterfeiting of Zerocash.

Private Blockchains. Bitcoin and Ethereum's blockchains are decentralized and permission-less public systems. This publicity comes at the cost confidentiality by revealing all the transactions history for everyone. It also leads to the privacy issues pointed above. Thus another solution that might be suitable for enterprises and financial institutions is to have a private blockchain. Such blockchain will operate in a closed network where a participant needs a permission to join the network. A private blockchains is a kind of shared database where all the interesting functions of public blockchains (i.e. consensus protocol, authenticated distributed data structure, smart contracts) are applied. However, they operate in a closed centralized network where the blockchain is accessible only by permissioned nodes.

4 Blockchains for IoT

Blockchain technology can provide a reasonable solution to some of the previously mentioned security and privacy problems existing in decentralized IoT networks [22]. In addition to security, blockchain offers the following to the IoT: data management and support for micro-transactions between IoT devices based on the exchange of data and services [22]. Next, we list possible use cases where blockchain-IoT combination can be useful.

4.1 Blockchain Use Cases in IoT

IoT was originally defined as a network of globally identifiable physical objects. Currently, IoT has become a generic term for any distributed connected devices/services. However, broadly speaking, IoT devices can be categorized as *devices having continuous power source* and *battery-powered or energy harvesting devices*. IoT in an enabling technology behind smart cities, smart homes, industry 4.0, etc. IoT and blockchain can go hand-in-hand in all those cases where the availability or use of a central entity is cumbersome or practically not possible, and most importantly the entity is not trustworthy. For completeness, we present some use cases where IoT can benefit from blockchain.

Supply Chain is one of the most hyped blockchain use case. Distributed IoT sensors (e.g. in smart containers) will be a major part of future supply chain management system.

Device-to-Device Communication in connected vehicles, future 5G-enabled devices, and wearable devices in another use case where blockchain can solve the painful cybersecurity authentication problem.

Software updates in billions of distributed IoT devices can be achieved using blockchain, where community built open source software for IoT can be distributed to devices without trusting or relying on a single software distribution entity.

4.2 Blockchain-IoT Solutions

In the following, we give a brief description about the currently proposed blockchain-IoT solutions.

IOTA. It is a public (or permission-less) cryptocurrency that does autonomous machine-2-machine transactions to enable technological resource trade which includes computational power, storage, data, bandwidth, electricity. Its core invention is a Directed Acyclic Graph (DAG) called the tangle [23] where all the transactions are stored. To issue a transaction, a user needs to verify and approve another two issued transactions chosen randomly beside solving a cryptographic hash puzzle [24] to stop spam and sybil attacks. IOTA was using a hash function called Curl [25] which has been recently replaced by the well-known SHA-3 hash function (Keccak) due to the recent practical collision attacks [26] on the Curl hash function. IOTA uses Winternitz hash-based signatures [27] in order to make it possible for IoT devices to sign transactions since IoT devices do not have the computational power to process the heavy mathematical operations existing in the standard digital signatures based on public key cryptography such as RSA, DSA and ECDSA. Moreover, hash-based signature also makes IOTA quantum-resistant which could be a major advantage in the future over standardized digital signatures.

KSI Guardtime. Key less Signature Infrastructure (KSI) [28] provides data integrity through the use of hash-based digital signatures [29] similar to IOTA.

Its blockchain is private (or permissioned) and thus it uses a scalable distributed consensus protocol to add new issued transactions.

IBM Private Blockchain. Enables IoT devices to send its data or transactions to a private blockchain network (e.g. hyperledger fabric [30]). Using a consensus protocol such as Practical Byzantine Fault Tolerance (PBFT) where an n nodes network can withstand $(n-1)/3$ non-honest nodes, IBM's private blockchain enables business partners involved to reach an agreement about any transaction executed in the network without the need for third-party authentication and validation. According to IBM, this allows the creation of more efficient and profitable business networks. However, IBM's private blockchain uses digital signatures based on public key cryptography which might not be suitable for constrained IoT devices.

ENIGMA. Storing, managing and using sensitive data collected by IoT devices in a decentralized fashion is one of Enigma's many applications suggested in [31]. It is a decentralized platform enabling private computations of data by employing secure multi-party computations (MPC). Private data is divided between different nodes which securely compute functions without leaking information to other nodes. It is not a cryptocurrency but a personal data management platform supporting privacy. Its incentive is not based on mining rewards as done in public blockchains but on fees where nodes are paid for computational resources. It uses a distributed hash table (DTH) accessible from the blockchain to store references of the location of data. Sensitive data are encrypted at the client side before being stored and its corresponding access policy are encoded in the blockchain. Encrypted data are stored in an off-chain distributed database shared by a number of nodes where each node has a distinct view of shares. Off-chain nodes perform secure multiparty computations to process the encrypted data. Security deposits are paid by nodes in order to join a multiparty computation in order to punish malicious nodes.

Discussion. *Data integrity* in IOTA's public network and Guardtime's private network is provided via the use of Hash-based signatures, which enable lightweight IoT devices to sign their issued transactions. However, IOTA's public network employs a hash puzzle proof-of-work mechanism to prevent sybil attacks. While a lightweight IoT device can sign transactions using a hash-based signature scheme such as Winternitz's one-time signature [27], solving a hash puzzle consumes a lot of energy and thus will not be possible using energy-limited IoT devices.

Confidentiality of IoT's data can be provided using ENIGMA, but one problem here is that secure MPC are not scalable even for standard computing devices let alone IoT devices in terms of computation time and communication size. Thus, the IoT use case in ENIGMA provides integrity to public non-sensitive data on its blockchain can only be suitable for *Class 2* IoT devices. However, *confidentiality* can be supported, in *Class 1* IoT devices where *only* symmetric cryptographic operations can be performed (e.g. subclass of *Class 1*), through the use of pre-shared symmetric keys in case of small scale IoT network with

limited number of users. Table 1 shows how current blockchain-IoT solutions are different from each other.

Though there are few blockchain solutions targeting IoT devices, blockchain for IoT is still in inception stage and there is lot to do before we can take full advantages of blockchain in resource-constrained IoT. On top the to-do list are lightweight privacy-enabled consensus protocols and permission management for private blockchain without a central permission granting entity.

Table 1. The table shows the difference between some Blockchain-IoT solutions. Proof-of-work is a requirement for public networks. Guardtime's KSI private blockchain uses an unspecified distributed consensus protocol without employing proof-of-work.

Solution	Network	Signature scheme	Security features	Consensus
IOTA	Public	hash-based (Winternitz [27])	Data integrity only	Proof-of-work
KSI	Private	hash-based (KSI [29])	Data integrity only	Not specified
IBM	Private	standard	Data integrity only	PBFT
ENIGMA	Public	standard	Confidentiality/integrity	Proof-of-work

5 Conclusion

Public blockchains use a proof-of-work consensus and thus they have a number of efficiency limitations represented in (a) the waste of energy done by the proof-of-work consensus mechanism, (b) limited number of transactions processed per second. Another concern in public blockchains is the growing size of the blockchain which makes auditing difficult for new nodes. However, a public blockchain with a secure proof-of-stake consensus algorithm might enable light clients such as IoT devices to join the network and add new blocks [32]. Moreover, confidentiality of transactions and privacy of users are major issues that halt the adoption of public blockchains in business enterprises. But even with a pro-privacy cryptocurrency such as Zerocash, the limited number of processed transactions per second will remain to be an issue that needs to be addressed in public blockchains.

Blockchain-IoT solutions can be useful in IoT applications where data integrity is needed but confidentiality and privacy are not needed for the users involved in the network. Due to employing a proof-of-work mechanism, public Blockchain-IoT solutions such as IOTA suffer from high energy consumption as well as a fewer number of transactions processed per second compared to standard payment systems such as VISA. Therefore, private blockchains using hash-based signatures (e.g. Guardtime's KSI) instead of standard digital signatures to provide data integrity are the most appropriate choice for IoT applications since they do not need to employ a proof-of-work mechanism and thus could enable energy-limited IoT devices where symmetric cryptographic operations can be performed to join the network.

Acknowledgments. This work is funded by the VR Strategic Research Area (SRA) Information and Communication Technology - The Next Generation (ICT TNG) program.

References

1. Office of Science UK Government Chief Scientific Advisor. Distributed ledger technology: beyond block chain (2016)
2. Bagci, I.E., Raza, S., Roedig, U., Voigt, T.: Fusion: coalesced confidential storage and communication framework for the iot. Secur. Commun. Netw. **9**(15), 2656–2673 (2016). sec.1260
3. Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. **11**(8), 2661–2674 (2013)
4. Bormann, C., Ersue, M., Keranen, A: Terminology for constrained-node networks. Technical report (2014)
5. Rescorla, E., Modadugu, N.: Datagram transport layer security version 1.2 (2012)
6. Raza, S., Helgason, T., Papadimitratos, P., Voigt, T.: Securesense: end-to-end secure communication architecture for the cloud-connected Internet of Things. Future Gener. Comput. Syst. **77**, pp. 40–51. Elsevier (2017)
7. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
8. Deetman, S.: Bitcoin could consume as much electricity. https://web.archive.org/web/20160828092858/http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
9. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy, pp. 459–474. IEEE (2014)
10. Biryukov, A., Khovratovich, D.: Equihash: Asymmetric proof-of-work based on the generalized birthday problem (2017)
11. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gün Sirer, E., Song, D., Wattenhofer, R.: On scaling decentralized blockchains. In: Clark, J., Meiklejohn, S., Ryan, P.Y.A., Wallach, D., Brenner, M., Rohloff, K. (eds.) FC 2016. LNCS, vol. 9604, pp. 106–125. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53357-4_8
12. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151 (2014)
13. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: Using blockchain for medical data access and permission management. In: International Conference on Open and Big Data (OBD), pp. 25–30. IEEE (2016)
14. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 6–24. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39884-1_2
15. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet measurement Conference, pp. 127–140. ACM (2013)
16. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 34–51. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39884-1_4

17. Ruffing, T., Moreno-Sanchez, P., Kate, A.: CoinShuffle: practical decentralized coin mixing for bitcoin. In: Kutyłowski, M., Vaidya, J. (eds.) ESORICS 2014. LNCS, vol. 8713, pp. 345–364. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11212-1_20
18. Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: anonymity for bitcoin with accountable mixes. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 486–504. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_31
19. Valenta, L., Rowan, B.: Blindcoin: blinded, accountable mixes for bitcoin. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) FC 2015. LNCS, vol. 8976, pp. 112–126. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48051-9_9
20. Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributed e-cash from bitcoin. In: 2013 IEEE Symposium on Security and Privacy (SP), pp. 397–411. IEEE (2013)
21. Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M.: Succinct non-interactive zero knowledge for a von neumann architecture. Cryptology ePrint Archive, Report 2013/879 (2013). http://eprint.iacr.org/2013/879
22. Brody, P., Pureswaran, V.: Device democracy: Saving the future of the Internet of Things. IBM, September 2014
23. Popov, S.: The tangle (2016). https://iota.org/IOTA_Whitepaper.pdf
24. IOTA infosheet // blockchain 3.0. http://iotanodes.org/IOTA_Infosheet_dec_2016_revised.pdf
25. Sønstebø, D.: The transparency compendium. https://blog.iota.org/the-transparency-compendium-26aa5bb8e260
26. Heilman, T.D.E., Narula, N., Virza, M.: IOTA vulnerability report: Cryptanalysis of the curl hash function enabling practical signature forgery attacks on the IOTA cryptocurrency (2017). https://github.com/mit-dci/tangled-curl
27. Buchmann, J., Dahmen, E., Ereth, S., Hülsing, A., Rückert, M.: On the security of the winternitz one-time signature scheme. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 363–378. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21969-6_23
28. Guardtime. KSI blockchain technology. https://guardtime.com/technology/ksi-technology
29. Buldas, A., Kroonmaa, A., Laanoja, R.: Keyless signatures' infrastructure: how to build global distributed hash-trees. In: Riis Nielson, H., Gollmann, D. (eds.) NordSec 2013. LNCS, vol. 8208, pp. 313–320. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41488-6_21
30. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers (2016)
31. Zyskind, G., Nathan, O., Pentland, A.: Enigma: Decentralized computation platform with guaranteed privacy (2015). arXiv preprint arXiv:1506.03471
32. Buterin, V.: Light clients and proof of stake (2015). https://blog.ethereum.org/2015/01/10/light-clients-proof-stake/