Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 177 (2020) 605–612

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Blockchain Security (IWBCS 2020)
November 2-5, 2020, Madeira, Portugal

Management and Monitoring of Blockchain Systems

Dominique Bernard Kanga[a]*, Mohamed Azzouazi[b], Mohammed Yassine El Ghoumrari[b], Abderrahmane Daif[b]

[a]*University HassanII, Faculty of sciences Ben M'sik Casablanca, Av Driss El Harti B.P 7955 Sidi Othmane, Casablanca , Morocco*
[b]*University Hassan II, faculty of sciences Ben M'sick Casablanca Av Driss El Harti B.P 7955 Sidi Othmane, Casablanca, Morocco*

Abstract

Blockchain technology is based on a decentralized model, in which pairs collaborate and build trust on a corporate or public network. Each peer organization can be represented by one or more nodes and this network of nodes is used to broadcast transactions and reach consensus for each transaction submitted. secure data encryption and new transactions linked to previous ones make it nearly impossible to edit old records without having to edit subsequent ones. On the other hand, controlling more than half of the nodes in the network could allow Blockchain data corruption. However, adding a layer of oversight of each Blockchain node and the entire Blockchain network could ensure truly decentralized and robust operations.

Keywords: organization; Blockchain monitoring; network security; monitoring; framework;

1. Introduction

Blockchain is today one of the most important technologies that emerged in recent years. Many experts believe that this technology has the potential to change the world over the next two decades. Although it is still in its infancy, the giants of the company are interested in its applications in several areas. So far, venture capitalists have invested billions of dollars in this area, with several applications.

* Corresponding author. Tel.: +212 06-69-08-82-30.
E-mail address: kangadominiquebernard@gmail.com

1877-0509
10.1016/j.procs.2020.10.086

Blockchain applications indeed seem close to infinity. If one immediately thinks of its financial applications - international payments, remittances, complex financial products - Blockchain can also solve problems and create new opportunities in the healthcare, defense, management sectors, supply chains, luxury goods and other industries. At more advanced stages, Blockchain could give rise to what Gartner calls the "programmable economy," fueled by entirely new business models that eliminate all kinds of middlemen.

Faced with this strengthening brought to society by Blockchain technology, researchers have undertaken work to further strengthen the level of security of this technology. However, monitoring all Blockchain nodes could present itself as an additional layer of security for corporate Blockchain networks. In this article, we will first present an overview of Blockchain, then list some security properties already implemented at the level of Blockchain systems before proposing a Blockchain monitoring system and a Blockchain monitoring framework; at the end we will make a synthesis and perspectives of this study[1].

2. Overview of the Blockchain Technology

A Blockchain is a record of the truth that creates trust between multiple parties. Specifically, it is a secure and tamper-proof ledger with time-stamped transactions, distributed among a number of entities[2].

Not all Blockchains work the same. They may for example differ in their consensus mechanisms, which prevail as the rules depending on the technology will update the ledger. But basically, a Blockchain is a ledger on which new transactions are recorded in blocks, with each block identified by a cryptographic signature of the data that it contains.

The same signature will always result from this data, but it is not possible to recreate the data from this signature. Likewise, if even the smallest detail of this transaction data is changed, it will create a very different signature, and since the signature of each block is included as a point born in the next block, subsequent blocks will also be returned with different hashes. This is what makes the registry inviolable[3].

Finally, the security of the Blockchain also comes from the fact that several computers called nodes store the Blockchain. To change the ledger, it is therefore necessary to take control of at least 50% of the computing power in order to change the data - a difficult feat especially for a public Blockchain such as the one that frames bitcoin.

With the advent of the quantum machine, this unequal security within the Blockchain may be questionable in the future. This is why Blockchain monitoring could add an important layer of security at the Blockchain level[4] [1] and our work is around discussing and studying this topic.

3. Blockchain's Security Basics, Properties, Techniques and Applications

The basic security properties of Blockchain flow from both advances in cryptography and the design and implementation of Bitcoin. Theoretically, the first secure Blockchain was formulated using cryptography in 1991 [4]. A proposal to improve efficiency of the crypto Blockchain was published in 1993, by incorporating Merkle trees and placing multiple documents in a block. The Blockchain is designed to ensure a number of inherent security attributes, such as consistency, proof of tampering, resistance to a distributed denial of service (DDoS) attack, pseudonymity, and resistance to a double attack. However, to use the Blockchain for secure distributed storage, additional security and privacy properties are required [5]. In this part, we describe the basic security and privacy properties of Blockchains before moving on to the topic of monitoring Blockchain systems with the aim of adding an additional layer of security that can be leveraged to further enhance security.

3.1 Consistency

The consistency concept in the Blockchain context as a distributed global ledger refers to the property that all nodes have the same ledger at the same time. The consistency property has raised some controversial debate. Some argue that Bitcoin systems only provide eventual consistency [6], which is a weak consistency. Others claim that Bitcoin

guarantees strong consistency, not eventual consistency [7]. Eventual consistency is a consistency model proposed for distributed computing systems by seeking a tradeoff between availability and consistency. Formally, it ensures that all updates to replicas are propagated in a lazy fashion and all read access to a data item will eventually get the last updated value if the item receives no new updates [8]. In other words, eventual consistency makes sure that data of each entry at each node of the system gets consistent eventually, and thus achieves high availability and low latency at the risk of returning stale data. With eventual consistency, time taken by the nodes of the system to get consistent may not be defined. Thus, data getting consistent eventually means that [1] it will take time for updates to be propagated to other replicas [2]; and if someone reads from a replica which is not updated yet (since replicas are updated eventually), then there is some risk of returning stale data[6], [9]. Within a Blockchain network system, the strong consistency model means that all nodes have the same ledger at the same time, and during the time when the distributed ledger is being updated with new data, any subsequent read/write requests will have to wait until the commit of this update. In contrast, the eventual consistency model means that the Blockchain at each system's node gets consistent eventually, even though, some read/write Blockchain's requests may return stale data. The key challenge for strong consistency is that the performance cost (w.r.t. latency/availability) is too high to be affordable for all cases. The key challenge for eventual consistency is how to remove the inconsistency that may be caused by stale data. The Blockchain in Bitcoin adopts a consistency model that seeks a better tradeoff between strong consistency and eventual consistency for achieving partition tolerance (P) and consistency (C) with deferred availability. In Bitcoin, transactions are grouped in blocks. When a sender node sends a transaction to the Blockchain network, miner nodes will mine it by adding it to a block with other unverified transactions and performing a proof of work challenge game. Upon completing its proof of work challenge, a miner sends its block and its proof to the network to solicit acceptances from other nodes, which will verify all transactions in the block. The other nodes accept the block by working on generating the next block using the hash of the accepted block as its previous hash. The miner whose block is contained in the longest chain and who is the first to obtain ω confirmations (a.k.a. ω blocks are appended on the top of the block, and $\omega = 6$ by default in Bitcoin consensus protocol) is the winner for chaining this transaction into the distributed global ledger. We can view the ω parameter as a mechanism to provide configurable or parameterized strong consistency in Blockchain. In summary, Blockchain is an elegant approach to addressing the CAP problem for storing a distributed ledger in a decentralized system. For Bitcoin, Blockchain implements the partition tolerance (P) while supporting consistency (C) and availability (A) on the clipped Blockchain with the most recent ω blocks disregarded. In short, the consensus protocol accepts an update to the Blockchain (the distributed global ledger) only when a number of confirmations received by a miner on its challenge solution is equal to or higher than ω, thus, the update availability is delayed until the ω confirmations is obtained from the network. The read protocol reads only the Blockchain with the last ω blocks on the chain clipped to ensure the strong consistency and the read availability on the ω-clipped Blockchain. Thus, some has argued that Blockchain in Bitcoin guarantees far stronger than eventual consistency. It offers serializability with a probability that is exponentially decreasing with latency [6]. On the other hand, certain Blockchain applications are less risk-averse and may benefit from a weaker consistency guarantee for convenience and performance. For instance, when $\omega = 0$, it means that zero-confirmation is required for both the consensus protocol and the read protocol. This may be a practical choice for those risk-free distributed applications. The blog from Emin Gün Sirer [4] is an excellent starting point for more readings on this subject. Furthermore, the time required to confirm a Bitcoin transaction with the ω constraint for strong consistency may be prohibitively slow for some applications, e.g., 10 minutes on average of generating a block in Bitcoin, and this high latency is aggravated when ω is configured with higher value. Recently, some research efforts try to build much faster, much higher throughput Blockchain systems that provide better guarantees than Bitcoin's 0-confirmation transactions. PeerCensus extends the Bitcoin Blockchain to support strong consistency and to decouple block creation and transaction confirmation[10].

3.2 Tamper-Resistance.

Tamper-resistance refers to the resistance to any type of intentional tampering to an entity by either the users or the adversaries with access to the entity, be it a system, a product, or other logical/physical object. Tamper-resistance of Blockchain means that any transaction information stored in the Blockchain cannot be tampered during and after the

process of block generation. Specifically, in a Bitcoin system, new blocks are generated by mining nodes. There are two possible ways that the transaction information may be tampered with: [1] Miners may attempt to tamper with the information of received transaction; [2] Adversary may attempt to tamper with the information stored on the Blockchain. We analyze why such tampering attempts are elegantly prevented by the Blockchain protocols in Bitcoin. For the first kind of tampering, a miner may attempt to change the payee address of the transaction to himself. However, such attempt cannot be succeeded, since each transaction is compressed by a secure Hash function, such as SHA-256, then signed by the payer using a secure signature algorithm, such as ECDSA, in a Bitcoin network, and finally, the transaction is sent to the entire network for verification and approval through mining. Thus, multiple miners may receive and pick up the transaction to mine, which is done in a non-deterministic fashion. If a miner alters any information of the transaction, it will be detected by others when they check the signature with payer's public key, since the miner cannot generate a valid signature on the modified information without the payer's private key. This is guaranteed by the unforgeability of the secure signature algorithm.

For the second kind of tampering, an adversary will fail its attempts to modify any historical data stored on the Blockchain. This is because of the two protection techniques used in the distributed storage of Blockchain in Bitcoin: the hash pointer and the network wide support for both storage and verification of the Blockchain. Specifically, if an adversary wants to perform tampering with the data on some block (say k), the first difficulty encountered by the adversary is the mismatch problem, namely, the tampered block k has an inconsistent hash value compared to the hash of the preceding block k maintained in the k + 1 block. This is because using a hash function with collision-resistance, the outputs of the collision-resistent hash function with two different inputs will be completely inconsistent with an overwhelming probability, and such inconsistency can be easily detected by others on the network. Even if the adversary attempts to disguise this tampering by cracking the previous block's hash and so on along the chain, this attempt will eventually fail as the head of the list (a.k.a. genesis block) is reached. Moreover, in the Blockchain of Bitcoin network, everyone has a copy of Blockchain. It is very hard for an adversary to modify all copies in the entire network. In short, as every transaction in Bitcoin is signed and distributed over all network's nodes through the Blockchain, it is practically impossible to tamper transaction data without the network knowing about it, showing the power of crowd for storing and distributing the Blockchain. This property is attractive to many applications. For example, in healthcare, the Blockchain could help to create immutable audit trails, maintain the reliability of health trials, and uphold the integrity of patient data.

3.3 Resistance to DDoS Attacks

A denial-of-service attack refers to as the DoS attack on a host. It is one of the cyber-attacks' type that disrupt the hosted Internet services, by making the host machine or the network resource on the host unavailable to its intended users. DoS attacks attempt to overload the host system or the host network resource by flooding with superfluous requests, consequently stalling the fulfillment of legitimate services. DDoS attack refers to "distributed" DoS attack, namely, the incoming traffic flooding attack to a victim is originated from many disparate sources distributed across the Internet. A DDoS attacker may compromise and use some individual's computer to attack another computer by taking advantage of security vulnerabilities or weaknesses. By leveraging a set of such compromised computers, a DDoS attacker may send huge amounts of data to a hosting website or send spam to particular email addresses [8]. This effectively makes it very hard to prevent the attack by simply jamming individual sources one by one. The arm-race depends on the repairing rate of such compromised nodes against the success rate of compromising computer nodes in the network. The serious concern in a DDoS attack is on the availability of Blockchain and is related to the question of whether a DDoS attacker can make the Blockchain unavailable by knocking out a partial or the whole network. The answer to this question is no, thanks to the fully decentralized construction and maintenance of the Blockchain and Bitcoin system and the consensus protocol for new block generation and addition to the Blockchain, which ensures that the processing of Blockchain transactions can continue even if several Blockchain nodes go offline. In order for a cyber-attacker to succeed in making Blockchain offline, the attacker would have to collect sufficient computational resources that can compromise overwhelmingly large portion of the Blockchain nodes across the entire Bitcoin. The larger the Bitcoin network becomes, the harder it is to succeed in such large-scale DDoS attack.

3.4 Resistance to Double-Spending Attacks

The double-spending attack in the context of Bitcoin Blockchain refers to a specific problem unique to digital currency transactions. Note that the double-spending attack can be considered as a general security concern due to the fact that digital information can be reproduced relatively easily. Specifically, with transactions exchanging digital token, such as electronic currency, there is a risk that the holder could duplicate the digital token and send multiple identical tokens to multiple recipients. If an inconsistency can be incurred due to the transactions of duplicate digital tokens (e.g., double spent the same bitcoin token), then the double-spending problem becomes a serious security threat. To prevent double-spending, Bitcoin evaluates and verifies the authenticity of each transaction using the transaction logs in its Blockchain with a consensus protocol. By ensuring all transactions be included in the Blockchain, in where the consensus protocol[4] allows everyone to publicly verify the transactions in a block before committing the block into the global Blockchain, ensuring that the sender of each transaction only spends the bitcoins that he possesses legitimately. In addition, every transaction is signed by its sender using a secure digital signature algorithm. It ensures that if someone falsifies the transaction, the verifier can easily detect it. The combination of transactions signed with digital signatures and public verification of transactions with a majority consensus guarantees that Bitcoin Blockchain can be resistant to the double-spending attack.

3.5 Resistance to the Majority (51%) Consensus Attack

This attack refers to the risks of cheatings in the majority consensus protocol. One of such risks is often referred to as the 51% attack, especially in the context of double-spending. For example, the 51% attack may occur in the presence of malicious miners. For example, if a miner (verification user) controls more than 50% of the computing power for maintaining the Blockchain, the distributed ledger of all transactions of trading a cryptocurrency. Another example of the 51% attack may happen when a group of miners collude to perform a conspiracy, e.g., with respect to counting the miners votes for verification. If one powerful user or a group of colluding users controls the Blockchain, then various security and privacy attacks may be launched, such as illegally transferring bitcoins to some target wallet(s), reversing genuine transactions as if they were never occurred, and so forth.

3.6 Pseudonymity. Pseudonymity Refers to a State of Disguised Identity.

In Bitcoin, addresses in Blockchain are hashes of public keys of a node (user) in the network. Users can interact with the system by using their public key hash as their pseudo-identity without revealing their real name. Thus, the address that a user uses can be viewed as a pseudo-identity. We can consider the pseudonymity of a system as a privacy property to protect user's real name. In addition, users can generate as many key pairs (multiple addresses) as they want, in a similar way as a person can create multiple bank accounts as she wishes. Although pseudonymity can achieve a weak form of anonymity by means of the public keys, there are still risks of revealing identity information of users.

4. Blockchain Monitoring Systems

Figure 1 summarizes Blockchain layout that we see the need of including monitoring, a typical Blockchain network consists of a set of interconnected nodes that act as pairs. These nodes are typically hosted on a cloud / on-premises infrastructure where the Blockchain runtime is configured natively on a virtual machine (VM) or using containerization technologies such as Docker. Transactions submitted to the Blockchain network are broadcast to all pairs and new blocks created are propagated, so that all pairs have an updated copy of the shared ledger. To get an overview of the block, regarding its transaction-related events and associated metadata, monitoring one of the pairs is sufficient. And is usually done with the help of Blockchain explorer[6], which listens for events and provides some visualization of how many transactions were received, queued, processed, and ultimately consolidated into a new

block. However, this level of monitoring does not provide any clues as to the resources usage on that node or the other nodes' health or the latency felt within the Blockchain network[6], [8], [11], [12].

Another key element that needs to be monitored to gain end-to-end visibility of a Blockchain-based solution is the off-chain components which includes the application layer (decentralized application). The DAPP layer includes a user interface, storage and SDK (Software Development Kit) API (Application Program Interface) components, through the interaction with a Blockchain node is enabled [2], [11].

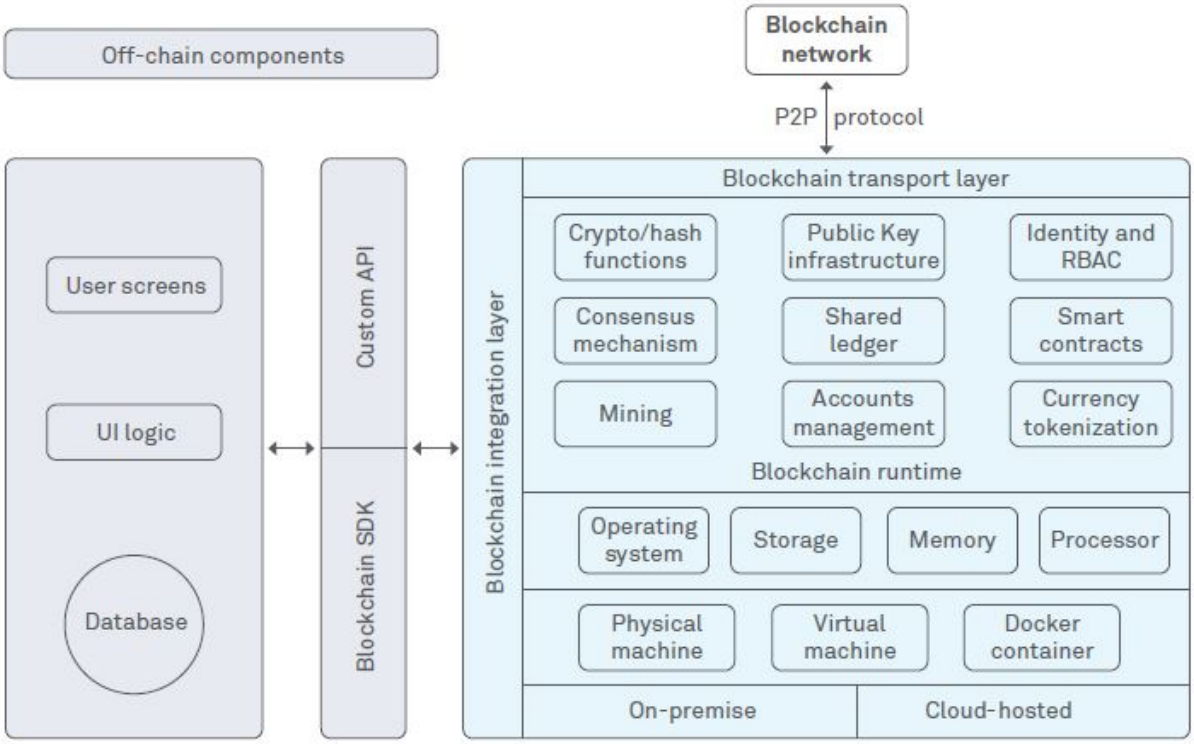

Fig.1 Blockchain layout needing monitoring

5. Proposed Blockchain Monitoring Framework

The effective monitoring and management of a Blockchain network provides a framework, which can integrate data, assimilate generated events, and provide efficient visualization of Blockchain-related matrices. This framework should be modular and support deployment topologies, which can enable monitoring both, an individual node level and the level of entire Blockchain network as a one element.

As shown in Figure 2, the diagram describes a proposed Blockchain monitoring framework, which includes the following elements:

- A monitoring agent[5], which is deployed on each Blockchain node and associated application infrastructure, can read logs generated as part of the transaction process and relay CPU, memory, and device usage data. I / O
- A log collection[3], [10] engine that manages streaming log information and assimilates it for further processing
- The elastic node cluster [13], [14], which processes a large amount of log data to organize and index it in corresponding documents, which are shared and stored as replicas

- A visualization platform [3], [15], [16], consumes the data gathered by elastic nodes and provides Blockchain node efficiency and network overview statistics
- Allows parties to conduct analytical research and generate reports
- Taking advantage of the proposed monitoring framework provides [12], [17]for:
  - Analyze how the processing of Blockchain transactions and the consensus mechanism uses the underlying infrastructure resources
  - Provide visibility into a business transaction - end to end - presented is initiated by a user from the dApp and captured in the Blockchain
  - Combine and correlate block and transaction related events from each node and determine the performance and throughput of the Blockchain network.
  - Configure a non-invasive monitoring solution that can be dynamically activated for each integrated pair and also support a common network provider model.

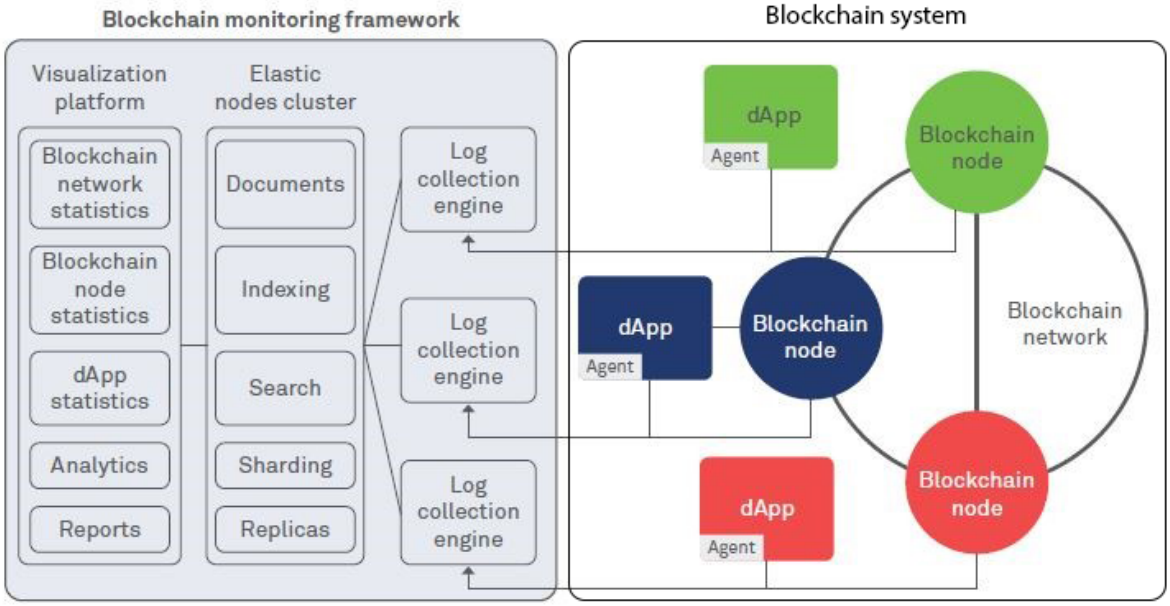

Fig.2 management and monitoring of Blockchain

6. Conclusion

While there is no shortage of monitoring solutions, the technique to effectively exploit existing Blockchain network monitoring mechanisms are not well thought out. The main reason is that few business use cases have translated into Blockchain production systems yet. Additionally, the decentralized nature of the Blockchain begs the question: is monitoring of the entire Blockchain network really necessary?

To maintain, analyze, and improve a blockchain-based business solution, a holistic monitoring solution is needed. This can further be combined with DevOps tools to enable maximum availability of the Blockchain network and ensure business continuity. It is for this reason that we have proposed a monitoring framework for a blockchain system and this proposal is supported by the work of Robert F. Rosin in his article Supervisory and Monitor Systems [1]. In addition, the establishment of a blockchain monitoring system could make it possible to detect anomalies or fraud in the entire system and for example to reject transactions even before the update of the blockchain registers.

The next step in our work would be to follow an approach that would allow us to design a model on a private blockchain in order to see the possibilities of exploitation, and list all the information; logs, and statistics that can be

used to detect an anomaly and subsequently see the possibilities of integrating this solution into public blockchain networks.

References

[1] R. F. Rosin, "S u p e r v i s o r y and M o n i t o r S y s t e m s PRE-1956 : JOB-BY-JOB . PROCESSING," no. 1, 1956.

[2] D. López and B. Farooq, "A multi-layered blockchain framework for smart mobility data-markets," *Transp. Res. Part C Emerg. Technol.*, vol. 111, no. January 2019, pp. 588–615, 2020, doi: 10.1016/j.trc.2020.01.002.

[3] M. Gorge, "Making sense of log management for security purposes - an approach to best practice log collection, analysis and management," *Comput. Fraud Secur.*, vol. 2007, no. 5, pp. 5–10, 2007, doi: 10.1016/S1361-3723(07)70047-7.

[4] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, 2019, doi: 10.1145/3316481.

[5] R. Ward and R. Ward, "Cognitive conflict without explicit conflict monitoring in a dynamical agent," *Neural Networks*, vol. 19, no. 9, pp. 1430–1436, 2006, doi: 10.1016/j.neunet.2006.08.003.

[6] M. J. W. Rennock, A. Cohn, and J. R. Butcher, "Blockchain Technology Regulatory and Investigations," *J. Litig.*, no. March, pp. 34–44, 2018.

[7] E. G. Sirer, "Bitcoin Guarantees Strong, not Eventual, Consistency," vol. 1, no. Security and Privacy on Blockchain, p. 1:35, 2016, [Online]. Available: http://hackingdistributed.com/2016/03/01/bitcoin-guarantees-strong-not-eventual-consistency/.

[8] W. Liang, Y. Fan, K. C. Li, D. Zhang, and J. L. Gaudiot, "Secure Data Storage and Recovery in Industrial Blockchain Network Environments," *IEEE Trans. Ind. Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020, doi: 10.1109/TII.2020.2966069.

[9] Y. Fu, "OpenCollab: A Blockchain Based Protocol to Incentivize Open Source Software Development," 2017, [Online]. Available: http://www.cs.dartmouth.edu/reports/TR2017-831.pdf.

[10] O. Choudhury, I. Sylla, N. Fairoza, and A. Das, "A blockchain framework for ensuring data quality in multi-organizational clinical trials," *2019 IEEE Int. Conf. Healthc. Informatics, ICHI 2019*, no. February, 2019, doi: 10.1109/ICHI.2019.8904634.

[11] P. Helebrandt, M. Belluš, M. Ries, I. Kotuliak, and V. Khilenko, "Blockchain Adoption for Monitoring and Management of Enterprise Networks," *2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018*, pp. 1221–1225, 2019, doi: 10.1109/IEMCON.2018.8614960.

[12] K. Jaswal *et al.*, "Management and monitoring of IoT devices using blockchain," *Sensors (Switzerland)*, vol. 18, no. 1, pp. 81–82, 2019, doi: 10.1136/adc.53.1.81.

[13] C. de Alfonso, A. Calatrava, and G. Moltó, "Container-based virtual elastic clusters," *J. Syst. Softw.*, vol. 127, pp. 1–11, 2017, doi: 10.1016/j.jss.2017.01.007.

[14] A. Calatrava, E. Romero, G. Moltó, M. Caballer, and J. M. Alonso, "Self-managed cost-efficient virtual elastic clusters on hybrid Cloud infrastructures," *Futur. Gener. Comput. Syst.*, vol. 61, pp. 13–25, 2016, doi: 10.1016/j.future.2016.01.018.

[15] A. Bujari, O. Gaggi, and C. E. Palazzi, "A mobile sensing and visualization platform for environmental data," *Pervasive Mob. Comput.*, vol. 66, p. 101204, 2020, doi: 10.1016/j.pmcj.2020.101204.

[16] H. Ma *et al.*, "Novel platform for visualization monitoring of hydrolytic degradation of bio-degradable polymers based on aggregation-induced emission (AIE) technique," *Sensors Actuators, B Chem.*, vol. 304, p. 127342, 2020, doi: 10.1016/j.snb.2019.127342.

[17] D. Bernard, M. Azouazi, M. Yassine, and E. Ghoumrari, "ScienceDirect Blockchain management and monitoring .," vol. 00, 2020.