BlockChains and IoT: A Literature Review

MEHMET DEMIR, Ryerson University, Canada

BlockChains are immutable distributed ledgers. BitCoin is a well-designed example of BlockChain model for monetary transactions. With the current popularity and success of the BlockChains, we are looking for further implementation opportunities of distributed immutable ledger technology. InternetOfThings (IoT) universe consists of devices in communication with each other. These devices add value by providing services. We believe that the next generation of IoT services would only be possible with democratic autonomy of devices in an environment where privacy, trust, transparency and security are provided. Peer-to-Peer interaction, trustless networks and financial transaction capabilities are main features that BlockChains enable for the next generation IoT. Smart Homes are the smallest scale implementation while Smart Cities are the largest model. Smart Homes model faces challenges from several low capability devices. Home devices' cryptographic abilities are not enough for BlockChain operations. On the other hand Smart Cities will see the volumes that billions of devices produce. We point out issues of BlockChains in IoT universe. We also identify research gap that should be filled in order to overcome the most important issues.

Additional Key Words and Phrases: Internet of Things, Security, Privacy, BlockChain, Trustless Networks

ACM Reference Format:
Mehmet Demir. 2017. BlockChains and IoT: A Literature Review. 1, 1 (October 2017), 6 pages. https://doi.org/0000001Mehmet.0000001Demir

1 INTRODUCTION

InternetOfThings (IoT) is the network and ecosystem of devices that collect and share data. This network of billions of devices demands more of everything. Network bandwidths are increasing to enable a high volume of communication. Wireless technologies and networking are increasing their coverage to include more participants. IoT infrastructure components are connecting devices to collect a massive amount of high quality data and to provide further intelligent services.

A distributed ledger is a dataset that is shared between participants of a network. This shared set of data can be stored and modified in the system. Most common reason to maintain such a ledger is to share the data related to interactions between the participants of the network. There are live examples of distributed ledgers for discovery services [6, 9] , virtual server management services [17] and monetary services [13, 14].

Distributed ledger definition above does not restrict the structure of the data. We are mainly focusing on the wide variety of possible technologies that can store shared information in a distributed way where the dependency on a central authority to produce and share the data is avoided. Even though the requirements change for each use case, quality is defined by the currency, availability, reliability and validity of the information. Currency and availability features are mostly provided by communication layers. Reliability and validity are specific to the security aspect of the distributed ledgers.

A BlockChain is a type of distributed ledger that is mainly focusing on providing solution to the requirements in the security domain. BlockChains provide ability for the participants to be collectively responsible for the reliability and validity of the data. Collective responsibility may change with the type of implementation. Some BlockChain implementations choose to be private where the rights of the participants are well defined and restricted based on their role. Other and

Author's address: Mehmet Demir, Ryerson University, Toronto, ON, Canada, mehmet.demir@ryerson.ca.

more popular BlockChains are public where all participants have equal rights and responsibilities for security within the consortium building capabilities of the network.

Most common risk related to a distributed ledger is the dishonest network participants trying to insert fraudulent information. BlockChains are developed in order to solve this problem and to keep the information protected when the transaction processing is completed. BlockChains commonly use cryptographic methods to fulfill this requirement. A block is a set of transactions collected in a specific time frame. Using cryptographic logic, a participant can seal the block by creating a hash of it. Whenever seal of the block is completed, it is communicated to the network. Nodes build consensus to verify block's validity. BlockChain network can verify if the block contains the correct data and valid hash. Once accepted, the information in the freshly sealed block becomes immutable under the brand new block that network starts building on top of it right after.

By placing hash of each block in to the content of the next block, system connects the blocks and form a chain. Hashing and sealing a block ensures modified data to be easily identifiable. It is extremely expensive to modify old data since it will require every block after the modified block to be re-hashed and re-validated. Even if this expensive operation is completed, distributed ledger implementations require consensus to accept the new blocks. Changes in the old blocks would be detected and rejected by other nodes of the network in comparison with their local copies of the distributed ledger.

Following sections will detail features of BlockChains that are related to IoT. We review the applications of BlockChains in IoT scope. And we review the issues of BlockChains in IoT. In the last section, we provide criticism to the literature coverage on key issues.

2 BLOCKCHAINS AND IOT

2.1 Significance

There is unlimited implementation potential for an immutable distributed data sharing mechanism. Big technology companies are investing in this technology [3] . They even started offerings private BlockChains [4] for their risk-averse clients.

Several countries are investing in programs to adapt this technology [19]. Even central banks are considering in their own implementations [12]. Importance of the BlockChains is beyond the BitCoin. The real innovation is the trust machine created with the networking nodes that is sustaining these cryptocurrencies. [1].

IBM predicts winners of the IoT technologies will be the ones that can decentralize peer-to-peer systems and can lower the costs. The winning choice would be privacy and long term sustainability instead of full control of data[15]. With this guidance, we will list the features of BlockChains can serve to the IoT space.

2.2 Peer-To-Peer networking

Members of the BlockChain network (nodes) are in peer-to-peer interaction in order to enable operations of the BlockChain. There are defined standards, but there is no single authority to operationally manage the system. Each involved node, by complying with the standards, is equally responsible for successful operation of the system within the rules of the BlockChain.

There are several issues in the IoT world that can be solved with collaboration. A good example of how a peer can provide a solution to a device to upgrade its firmware after the manufacturer disconnects the necessary service [7]. Discovery information about the correct firmware file and conditions to receive such service can be made available with smart contracts. For instance properties of the file and the hash of the file can be specified in the contract in order to help requesting parties authenticate supplied file.

Decision making mechanisms based on peer-to-peer networking is essential for IoT. There are no central trust figures or authorities anymore. A community of peers in the form of a peer-to-peer network fulfills this requirement where all decisions are made collectively and unilateral choices are prevented[18]. Since devices on the Internet will have to act independently and have to carry their operations individually, peer to peer solutions are essential for IoT adoption.

For IoT based systems, addition of one more node should be as easy as plugging a device to the network. Especially if this new node or device is equipped with required storage and cryptographic processing capabilities, it is easy to start it as a member of the BlockChain community.

2.3 Trustless Networks

Trust is important to online transactions [5]. Building trust is a time consuming activity that delays the progress. Currently, most payment systems are built around central authorities in order to expedite the trust. Credit card companies manage the payments and provide trust to both sides of trade. How can we handle trust in a peer-to-peer network without any central authority?

BlockChains enable trustless networks [7]. BlockChain model actually removes the need for trust with full transparency and anonymity. Any node can download and maintain the immutable history of transactions. This makes every detail available to every node in the system transparently. Even though every transaction information is available to all, identity of the participants are hidden behind their public keys.

BlockChains take care of the trust issues between parties. A BlockChain based economic system makes transactions trust-free[18]. This is a significant advantage compared to the traditional systems. Having a reliable party is often expensive considering legal or monetary responsibility. Traditional processes also take longer time due to time spent on complicated processes of central authority.

2.4 Financial transactions

New payment systems based on BlockChains already are integrated into the economy. We can predict further transformations. World markets will reimagine the definition of commercial interactions with this new technology. Partners in this new commence will utilize this trust-free environment with new style of interactions[18]. Education and repeated experiences will enable shoppers to adopt the trust free services provided by the BlockChains.

BlockChain technology replaces single authority with public acceptance. IoT needs easy integration and IoT demands an environment that doesn't care whether transacting parties are human or a device. In the new realm of BlockChains, new entrant does not require any central authority to provide explicit trust in the form of a credit score. This kind of standard and easy access to a billing platform will empower the BlockChain enabled devices. Service provided in the system can be compensated with peer-to-peer payment. With payment being possible, there would be more service providers willing to serve. Without the ability of a driverless car to pay, it is not convincing enough to produce parking spots for them. But with such ability, services would be provided. A marketplace of services between devices can be created with a convenient billing layer such as solar panels selling electricity to neighbour devices [7]. Such examples are rare at the moment but executing contracts without human intervention will be revolutionary for IoT sector.

Currently, most supply-chain systems are managed centrally. There is a heavy burden on this central authority to collect information, recognize events and take actions such as billing and payments. Consider the example where a package is transported through several handovers [7]. Several events in this transportation scenario can be stored in a BlockChain utilizing all the features related to being a ledger. Moreover, when the delivery events happen, smart contracts can be executed automatically and pay transaction related fees. Companies at distributed locations can conduct business without the need for traditional trust or central management but only with BlockChain technology where every event and action is recorded immutably.

3 TWO MAIN APPLICATIONS OF BLOCKCHAINS FOR IOT

"The most demanding use of the Internet of Things involves the rapid, real-time sensing of unpredictable conditions and instantaneous responses guided by automated systems" [11]. Starting from these technically challenging requirements, we present two popular implementation domains of IoT: Smart Cities and Smart Homes.

3.1 Smart Cities

A Smart City is a collection of integrated assets utilizing modern and secure communication technologies to produce better services for residents. Smart Cities are the service relationships between human, technology and organizations [18]. Besides the human and organizational involvement, we build Smart Cities by applying technology to the shared services and infrastructure. Advanced utilization of the technology resources and devices towards sharing economy enhances the Smart Cities.

People, organizations and devices in the Smart City concept has complicated technology requirements. Technology platforms need to provide automation, democratization, distributed computing, trustless environments, transparency, privacy and security. BlockChain is the right solution since it fulfills all these requirements. BlockChains provide an environment where peers are collaborating towards building a distributed information management system and they are using smart contacts for automated event based actions. Most trust issues are handled with the transparency and consensus while their identity and vulnerabilities are protected by the inherent privacy and security.

3.2 Smart Homes

Smart Homes are the micro blocks of the IoT architecture. In order to reach more sophisticated levels in IoT, one of the most important target is integrating all sensors and devices. There is a need for data sharing and information integration. This also needs to be on a secure platform since privacy is a big concern when data is collected from people's homes.

Distributed ledgers would be a great tool to integrate the home devices. But with their current model BlockChains are not suitable for crowded and high volume IoT architectures. BlockChains are computationally expensive, create high network overhead and result in delays [10]. This combination is not suitable for most IoT devices situated in a house. Most of these simple devices don't have the computation power, cryptographic ability and storage capacity. Most devices also have low adaptation capacity for new technologies. A new type of distributed ledger is needed.

One of the proposals is a lightweight BlockChain-based hybrid architecture with three layers [10]. Layered architecture consists of Smart Home, overlay and cloud storage. This architecture will integrate the home devices with a private immutable ledger that is managed centrally. This private ledger will avoid expensive cryptography such as proof-of-work and will not need to build consensus. At each home, a Smart Home Manager manages this house ledger. Local storage and local keys will be used for the cryptographic operations and ledger storage. Devices in the home and overlay node structure can create transactions. Overlay layer is the clustered members of the network. Each cluster has a head that has the cryptographic community information such as the public keys of the members of the cluster. There would be a request-trust pairing for the transactions generated from a cluster and a history of transactions for cluster and members would be maintained. Blocks will be formed and accepted at this layer. Forking and related problems are solved at this layer as well. Cloud storage is where the data is stored in blocks.

4 DISCUSSIONS

BlockChains have some great features for IoT. These features also are costly. In this section, we will review the issues related to BlockChains and IoT. We will also provide our opinion related to literature coverage.

IoT demands speed and volume. BlockChain systems have lower transaction throughput and higher latencies. They severely underperform compared to traditional models. Trustless decentralization and resiliency is costly and causes this performance hit. In the decentralized model of BlockChain, each node performs the same task instead of benefitting from parallel execution[7]. This is the reason that IoT systems are looking for hybrid architectures. As the scale changes, we believe there would be a need for more layered solutions. Smart Homes will have layers, public buildings will have different layers and cities should have even more layers. One BlockChain architecture can not satisfy the needs of a city with its billions of devices.

IoT systems have high level of dependency on events and their outcomes. Smart contracts seem to be a solution to this requirement. Current implementations of smart contracts have concurrency issues. They have to be executed on a single node. This dependency on serial execution impacts the performance of the large systems. Parallel execution has further vulnerabilities such as re-entrancy attacks [8]. Such risks of BlockChains are not discussed extensively in the literature.

Most IoT projects currently focus on providing service to people. Whether it is Smart City or a Smart Home, personal information is at stake. Privacy is still a big concern while using BlockChains. BlockChains is built on transparency. BlockChains can hide personal information but complete confidentiality is hard to attain. There are breadcrumbs stored in the chain that may lead to precise information. Transactions and contract information can potentially be traced to more information. This subject is not discussed extensively in the literature.

Devices have more disadvantages compared to the human-to-human interaction systems. Recognizing and fixing BlockChain issues within devices can be time consuming and expensive. Tolerance to exceptions is very low in the IoT interaction scenarios. We can not imagine devices to be very fuzzy and act creatively to handle unexpected issues. Therefore a potential issue for a human managed system can turn out to be a big risk for autonomous device environment. This aspect is not discussed in these papers.

Whether the work is done at the lower or higher levels, whenever there is BlockChain and security is required, there is a high demand for cryptography. Literature does not mention the cost of cryptographic operations in current implementations. IoT universe consists of devices. How can we improve these devices. Would a separate cryptographic circuit is needed? Is there a way to outsource the work? Can we have this work done in network devices such as routers or switches. Costs as high as BitCoin systems accrue are a potential no-go for IoT projects.

BlockChain participants have a vulnerability at the legal platforms. It is not straightforward what participants can do and which rights they have in front of the court of law. Enforceability of the smart contacts is very limited [7]. This translates into a big problem in finance sector [16]. Lack of clarity about jurisdiction [2] and how smart contracts would be treated in court continues to be a obstacle for future adoption.

Besides all technical points in the reviewed papers, there are not many realistic examples of revenue generation and willingness of trusting a wallet to a device. And finally, literature currently only covers the BlockChains as a distributed ledger. But there are other technologies that can play the same role. There is a crypto currency named Iota suggesting a new type of distributed ledger named Tangle [14]. IOTA argues to be the crypto currency for the IoT. We think a low-cost or a no-cost crypto currency would revolutionize IoT.

5 CONCLUSIONS

BlockChain technology is one of the most popular subjects among researchers due to its revolutionary implementation of distributed ledgers. It brings several advantages to the platforms enabling transactions and contracts. IoT universe needs a distributed information sharing mechanism such as BlockChains in order to reliably share the transaction information and in order to facilitate contractual agreements. This can not be done without addressing several issues listed in this paper. We need new architectures that can carry billions of transaction creating devices. This has to be done while solving performance, privacy, exception handling and legal issues. A balanced chequebook will be very important as well.

REFERENCES

[1] 2015. The promise of the blockchain: The Trust Machine. (Oct. 2015). Retrieved October 10, 2017 from https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

[2] 2016. Smart contracts pose enforceability issues. (Nov. 2016). Retrieved October 10, 2017 from http://www.businessinsider.com/smart-contracts-pose-enforceability-issues-2016-11

[3] 2017. Oracle BlockChain Cloud Service. (2017). Retrieved October 10, 2017 from https://www.oracle.com/cloud/blockchain/index.html

[4] 2017. Oracle BlockChain Cloud Service eBook. (2017). Retrieved October 10, 2017 from https://cloud.oracle.com/opc/paas/ebooks/Oracle_Blockchain_Cloud_Service.pdf

[5] Amit Bhatnagar, Sanjog Misra, and H. Raghav Rao. 2000. On Risk, Convenience, and Internet Shopping Behavior. *Commun. ACM* 43, 11 (Nov. 2000), 98–105. https://doi.org/10.1145/353360.353371

[6] Arne Bröring, Soumya Kanti Datta, and Christian Bonnet. 2016. A Categorization of Discovery Technologies for the Internet of Things. In *Proceedings of the 6th International Conference on the Internet of Things (IoT'16)*. ACM, New York, NY, USA, 131–139. https://doi.org/10.1145/2991561.2991570

[7] K. Christidis and M. Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* 4 (2016), 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[8] M. Coblenz. 2017. Obsidian: A Safer Blockchain Programming Language. In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*. 97–99. https://doi.org/10.1109/ICSE-C.2017.150

[9] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini. 2017. CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In *2017 IEEE International Conference on Communications (ICC)*. 1–6. https://doi.org/10.1109/ICC.2017.7996641

[10] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. 2017. Towards an Optimized BlockChain for IoT. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17)*. ACM, New York, NY, USA, 173–178. https://doi.org/10.1145/3054977.3055003

[11] Chui M., M. Löffler, and R. Roberts. 2010. The Internet of Things. (March 2010). Retrieved October 10, 2017 from https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things

[12] et al. Mills, D. 2016. Distributed ledger technology in payments, clearing, and settlement. (2016). Retrieved October 10, 2017 from https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

[13] S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). Retrieved October 10, 2017 from http://bitcoin.org/bitcoin.pdf

[14] S. Popov. 2017. The Tangle. (Oct. 2017). Retrieved October 10, 2017 from https://iota.org/IOTA_Whitepaper.pdf

[15] V. Pureswaran and P. Brody. 2015. Device democracy- Saving the future of the Internet of Things. (2015). Retrieved October 10, 2017 from http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/

[16] N. R. 2016. Can smart contracts be legally binding contracts? (2016). Retrieved October 10, 2017 from http://www.nortonrosefulbright.com/files/norton-rose-fulbright--r3-smart-contracts-white-paper-key-findings-nov-2016-144554.pdf

[17] Mayra Samaniego and Ralph Deters. 2016. Using Blockchain to Push Software-Defined IoT Components Onto Edge Hosts. In *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies (BDAW '16)*. ACM, New York, NY, USA, Article 58, 9 pages. https://doi.org/10.1145/3010089.3016027

[18] Jianjun Sun, Jiaqi Yan, and Kem Z. K. Zhang. 2016. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation* 2, 1 (13 Dec 2016), 26. https://doi.org/10.1186/s40854-016-0040-y

[19] D. Tapscott and A. Tapscott. 2017. How Canada can be a global leader in blockchain technology. (March 2017). Retrieved October 10, 2017 from https://beta.theglobeandmail.com/report-on-business/rob-commentary/how-canada-can-be-a-global-leader-in-blockchain-technology/article34259697/