IJIRIS: International Journal of Innovative Research in Information Security
Volume 09, Issue 03, June 2023
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives

IoT Based Blockchains and IPFS

Dr. A.Mahesh, Professor,
Dept. of Computer Science and Engineering
Sri Sairam College Of Engineering,
Bangalore,India
Mahesh.cse@sairamec.edu.in
Shaibha.B, Shabu B, Nagella Nithish Sai
Dept. of Computer Science and Engineering
Sri Sairam College Of Engineering,
Bangalore, India

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.09/Issue03/JNIS10112
Research Article | Open Access | Double-blind Peer-reviewed |Article ID: IJIRIS/RS/Vol.09/Issue03/JNIS10112
Received: 02, June 2023 | Accepted: 20, June 2023 | Published: 23, June 2023
Volume 2023 | Article ID JNIS10112 http://www.ijiris.com/volumes/Vol09/iss-03/33.JNIS10112.pdf
ArticleCitation: Mahesh,Shaibhu,Shabu,Nageela,(2023).IoT Based Blockchains and IPFS. International Journal of Innovative Research in Information Security (IJIRIS), 10, 234-241 **doi:** https://doi.org/10.26562/ijiris.2023.v0903.33
BibTex key: **Mahesh2023IoT**

Copyright: ©2023 This is an open access article distributed under the terms of the Creative Commons Attribution License; which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract : Block chain, the underlying technology of crypto currency networks like Bitcoin, is designed to realize the vision of a decentralized, secure and open Internet of Things (IoT) revolution with a centralized data access model. Essential. It may be so. This article proposes a distributed access model for IoT data using a network architecture called the IoT and Blockchain Modular Consortium Architecture. The proposed architecture facilitates IoT communication via a blockchain software stack and a peer-to-peer data storage mechanism. This architecture is intended to provide privacy and be adaptable to various IoT use cases. To implement the proposed architecture, we conduct a performance analysis of existing blockchain development platforms, Ethereum and Monax. .

Keywords : Internet of Things; Privacy; Blockchain; Distributed Access Model; Computer Networks

INTRODUCTION

These devices monitor and collect information about the environment and communicate with each other to perform automated tasks and services. Despite the benefits of IoT, the vast amount of data generated by IoT can raise privacy concerns. His current IoT implementation is based on a centralized client/server- based access model, with user data entrusted to central service providers. IoT devices and the data they generate can reveal personal information such as user actions and behaviour. preferences. Centralized service providers can make illegitimate use of IoT data; mass-surveillance programs being one example [1]. The aim is to introduce user data protection to IoT. Build a decentralized IoT with built-in data protection. A world of direct, data-driven insights means IoT data will flourish, be democratized, and be made available to users. Having complete control over your data is revolutionary. A model of digital commerce [2]. A decentralized IoT data controller allows you to share or sell sensor data without passing it to third parties. The goal, therefore, is to eliminate the need to hand over user data to central authorities or institutions through the IoT's decentralized data access model. It belongs to the user, not the company. Blockchains and other peer-to-peer techniques can prove to be crucial in realizing this goal [3]. The blockchain is a peer- to-peer distributed data structure that represents an immutable ledger of 'transactions'. The transactions refer to data exchanges that occur in a network. In cryptocurrency networks, the transactions involve transfer of cryptocurrency. In a blockchain network, the entire ledger is distributed over all the nodes, and every node casts a vote over the validity of every new transaction that is added to the ledger. Since the same copy of the blockchain is maintained over all the nodes using peer-to-peer consensus algorithms, there is no central entity entrusted with maintaining transaction records. Therefore, blockchains create a 'trust- less' environment with accountability built into it. Towards a decentralized data access model for IoT data privacy, we propose an IoT network architecture that we call a 'modular consortium network'. In this architecture, we use a software stack of block chain and IPFS (the peer-to-peer 'Interplanetary file system') to provide decentralized access control. Furthermore, the block chain provides an immutable log of all IoT data operations including sensor data creation and IoT data access. The IoT devices being used for any singular use case are grouped together into private block chains, or 'side chains'. Users can own multiple side chains, and each side chain network is made responsible for maintaining a secure log of the IoT data operations that occur within it. The side chain networks are connected in a modular fashion to a larger, decentralized peer-to-peer 'consortium' network, which runs its own block chain.

The consortium block chain is responsible for securely logging any incoming access requests for any user's IoT data, and

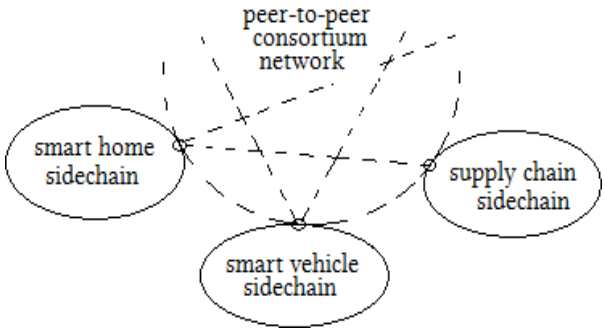


Figure 1. Modular consortium network, a decentralized peer-to- peer network made up of isolated side chain networks performing access control for those incoming requests. Figure 1 shows a high-level depiction of our modular consortium network. Here, modularity allows individuals or groups to seclude themselves, or information about themselves, and thereby express themselves selectively. Current blockchain development platforms are constantly evolving, and deployment considerations must be considered when applying blockchain-based applications in IoT. To better understand these deployment considerations, we conducted a performance analysis of existing blockchain platforms, Ethereum and Monax. The reason for this choice is the difference in the consensus mechanisms used by these platforms.

STATE OF THE ART

IoT data privacy continues to be a research challenge because of the lack of standardization in IoT, the sheer scale of IoT networks, and centralized access models for IoT data. Numerous research contributions have been made for enabling secure data accessing in the traditional 'client- server'-based access control models [4,5]. IoT service providers also use proprietary authorization techniques, where they act as centralized authorizing entities. However, centralized IoT data management and access control models lead to scalability issues in IoT, and force users to place their trust in centralized third-party intermediaries to manage their data, thus compromising user data privacy as well as end-to- end security [13]. As such, research focus is being drawn towards developing a decentralized security and privacy model for IoT, using blockchains along with peer-to-peer data storage mechanisms. The reason for the research popularity of blockchains in the IoT domain stems from their proven potential of providing security to large scale distributed networks, as seen in Bitcoin, and other cryptocurrency networks. In [6], the authors describe the capability of blockchains to maintain an immutable log of data exchanges as well as to perform access control. The access control element comes from creating access polices around the public key infrastructure (PKI) of blockchain networks [7,8]. Authors in [9,10] highlight the benefits of ensuring users' ownership of They discuss blockchain's potential to power the sensor data economy, where users with full ownership of their private data can sell their data to third parties. The authors of [11] describe data-centric protocols for data storage and data access, and add programmable access control mechanisms to blockchains while protecting user privacy in [12]. We propose a framework for implementing blockchains that enable access control. In [13], the authors leverage Ethereum's programmability to provide its blockchain development platform. IBM Adept [14], a collaboration between IBM and Samsung, aims to leverage blockchain to develop a decentralized platform for IoT. Adept uses TeleHash, the Ethereum blockchain development platform for peer-to-peer messaging, in addition to BitTorrent for peer-to-peer file sharing. The solution to IoT decentralization is the low scalability of blockchains and the latency inherent in blockchain consensus. The authors of [6] split the IoT blockchain network into smaller sub-networks because a single blockchain cannot scale sufficiently to perform consensus-based verification of transactions originating from a large and growing network. proposed [15]. The authors of [16] propose a layered architecture for blockchains in IoT, with overlaying his blockchain network connected to sub-networks of local blockchains. It provides access control by writing access policies in the blockchain header. Retrieving data from this network is done by sending IoT data stored in local storage or third-party cloud storage services to the requester. The Internet of Things as it exists today is a decentralized network of intelligent objects whose software and data management is provided by a centralized third-party provider. This client/server model not only increases network limitations, but also requires users to rely on a third party to manage their data without abuse. Therefore, the research question to be solved is to leverage blockchain and peer-to-peer data storage technologies for IoT privacy. With this technology, each user has complete authority over their data without leaving IoT software or data management to a third party.

MODULAR CONSORTIUM ARCHITECTURE FOR BLOCKCHAINS IN IOT

To provide decentralized access model for IoT data privacy, we propose an IoT network architecture we call the 'modular consortium' architecture. With this architecture, we aim to provide IoT data privacy via blockchains, and address the challenges associated with implementing blockchains to IoT networks, as discussed in the state of the art.

One of the challenges is the scalability of blockchains in IoT. Since every entry on the blockchain requires consensus among the network nodes, a single blockchain responsible for logging every IoT data operation would not scale well. To address this issue, we break the network down into smaller, private blockchains, or 'sidechains'. These sidechain networks are connected together to form one decentralized, peer-to-peer 'consortium' network. The benefit of implementing private sidechains is that the nodes participating in one sidechain's consensus algorithm don't have to validate or verify transactions occurring in an entirely different sidechain. Users can own and manage one or multiple sidechains as per the users' requirements. Each sidechain network is used separately for different IoT use cases, and can be added or removed from the consortium network in a modular fashion. To access IoT data on a sidechain, a request or must become a member of the peer-to-peer consortium network and submit an access request. A consortium network operates its own blockchain, which is called a consortium blockchain. The consortium blockchain will perform access control to prevent unauthorized access to her IoT data from the sidechain to another member of the consortium network. While each sidechain is responsible for logging sensor data creation events within the sidechain network, the consortium blockchain maintains a log of successful and failed data access requests made between members of the consortium. be responsible for. Separating logging responsibilities between sidechains and consortium blockchains can alleviate the problem of public disclosure of blockchain content. Having a single blockchain log all IoT data operations would compromise privacy as all members of the blockchain network would have access to the blockchain log content. However, in the case of our proposed architecture, each member of the consortium network will only have access to her record of IoT data access requests, and the logs of IoT data creation events will remain private within the sidechain. Applicant and Applicant Responsibilities Responsibility is given to both requesters and applicants by allowing members of the consortium network to access an immutable log of all successful and failed access requests. Consider a scenario where a user sells sensor data to a marketing company. User agrees to allow access to the company for her one month. If the user revokes access at the sidechain level by the end of the month, the company's access request will fail. And as evidence of misconduct by sidechain owners, the company can create time-stamped logs of failed access requests.

Blockchain and IPFS Software Stack

A decentralized access model, with privacy built into it by design, is made possible by a software stack of blockchains working on top of a decentralized peer-to-peer file system, IPFS. IoT data can be grouped together and stored in IPFS, while the blockchain itself only needs to hold the hash of the IPFS files containing the IoT data. The programmability and PKI properties of blockchains enable secure access control, and IPFS eliminates the need for centralized IoT data management.

Technology that enables: blockchainA blockchain is a peer- to-peer ledger that records transactions on a network. A transaction constitutes a transfer of data. Bitcoin is just one example of blockchain use cases where transactions represent transfers of cryptocurrencies. Public key cryptography is used to execute transactions. Nodes use their private keys to sign transactions and their public keys to address transactions to other nodes. Transactions are transferred to the blockchain network, and peers (also called "miners") responsible for validating transactions group them into candidate blocks. Validating peers who successfully solve a complex mathematical puzzle over the block's hash are selected and their candidate blocks are added to the blockchain. As shown in the diagram, each newly added block contains the hash of the previous block.2. Linking blocks in this way makes the content of the blockchain immutable, as changes in previous blocks are easily recognizable. The rest of the nodes validate that the new block is valid and update their copy of the blockchain. Each node holds the same copy of the blockchain, creating a "trusted" decentralized network.

Alternative block verification

methodThe method of validating new transactions in a block by computationally solving a puzzle is called "Proof-of- Work" (PoW). In PoW, a node that adds a new block to the blockchain is chosen based on competition to find a nonce that, when hashed with the rest of the block, returns a result containing a specified number of leading zeros. PoW-based consensus is therefore computationally expensive and laggy, both of which are undesirable in IoT. An alternative consensus algorithm, Proof-of-Stake (PoS), selects validator nodes to add candidate blocks in a pseudo-random fashion. The probability of a node being selected is proportional to its share in the network. The advantage of PoS is that it does not consume a large amount of computing power to validate and add new transactions to the blockchain. However, PoS leaves the network vulnerable to nothing-at-stake attacks [17]. This attack allows nodes to easily create branches in the chain without owning a share of the network or using much computing power. Blockchain development platforms that employ PoS such as Ethereum's Monax and Casper[18] deal with nothing at stake attacks by slashing the stake of any nodes that create false blocks. PoS provides us with the opportunity to further explore the viability of blockchains in IoT, since low processing requirements are desirable for IoT networks.

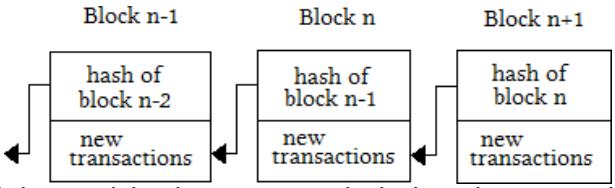


Figure 2. Blocks in a blockchain, with headers containing the hash to the previous block; the first block in the blockchain being the 'genesis' block

Smart Contracts and Blockchain Programmability

'Smart contracts' bring programmability to the blockchain, in the sense that they facilitate the execution of transactions while meeting the terms of a contract written in code. Smart contracts are deployed in the blockchain with specific addresses, so in order to invoke a function written in a smart contract, transactions are signed off by nodes and addressed to the smart contracts themselves. While smart contracts enforce terms and conditions for transactions in financial applications, they can enforce access control policies in the modular consortium architecture.

Enabling Technology: IPFS

IPFS (Interplanetary File System) aims to be a fully decentralized file system for the Internet [19]. IPFS currently makes up a subsystem of the Internet as one single peer-to- peer swarm, making file exchange over the Internet secure and open. IPFS files are content-addressed and are identified by their hashes. This makes them cache-friendly, and IPFS file hashes can be easily stored within the blockchain. IPFS is therefore, an ideal file storage and sharing platform for developing a decentralized access control model for IoT.

WORKING PRINCIPLES OF THE MODULAR CONSORTIUM ARCHITECTURE FOR IOT

Private Sidechains for IoT Users

The private sidechains maintain logs of all IoT data operations that occur within a private IoT network. The private IoT network consists of IoT devices and one validator node running the sidechain. The IoT devices are given unique public and private keys, which they use to send encrypted sensor readings to the validator node. The validator node logs any data received with authorized key encryption as data creation events. The validator node adds new blocks to the sidechain, and has higher computational power as well as storage space. A smart contract is deployed within the sidechain to perform the following functions:

- Storing a dictionary of each authorized smart device's public key and the hash of the IPFS file storing the smart device's data.
- Ensuring that only the data incoming from authorized smart devices are able to communicate with the sidechain validator.
- Storing a dictionary of public keys of requesters in the consortium network with access privileges, and the public keys of the smart devices whose data the requesters have access to.
- Performing access control on incoming access request transactions.

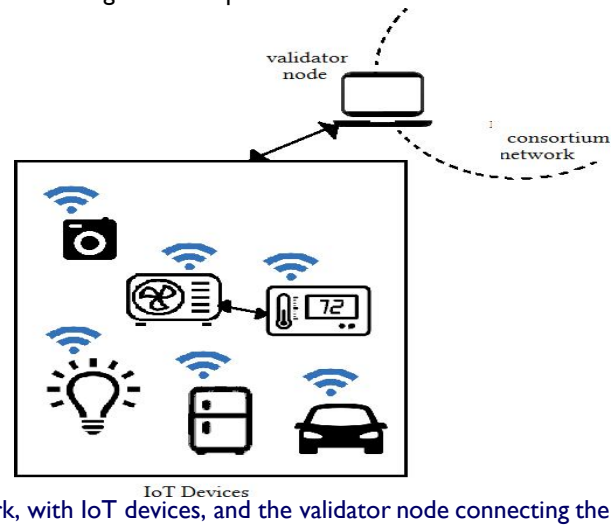


Figure 3. Sidechain Network, with IoT devices, and the validator node connecting the sidechain to the consortium

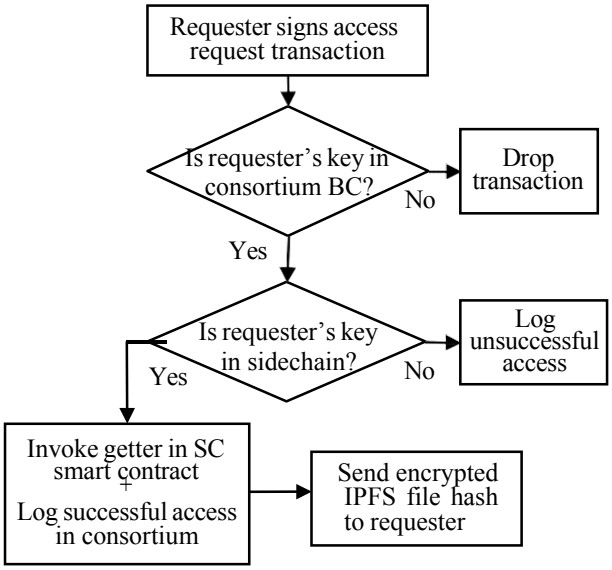
To add more IoT devices to the network, each new device will be given a public key, which will be stored onto the smart contract in the sidechain. Maintaining a list of authorized smart devices in the validator node ensures no unauthorized device can flood the validator node with fake incoming data.

Storing IoT Data

Whenever a smart device generates data, it encrypts it and sends it to the validator node. The validator node identifies any unauthorized device attempting to participate in the sidechain. Subsequently, the validator node blocks all incoming data packets from the unauthorized device. Upon receiving data from an authorized device, the validator node logs a 'creation of IoT data' transaction in a new block. The validator node then updates the IPFS file, as well as its hash stored in the smart contract.

Consortium Blockchain Network

The validator nodes in each sidechain are connected to form the decentralized consortium network, running a global consortium blockchain. The consortium blockchain carries within itself a smart contract that stores a list of the public keys of devices authorized to make access requests for IoT data. While the private sidechains are responsible for securely storing IoT data and keeping a log of all the local IoT events, the consortium blockchain is responsible for allowing access to the IoT data to external requesters who are given access privileges. The access policies written in the consortium blockchain's smart contract, together with the access policies written in the sidechain's smart contract, provide fine-grained access control so as to limit requesters to only be able to access the data of specific smart devices within specific sidechains.



Transactions Per Minute	Ethereum	Monax
10	~97%	~0.5%
300	~98%	~0.6%

Table 1. CPU usage on core-i7 laptop as validator node

Figure 4. Flowchart of steps for access control following an access request transaction

Accessing IoT Data

To access user data, a requester joins the consortium blockchain network via a client application as a participating peer, i.e., the requester can make requests for the data, but doesn't add blocks to the consortium blockchain. In the case of either IoT data sharing or selling, the sidechain owner adds the requester's public key to the sidechain's smart contract along with the amount of time the requester has access privileges. At this point, the validator node adds this same public key to the list of authorized requesters in the consortium blockchain. This is to ensure that the requester is only able to make access requests on the consortium level, if a sidechain owner vouches for them. To gain access to a user's IoT data, the requester signs an access request transaction with their private key. Figure 4 shows a flowchart of the steps taken in response to an incoming access request on the consortium network Upon receiving the encrypted IPFS file hash, the requester can decrypt it using their private key, and access the file containing the smart device's data via HTTP using www.ipfs.io/ipfs/<FileHash>. The ability to modify access policies gives the user the choice to share their IoT data with whomever they choose. The smart contract on the consortium blockchain also prevents requesters from flooding the consortium blockchain with unauthorized request transactions. After a requester makes a specified number of consecutive unsuccessful requests, the smart contract removes the associated public key from the list of authorized requesters.

IMPLEMENTATION AND PERFORMANCE ANALYSIS

To gain insight about the feasibility of implementing the proposed architecture and the relevant deployment considerations, we conducted a performance analysis of existing blockchain application development platforms on both the sidechain and consortium level. We used Ethereum, the blockchain development platform, whose cryptocurrency Ether is second only to Bitcoin. Other than Ethereum, we used Monax, the blockchain application development platform for business ecosystems. Ethereum achieves consensus via the PoW algorithm. Monax achieves consensus using the Tendermint [20] consensus engine, which employs PoS. Our testbed was built on a consortium of five validator nodes, each receiving incoming data from five smart devices. The performance metrics we used for our analysis were processing overhead, network traffic overhead and block processing times.

Processing Overhead

On the sidechain level, we conducted tests on CPU usage when validating new blocks with Ethereum and Monax. We compared processing overhead by comparing CPU usage of the blockchain client's specific process ID. Considering five smart devices are connected to each validator node, we carried out tests with varying number of incoming transactions from within the sidechain network. Throughout all variations in the incoming transactions, the processing overhead remained unchanged with both platforms. Therefore, in Table1, we display the processing overhead only for the lowest and highest transaction rates that we tested.

Network Traffic Overhead

In blockchain applications, there is network traffic overhead that comes from the nodes of the network participating in the consensus algorithm. We measured traffic overhead for the consortium blockchain, because the sidechains only involve one validator node. For this experiment, the rate of access requests transactions is assumed to be less than the data creation transactions within the sidechains.

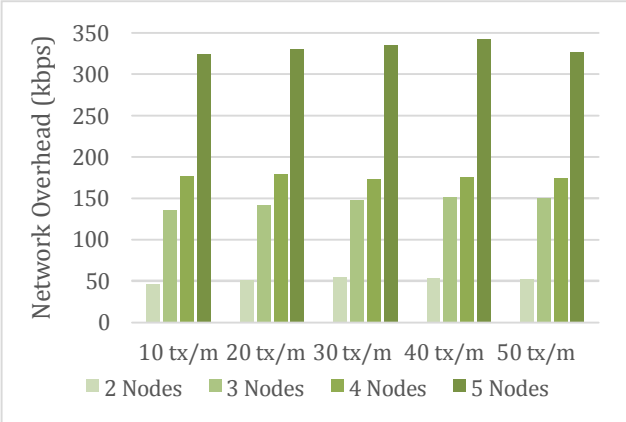


Figure 5. Network Traffic Overhead in Monax

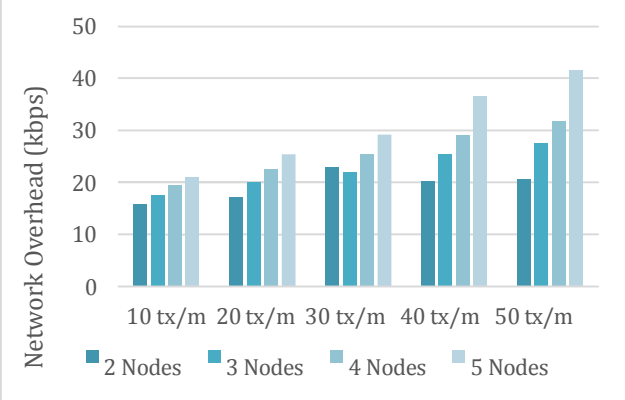


Figure 6. Network Traffic Overhead in Ethereum

As observed from the network traffic overhead coming from Ethereum and Monax, while Ethereum traffic does increase with increasing number of nodes in the consortium, it is significantly smaller than the traffic overhead of Monax. The high network overhead in Monax is due to the fact the the Tendermint consensus engine sends out empty blocks as heartbeat to check if a peer is up. Monax was developed for business applications and it was not meant to be used in a scalable public network, the way the consortium network aims to be. In this experiment, we measured network traffic with varying number of nodes in the consortium network, and varying amount of access request transactions incoming per minute. The observations we gathered from this experiment are illustrated in Figures 5 and 6.

Block Processing Time

In its current stage of development, Monax does not group different transactions into one block, and in our tests, it processed blocks consistently at ~1 block per second, with one transaction per block. On the other hand, Ethereum grouped transactions together in blocks. Figure 7 shows the block processing time information we obtained from the Ethereum client's log file. We ran the experiment with Ethereum for 60 minutes, and set the 'difficulty' in the genesis block to 200000. Difficulty relates to the hashing power required for processing. In this experiment, we observed a trend of rising difficulty and processing time with increasing number of blocks.

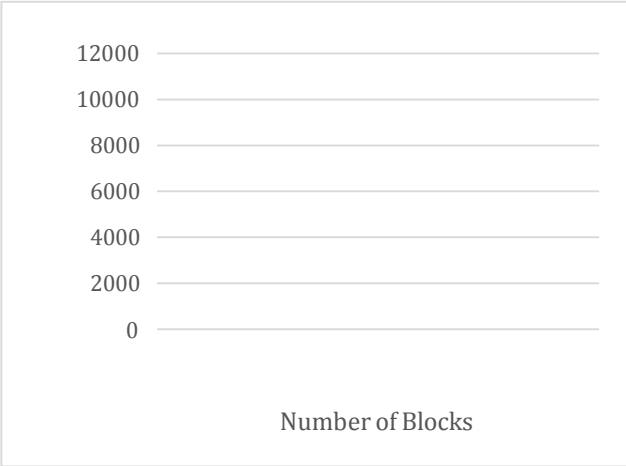


Figure 7. Block Processing Time in Ethereum

We have made the log files of our experiments available via IPFS and can be accessed here: http://ipfs.io/ipfs/QmPNUYLFu2To9b5YYgrpYqQeREph wqN9iBe5WyFnGrzQEp

DEPLOYMENT CONSIDERATIONS

While using Ethereum and Monax to implement the modular consortium architecture, there are certain deployment considerations that need to be made. Firstly, Monax blockchain development platform was built for private business applications, and judging from the network traffic overhead, it does not scale well on the consortium level. When used on the sidechain level, Monax outperforms Ethereum in terms of processing overhead. However, from the observations we made of Monax's block processing time, creation of data from different streams or IoT devices will need to be bundled together natively in the validator node, and logged together as a single transaction in Monax.On the consortium level, Ethereum performs well in terms of network traffic overhead, however, to validate new blocks on an Ethereum based consortium blockchain, every validator node will be faced with processing overhead. To alleviate the processing overhead from the validator nodes, separate dedicated validators can be set up on the consortium level. In that case, while validation of new blocks will not be fully decentralized, the members of the consortium network will be able to sign access request transactions and access the consortium blockchain. Even if one of the dedicated validator nodes is compromised, the sidechain owners' IoT data remains private, since access privileges are set at the sidechain level.

FUTURE WORK

We aim to continue our work with the modular consortium architecture by stress testing it against different use cases and with larger scale networks. We intend to implement other blockchain development platforms like Hyperledger and Parity to assess their suitability for our architecture, as well as design customized blockchains to optimize them specifically for IoT. Further work needs to be done on how to advertise the availability of certain data in a sidechain, either via broker or by keeping a list within the consortium smart contract. As of now, the architecture facilitates fetching data from specific time periods. More work will be carried out to maintain a data stream for valid requests via IPFS. We intend to explore blockchain pruning to combat the trend of rising block processing time, as well as conserving storage space on validator nodes.

CONCLUSION

In this paper, we propose a network architecture for providing IoT data privacy via blockchains and IPFS. In the proposed 'modular consortium' architecture, blockchain smart contracts perform access control, while providing accountability for both the data owners and the third parties whom the users allow access to. We built implementations of the architecture using two existing blockchain application platforms. Performance analysis of the blockchain platforms provided insights into the architecture's feasibility and further considerations for deploying a usable implementation. The main contribution of this paper is to implement a software stack of blockchain smart contracts and peer-to-peer file storage, to give IoT users authority over their data, and to eliminate the need for centralized IoT data management.

REFERENCES

[1]. The NSA Prisma program accesses user data from Apple, Google, etc. received in May 2, 2017 from https://goo.gl/2RCCQ
[2]. Vijay Shivaraman, Hassan Habibie Galakeili, Arun Vishwanath, Roxana Borelli and Olivier Mehani. 2015. Network-level security and privacy controls for smart home IoT devices. On Wireless and Mobile Computing, Networking and Communications (WiMob) at the 11th International IEEE Conference 2015. IEEE、163-167
[3]. Giskind, Guy, Oz Nathan, Alex Pentland. "puzzle: A decentralized computing platform with guaranteed privacy. XIV: 1506.03471 (2015).
[4]. Louise axons. 2015. Privacy awareness in his blockchain-based PKI. Retrieved from http on April 12, 2017://goo.gl/3Nv2oK
[5]. Dominik and Thomas von Boomhardt (Warner) 2014. When sensors make money: Exchange your data for cash using Bitcoin. In his 2014 ACM International Joint Conference Proceedings on Pervasive and Ubiquitous Computing, he states: Supplementary Publications, 295-298
[6]. Shafag Hossein, Anwar Hisnawi, and Simon Duquenoy. 2017. Toward blockchain-based auditable IoT data storage and sharing. arXiv preprint arXiv: 1705.08230 (2017)
[7]. Decentralized data protection:Protect your personal data using blockchain. As part of the IEEE Security and Privacy Workshop (SPW) 2015, DOI will:10.1109/SPW.2015.27
[8]. Wadda Afaf, Anas Abu Elkaram and Abdella Ait Warman. 2017. Towards a new privacy-preserving access control model based on blockchain technology in IoT. Further development of cooperation between Europe and MENA in information and communication technology.
[9]. Device democracy:Save the future of the Internet of Things. Retrieved May 10, 2017 from https://goo.gl/18Y16F
[10]. Barber, Simon, Xavier Boyen, Elaine 7Shi, and Ersin Uzun. 2012. Bitter to better—how to make bitcoin a better currency. In International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, (2012), 399-414.
[11]. Kanhele and Rajah Jurdak. 2017. Towards an IoT- optimized blockchain. Paper presented at the 2nd International Conference on IoT Design and Implementation. ACM, 2017
[12]. Ethereum Wiki: Problems. Retrieved May 17, 2017 from https://github.com/ethereum/wiki/wiki/Problems
[13]. Ethereum Wiki: Proof of Stake FAQ. Retrieved May 17, 2017 from https://github.com/ethereum/wiki/wiki/Proof-of-Stake- FAQ
[14]. IPFS – The Permanent Web. Retrieved May 18, 2017 from https://github.com/ipfs/ipfs
[15]. Kwon, Jae. 2014. Tendermint: Consensus without mining. Retrieved May 18, 2017 from http://tendermint. com/docs/tendermint {_} v04. pdf