Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks

Jollen Chen
Flowchain Open Source Project
Devify, Inc.
jollen@flowchain.io

ABSTRACT

This paper addresses the issue of *secure and trusted* Internet of Things (IoT) networks by adopting the emerging blockchain technologies. This paper proposes a new hybrid blockchain technology to address the trusted IoT issues such as trustless communications and decentralized applications. Besides, we also present that the pseudonymous authentication technique can use a puzzle-solving computation to enable trustless communications for the IoT and provide the capabilities of near real-time transactions. In our previous work, we presented a decentralized software framework for the IoT by using a p2p network and the concept of the blockchain. In this paper, we outline the core components of the hybrid blockchain and delve deeper the algorithms of the *hybrid consensus* to provide the capabilities for our hybrid blockchain technology.

Keywords

Internet of Things, Blockchain, Hybrid Consensus, Peer-to-Peer, Trustless Computing, Decentralized

1. INTRODUCTION

The Internet of Things (IoT) devices can generate and exchange security-critical data over the IoT network. Many IoT networks use the public-key infrastructure (PKI) to authenticate devices and ensure the data security as well as the data privacy. The IoT device has to sign the generated data by a digital public key, and deliver the data to the network for exchanging. However, such authentication method tends to be *expensive* for an IoT device regarding computing power and energy consumption.

Furthermore, the blockchain technology has the decentralized, secure, and private nature to become a promising idea that can be approaching the next-generation IoT architecture. Therefore, in our previous works, Flowchain and Devify have already been proposed to build a blockchain technology for the IoT device over a p2p network. Therefore, to achieve a secure and *inexpensive* blockchain for the IoT, this paper proposes *Flowchain Hybrid Blockchain* to enable *fast authentication* by eliminating the concept of traditional PKI methods. Furthermore, our work can address the technical challenge of achieving an efficient and secure IoT device to exchange the captured data by the blockchain technology.

The rest of the paper is organized as follow: In Section 2 we describe the main components of the hybrid blockchain design. In Section 3 we present the model including the architecture, algorithms and the hybrid blockchain design. The IoT blockchain economy is discussed in Section 4. Finally, Section 5 concludes the paper.

1.1 Previous Works

A. Devify

Devify has already proposed a generic and comprehensive software framework for building various types of trust IoT networks in a decentralized manner that can execute on a variety range of hardware devices, such as cloud servers, mobile devices, and resource-constrained devices.

B. Flowchain

Flowchain is the blockchain technology for the IoT developed on Devify. In a blockchain network, the consensus system can ensure the trusted transactions among all IoT nodes in a p2p network. The blockchain for the IoT technology comprises of a p2p network system, and a consensus system. The traditional public blockchains, such as Bitcoin [12] and Ethereum, use proof-of-work (PoW) consensus system; however, the PoW consensus system does not provide the ability of near real-time transactions. Therefore, in our previous work, Flowchain has also already proposed an IoT blockchain technology and a mining based proof-of-stake (PoS) miner to ensure the real-time transactions for IoT blockchain. Consequently, IoT devices vary, e.g., resource-constrained devices, mobile devices, and high-performance server frames that the computing power varies from devices. Flowchain uses the Devify software framework as the underlying p2p network system to implement such IoT blockchain technology. Thus it can execute on various IoT devices.

1.2 Type of Blockchains

The blockchains could be either a public blockchain or a private related to who is allowed to join the blockchain network [7].

A. Public Blockchain

Anyone can join the blockchain network, meaning that the blockchain network is entirely open to users for submitting transactions, accessing shared ledgers, and *mining*. More specifically, since the creation of Bitcoin in 2009, the public blockchain can enable a decentralized model that it can operate without any central authorizations; thus the public blockchain has the natures of *openness* and *trust*.

B. Private Blockchain

Unlike public blockchains, only authenticated users can join the private blockchain network. The user needs to request permissions from an *authority* in the private blockchain for joining the network. The authority validates the authenticity of a user, and grant permissions to authenticated users for submitting transactions and accessing shared ledgers.

C. Hybrid Blockchain

A hybrid blockchain comprises of public and private blockchains. The hybrid blockchain creates openness and trust of transactions in the public blockchain, and protect the privacy-sensitive data in the private blockchain. Such technique has already been proposed to secure blockchains and applied to digital rights management [15]. The use cases of the hybrid blockchain are as follows.

- In a hybrid blockchain, the private blockchain can determine which transactions are public, and submit these transactions to the public blockchain for open access.
- In a hybrid blockchain, the public blockchain can store transactions to secure data provenance.

Based on the application design and business logic, the blockchain architect can use the public blockchain, private blockchain, or a *hybrid* model by leveraging the benefits of both public and private blockchains.

1.3 Related Work

The standard methods of distributed computing desire stronger notions of security, where authentication may be provided by the PKI. Nevertheless, the study [8] describes that such methods are too strong for open and p2p networks; moreover, the study shows that a group of n nodes can generate a *pseudonymous PKI* by solving cryptographic puzzles at some bounded rate. As such, the nodes are validated by *pseudonymous authentication* rather than by true authentication. We show that such pseudonymous authentication method can be achieved by a hybrid blockchain model with secure and fast by encouraging public miners to generate cryptographic puzzles.

Accordingly, the study [2] showed a Byzantine agreement model without a PKI by solving computational puzzles at some bounded rate and assume authenticated channels between honest nodes. Moreover, our hybrid blockchain technology achieve pseudonymous authentication without such authenticated channels; thus, the hybrid blockchain can have *unbounded number of corruptions*. Also, the study [14] proposed a framework to efficiently and securely capture and validate provenance data; our hybrid blockchain technology can ensure such capabilities with the concept of hybrid blockchain technology.

2. CORE COMPONENTS

This section describes the main Hybrid Flowchain components as shown in Figure 1.

A. Private Blockchain

The private blockchain is where IoT devices can store their private data and ensure their data privacy. The IoT devices in the private blockchain can decide which data can be public by submitting the transactions of the data to the public blockchain.

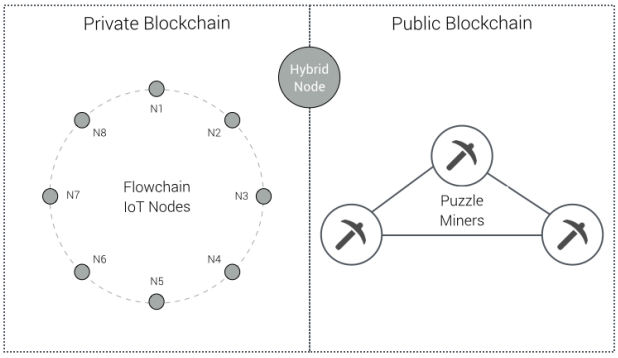

Figure 1: Core components of our hybrid blockchain design.

B. Public Blockchain

The public blockchain can verify transactions and record the verified transactions in the distributed ledgers across miners. The transactions in the public blockchain are public and opened to anyone, meaning that anyone can access the transactions in the public blockchain.

C. Flowchain IoT Nodes

The IoT nodes is an IoT device that executing the Flowchain [5] application previously proposed by this paper. The IoT nodes can be self-organized as a peer-to-peer (p2p) network by using the Chord algorithm [1] and Flowchain protocols.

D. Puzzle Miner

Puzzles Miner is a computer that aims to generate the *puzzles* and broadcasts the puzzles to the private blockchains. Section 4 describes the design and purpose of the puzzle miner.

E. Hybrid Node

Hybrid node is a device that receives the puzzles from the public blockchain and delivers the puzzles over the p2p network of the private blockchain.

3. OUR MODEL

3.1 Hybrid Blockchain Architecture

Public blockchains, such as Nakamoto blockchain, use the permissionless blockchain to build a trusted machine to read and submit transactions. Furthermore, private blockchains use the permissioned blockchain to build such trusted machine by granting access permissions only to authenticated participants. In a private blockchain, users need to be pre-authenticated before reading and submit transactions. However, the pre-authenticated is time-consuming to achieve near real-time transactions for today's IoT applications. Therefore, this paper proposes the hybrid blockchain architecture designed for the decentralized IoT application that can ensure a near real-time ability to read and submit transactions without such full authentication.

Accordingly, the most important features of the decentralized IoT is the consensus system. A consensus system can verify the transactions from a less trust state to a trusted state, as such, this paper will also propose a fast hybrid consensus system by combining a permissioned public blockchain

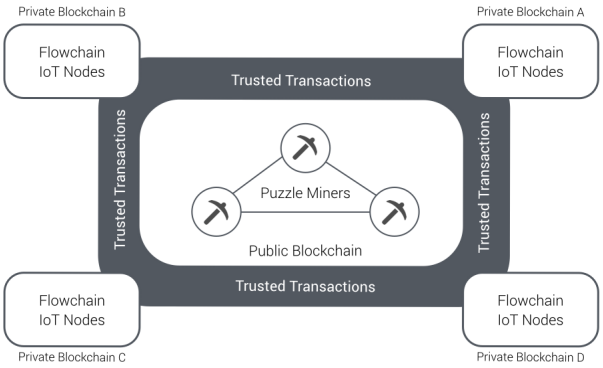

Figure 2: The hybrid blockchain network.

with a permissionless blockchain to verify transactions over the hybrid blockchain system. In hybrid blockchains, the public blockchain is accessible by any participants, and the private blockchain is only opened and accessible to authenticated users. The private blockchain is a permissioned network such as a wireless sensor network, and a Machine Learning network that can determine which transactions can be submitted to public blockchains. Figure 2 summarizes that the decentralized IoT application proposed by this work can provide the settings for today's IoT requirement.

- In the private blockchain, the users can submit sensory data, issue such data as digital assets, and submit to the hybrid consensus system
- The consensus system can determine which transactions are opened to public blockchains for public access.
- The consensus system can subsequently record such transactions in the public blockchains with openness, trust, provenance, and immutability.

More importantly, since the creation of Bitcoin in 2009, the decentralized model has been proposed to ensure an openness and trust network by verifying transactions without any central authorizations. Therefore, this paper introduces the hybrid blockchain model by using the public blockchains to provide such decentralized model.

3.2 Pseudonymous Authentication Method

The distributed computing uses the full authentication technique such as the PKI to control access to their networks. Also, most existing blockchains use such PKI technique to authenticate users, secure the communications and verify transactions by multi-party computation [6]. However, the study [8] has figured that such PKI technique is too strong to enable a fast communication. Specifically, the IoT blockchain need to authenticate nodes with fast; as such, this paper will propose the pseudonymous authentication technique to address such technical challenge. The pseudonymous authentication uses the technique of computational puzzles solving to replace the PKI to enable a fast authentication.

Moreover, such PKI technique is too strong that it involves confirming the identity of a user by validating the authenticity of a user with a digital certificate. Unlike a strong authentication technique, the user is anonymous in such pseudonymous authentication system, and the system validates the authenticity of the anonymous user by the consensus of the *solution*. The pseudonymous authentication uses a weaker but secures enough authenticity system. The

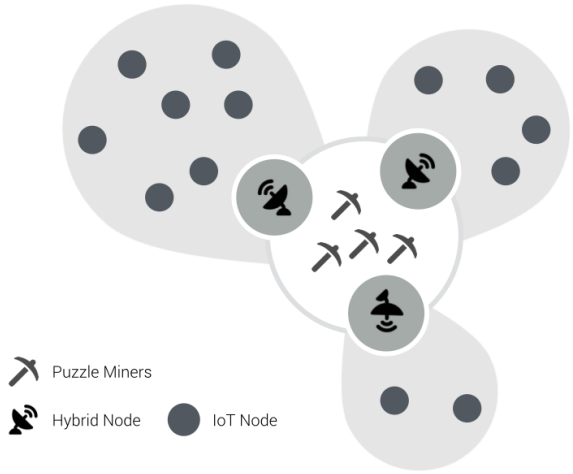

Figure 3: Puzzle mining and broadcast to private blockchains.

blockchains such as Bitcoin which don't use strong authentication systems have proven the notion of pseudonymous authentication to be a tremendous success. In summary, figure 3 shows that IoT nodes in the hybrid blockchain network are pseudonymously authenticated in the private permissioned blockchain to ensure near real-time transactions.

3.3 Puzzle Miner Algorithm

The users, represented as IoT nodes in this paper, can join the private blockchain and *submit transactions* to the public blockchain by solving a computational puzzle *mined* by the miners. The puzzles are computed by miners in the public blockchain, and broadcasting to the private blockchains. As previously described, the pseudonymous authentication needs to ensure a fast validation of the authenticity of an anonymous user. Therefore, this paper proposed that the hybrid blockchain use a lottery function to generate Konami Code that can be used to verify the solution.

Formally, let λ be *Konami Code*, a truly random magic string generated by the lottery function, and each puzzle is bound to this Konami Code. Let $\mathcal{F}puz$ be the puzzle solving function, and $\mathcal{U}i$ represents each user. Then, if the user does not submit the solution of the puzzle to the public blockchains within a fixed time interval, the public blockchain assumes that the user is *unauthenticated*. Also, the transactions submitted by the unauthenticated user are considered *untrusted* which can be discarded. Therefore, untrusted transactions will not be recorded in the public blockchain.

This paper assumes that the user can solve a puzzle within a fixed time interval σ, then the mining process of the miners is as follows.

1. $\mathcal{U}i$ starts receiving λ from the broadcasting
2. Let $\mathcal{P}uzzle$ be a function and $\S_j$ be a string; $\mathcal{U}i$ receives a puzzle $(\mathcal{P}uzzle, x_j)$ from a peer $\mathcal{U}j$ in the private blockchain over the p2p network
3. Let $\mathcal{P}uzzle(\lambda)$ gives an arbitrary-length vector $\vec{x}$ of the Konami Code, then $\vec{x} = (x_1, \ldots, x_n), n < j$
4. Let $\mathcal{F}puz$ maintain a set $\mathcal{T}$ of puzzle solutions, then $\mathcal{F}puz$ computes each entries in $\vec{x}$, let $y_i = \mathcal{F}puz(x_i), i = (1, \ldots, j)$
5. The miners say that $\mathcal{U}i$ solves the puzzle $(\mathcal{P}uzzle, x_j)$ if

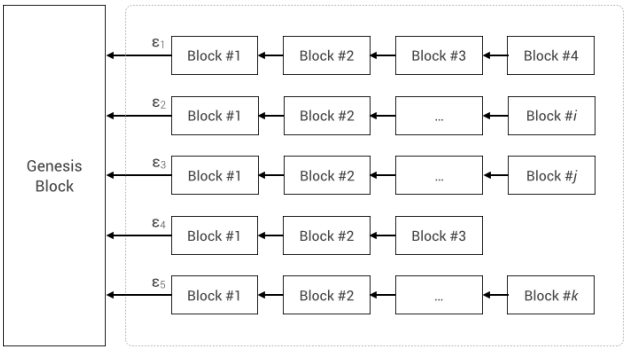

Figure 4: The virtual blocks and local blockchain.

$\mathcal{F}puz$ successfully finds $y_i = x_j$ within the time interval σ

6. $\mathcal{F}puz$ returns $\S_j$ to $\mathcal{U}j$ and stores $\mathcal{H} = (\vec{x}, y_i, \lambda)$ in $\mathcal{T}$
7. The miners and $\mathcal{U}j$ confirm the user $\mathcal{U}i$ is *authenticated*

Also, the user $\mathcal{U}i$ can thus use $\mathcal{H}$ to sign transactions and submit the transactions to the public blockchains for verifying; the submit process be as follows.

1. The trusted user $\mathcal{U}i$ produces a message or receives a message from another user through the p2p network; formally, let $\mathcal{M}$ be this message
2. The trusted user $\mathcal{U}i$ has the keypair (sk_i, pi_i); let $\mathcal{S}ign$ be the signature function
3. Let $\mathcal{T}i$ be the new transaction and $\mathcal{H}ash$ be a hash function so that $\mathcal{T}i = \mathcal{H}ash(\mathcal{S}ign(M), H, pk_i)$;
4. $\mathcal{U}i$ submits $\mathcal{T}i$ to the public blockchain

Accordingly, regarding the implementation selection, the hash function $\mathcal{H}ash$ can be SHA-256, SHA-512, etc.

3.4 The Hybrid Consensus

The public blockchain network can record transactions in the distributed ledgers, the blockchains across all miners after some miners successfully *agree on* the transactions; the process is called proof-of-work consensus. The transactions recorded in the public blockchain are trusted transactions and *immutable.* Moreover, the miners should ensure that the transactions were submitted from an authenticated nodes. As such, the hybrid blockchain has a *hybrid consensus* that can achieve such *multi-party trust.* The hybrid blockchain provides these settings to support the consensus system for multi-party trust:

- In the public blockchain, the miners can verify transactions from a pseudonymously authenticated node.
- The public blockchain network can agree on the transactions by proof-of-work consensus.

Also, the hybrid blockchain can provide the ability to exchange messages between different private blockchains via the public blockchain.

3.5 The Local Blockchain

As previously described, Flowhain can build a private blockchain that the IoT devices can self-organize as a p2p network. Every *Flowchain IoT Node* in the private blockchain has a *local blockchain* that keeps the privacy-sensitive data. Figure 4 depicts the concept of virtual blocks and the local blockchain. The local blockchain starts from the genesis block and is chained by *virtual blocks* mined by a *local miner* executing on the IoT node. Section 3.6 describes the algorithm of a local miner.

Flowchain comprised a mining-based proof-of-stake model for IoT devices that the *block time*, the time to find a valid block, is predictable and can be timed in a fixed number calculation per second. Furthermore, Kraft and Daniel [10] studied the predictable block times for various hash-rate scenarios as the Poisson process with time-dependent intensity. Therefore, we model the prediction of block times as a Poisson probability density function to ensure a cost-effective difficulty control system. Figure 5(a) depicts the concept of this mining process.

1. The block time is determined by P, the Poisson distribution function
2. The value of P is resulted by *stakes* such as the battery level and WiFi signal strength
3. At the time t_1, P predicts that if the termination time of the current block is exactly *early* than the end of t_1, than *block #1* is successfully mined
4. The local miner continues the step 2 and 3 to mine more virtual blocks

In figure 5(a), the local miner predicts that *block #2* can be found at t_2, and *block #4* can be found at t_9. The block time of *block #4* is *longer* than expected because that the WiFi signal is weak at time t_4 to t_8.

Furthermore, the Byzantine agreement is a consensus algorithm to avoid distort data [11] across p2p nodes. The Byzantine agreement can be found in many database systems to ensure data replication and redundant. Technically, the Byzantine agreement is a distributed decision-making process that some amount of nodes are agreed on transactions and can replicate the data; such a mechanism is also known as *fault-tolerance.*, and Byzantine agreement is known as Byzantine Fault-Tolerant (BFT). Therefore, the private blockchain can also agree on the *private transactions* by fault-tolerance, meaning that the p2p network in the private blockchain can replicate a certain of private transactions.

In general, if a maximum number of n node can distort data, a BFT algorithm can be achieved with a total of $3n+1$ nodes to tolerate the network. However, if nodes can not distort application data submitted through them, then an amount of $2n+1$ nodes is capable of tolerance the network. There are various BFT implementations such as Practical Byzantine Fault-Tolerant (PBFT) [3], and Speculative Byzantine Fault Tolerant (Zyzzyva) [9] can be employed in the private blockchains of our hybrid model. The implementation is a selection according to the difference in their business logic.

3.6 The Local Mining

The previous work of this paper [5] proposed that the IoT nodes can use the *virtual blocks* concept to store local transactions. IoT nodes can temporarily store their transactions in the virtual blocks and submit the stored transactions to the private blockchain network for replicating. This setting, called *gathering transactions*, can provide additional abilities to hybrid blockchains as follows.

- The IoT nodes can submit real-time sensitive transactions immediately to the public blockchain and save the transactions in the virtual blocks

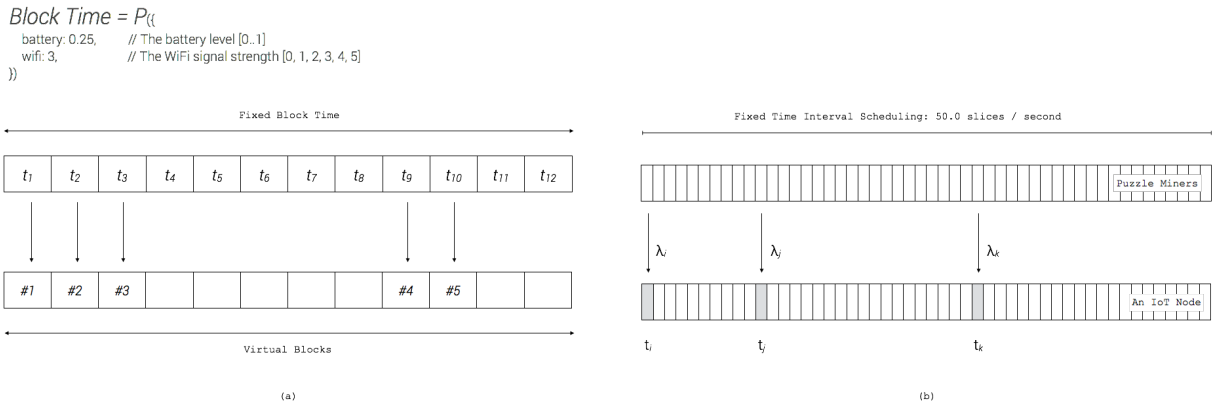

Figure 5: (a) Local mining, and (b) the pseudonymous authentication.

- The IoT nodes can gather and store none real-time sensitive transactions in virtual blocks as well
- The IoT nodes can submit their virtual blocks to the private blockchain for data replication

As described previously, we present a *local miner* by which virtual blocks are mined. Moreover, the genesis block is pre-defined by the private blockchain developers. As figure 4 previously figured that the genesis block, formally denoted as $\mathcal{G}$, which is pre-defined by private blockchain developers, and there are give entities $\mathcal{E}1$, $\mathcal{E}2$, $\mathcal{E}4$, $\mathcal{E}4$, and $\mathcal{E}5$ in a private blockchain. As such, figure 5(a) depicts the process of local mining, and the following example shows $\mathcal{E}1$.

1. The public blockchain has σ slices per second, meaning that the puzzle miner uses a fixed time interval mining mechanism
2. The puzzle miners in the public blockchain are broadcasting λ_1 at time t_1
3. The Flowchain node $\mathcal{E}1$ has a sensory data, formally denoted $\mathcal{M}$, and $\mathcal{E}1$ generates a transaction $\mathcal{T}1 = \mathcal{H}ash(\mathcal{S}ign(M), H, pk_i)$
4. The Flowchain node $\mathcal{E}1$ successfully mines *Block #1* after $\mathcal{F}puz$ solving the puzzle bound with λ_1, and stores $\mathcal{T}1$ in virtual block *Block #1* of $\mathcal{E}1$
5. $\mathcal{E}1$ repeats steps 2, 3, and 4, until the end of σ slices and resulting in a total number of 5 transactions, $[\mathcal{T}1, \ldots, \mathcal{T}5]$, which were stored in virtual block *Block #1*
6. $\mathcal{E}1$, subsequently continues to get λ_2 at t_1, as well as resulting in 10 transactions, $[\mathcal{T}6, \ldots, \mathcal{T}15]$, which were stored in virtual block *Block #2*
7. At the time t_3, the IoT node $\mathcal{E}1$ submits $[\mathcal{T}1, \ldots, \mathcal{T}15]$ in the virtual blocks, *Block #1* and *Block 2*, to the private blockchain network
8. All authenticated nodes in the private blockchain can join the consensus activity to agree on $[\mathcal{T}1, 1 \ldots, \mathcal{T}15]$, that all the transactions will become *trusted*
9. The BFT consensus can ensure that trusted transactions $[\mathcal{T}1, 1 \ldots, \mathcal{T}15]$ were replicated in the private blockchain, meaning that the private blockchain is capable of *fault-tolerance of private trusted transactions.*

Figure 5(b) shows such local mining technique that the Flowchain node was pseudonymously authenticated to submit transactions at (t_i, t_j, t_k). Furthermore, the above process also gives the *deferred submission* concept. The Flowchain node can *gather* transactions in its virtual blocks and submit *gathered* transactions to the public blockchain in a future time.

Table 1: The attributes of the perfect blockchain

Perfect Blockchain	**Our Model**
Predictable block times:	We use the probability density function to predict block times.
Stability of block times:	We use a periodical mining system to ensure the stability of block times.
An alternative difficulty control:	We use a PoS miner to control the mining difficulty.
Secure and trusted transactions:	We use the hybrid blockchain model together with the pseudoymous authentication technique to ensure secure and trusted transactions.

The blockchain model provides additional advantages for the IoT; thus, this paper selects the blockchain technology to provide a decentralized and secure IoT network. Table 1 summarizes the results of our work to highlight attributes of a promising IoT blockchain.

4. THE IOT BLOCKCHAIN ECONOMY

Describing the benefits of a new blockchain technology in the economy is fundamental. Thus, in addition to the blockchain technology, this work also describes the blockchain economy: how blockchain technology can benefit the IoT technology as well as why the blockchain technology is necessary for the next-generation IoT innovation. More specially, this section also describes how to adapt our hybrid blockchain model to gain such benefits.

4.1 Tokenized Hardware

There are various types of tokens currently existing in the cryptocurrency economic, such as utility token, security token, and coins. The SEC recently announced to consider Initial Coin Offering (ICO) as securities which could be a good thing since the ICOs as securities is a new viable way to raise funds, called tokenized securities. In this paper, we propose the tokenized hardware, another new viable way to hardware manufacturing and production for open hardware economic. Tokenized hardware can ensure the assets of

the hardware rights, data privacy, and data security by hardware tokens. Therefore, this paper also proposes the concept of *tokenized hardware* that the hardware ecosystem comprised of manufacturers, developers, and consumers can collaborate on mining to mine a fixed amount of *hardware tokens*. We consider that the tokenized hardware technology will represent a revolutionary innovation to build more trust and secure hardware.

Furthermore, in recent years, the *crypto* has become an emerging technology for creating more secure and decentralized systems. Ethereum platform, an Ethash-based blockchain system, uses such technology to issue *tokens*, which can be utilized as *cryptocurrency* that can be traded in any central exchange. Accordingly, startups can also raise funds by selling virtual shares in the form of security tokens, called tokenized security. Moreover, the underlying infrastructure of IoT blockchain technologies is consolidated by the orchestration of hardware and software components that can support the implementation of cryptographic technologies. As such, figure 6 presents that the proposed software architecture of our previous work can implement the *tokenized hardware* firmware.

4.2 The benefits of IoT Blockchain

It is the token fundamentals to define the benefits the customers gain from holding tokens, thus, linking viable benefits with token usage models is a critical issue in our research. The benefits customers gain from utility tokens are as the following examples.

1. Access the basic cloud service
2. After-sales service
3. Purchase discount

The amount of total supply of utility tokens equals to the total quantity of each shipment, and utility tokens must record their *benefits* provided on public blockchains, such as Ethereum and Hyperledger. In short, utility tokens can grant permissions to authorized hardware for accessing cloud service, request for the after-sales service, and other available benefits provided by hardware manufacturers. Also, unlike public blockchains, private blockchains are permissioned blockchains that are controlled by their operators, and only grant permissions to authorized users [7]; thus, each shipment of the hardware can be employed as a *private blockchain* by which utility tokens are mined.

Internet of Things (IoT) is a connected device enables the sensory data transfers to the Internet, and applications can participate the IoT device to access these sensory data. For participating the IoT device, the participants have to pay the device for data access. Unlike utility tokens, the payment is in cryptocurrencies, such as Bitcoin and ERC20 currencies, which uses encryption techniques to regulate the generation units of the cryptocurrency and verify the transaction of funds.

Moreover, unlike fiat currencies, cryptocurrencies are usually operating independently without a central bank and can be minted on public blockchains, such as Ethereum. In conclusion, the payment of funds is achieved with cryptocurrencies in a peer-to-peer (P2P) manner, called client-to-client (C2C) model.

The WiFi camera is a use case among tokenized hardware products. The WiFi camera is a tangible asset while the video streams produced by the camera are digital assets

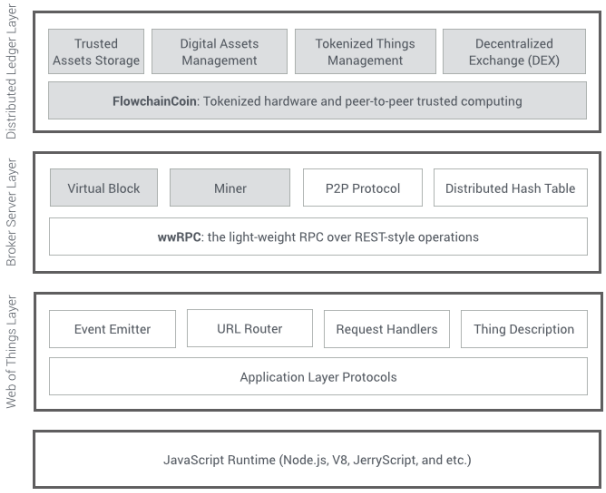

Figure 6: The software on a Flowchain IoT node.

[16], in short, the tokenized camera is an asset comprised of the hardware asset and the digital assets, and the token holder has the rights to use these assets. Subsequently, the blockchain can issue access tokens to users who want to access the digital data from the camera. As such, there is a use scenario of such tokenized camera hardware.

1. John has an app on his mobile phone
2. An app pays some units to the WiFi camera
3. The blockchain issues an access token to mobile apps after verifying the transactions
4. The app starts with received video streams, the digital assets of the tokenized hardware
5. John can watch the video from the camera

Such use scenario is a use case of tokenized hardware proposed by this paper; nevertheless, we define connected tokenized hardware as *Tokenized Things* compare to the traditional Internet of Things (IoT). Also, technically, a tokenized thing has to be represented as *Virtual Things* with the ontology of Web of Things (WoT) [13] and operates in a p2p manner. Therefore, this paper has also developed the *Devify* software framework [4], a generic and comprehensive software framework based on Flowchain for building p2p IoT networks.

4.3. Incentive

One of the most visible impacts is that the hybrid blockchains have to provide an incentive design. A favorable incentive design can help to build a sustainable blockchain network and keep the network healthy, meaning that the incentive can encourage participants to support the blockchain network by participating in the activities of the public blockchains, such as puzzles mining as previously described.

In our hybrid blockchain model, the public blockchain can fund incentive either by puzzles mining, proof the *existence* of specific application data or run smart contracts.

Puzzles Mining

Participants have to join the public blockchain network and spend their *time* to generate and broadcast puzzles.

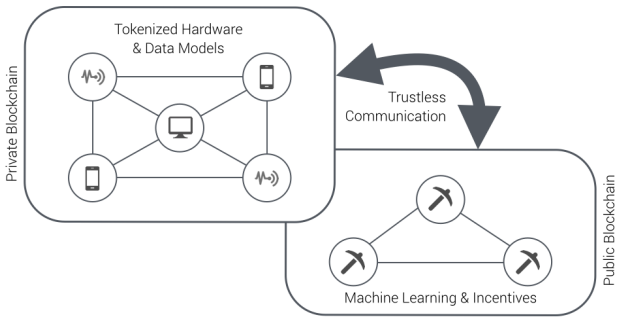

Figure 7: The hybrid blockchain architecture for the IoT and AI. The IoT devices can be tokenized to ensure their trust and submit datasets to the public blockchain for data analysis.

Proof of Existence

A transaction *exists* if it has been verified and recorded in the public blockchain. The miners can assist smart contracts for validating the existence of a transaction, call *proof of existence.* More importantly, the proof of existence can ensure the data *trust* and *provenance.*

Hosting Smart Contracts

The smart contract is one type of the decentralized applications (Dapps), and in our hybrid blockchain model, the developers can build a private blockchain, develop smart contracts for their private blockchain, and *deploy* smart contracts to the public blockchain for invocation.

5. CONCLUSION

To conclude the contribution of our work, we illustrate the machine learning network as an example. Hybrid Flowchain comprises of private permissioned and public permissionless blockchains that can enable the machine learning on IoT Blockchain with the allowance of multiple organizations to perform collaborative data analytics and machine learning while guaranteeing the data privacy of their datasets. The *consortium* blockchain is a type of hybrid blockchain that it allows multiple organizations to exchange trusted transactions through the public blockchain. The organization has their private blockchain, and the hybrid consensus can ensure the multi-party trust as previously described in section 3.4. Figure 7 depicts the hybrid blockchain architecture that can enable such machine learning network on the Hybrid Flowchain. The paper has already built Hybrid Flowchain for proof-of-concept accessible at https://github.com/flowchain.

REFERENCES

[1] Chord (peer-to-peer). https://en.wikipedia.org/wiki/Chord_(peer-to-peer).

[2] J. Aspnes, C. Jackson, and A. Krishnamurthy. Exposing computationally-challenged Byzantine impostors. Technical Report YALEU/DCS/TR-1332, Yale University Department of Computer Science, July 2005.

[3] M. Castro and B. Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.

[4] J. Chen. Devify: Decentralized internet of things software framework for a peer-to-peer and interoperable iot device. *Proceedings of the Workshop on Advances in IoT Architecture and Systems (AIoTAS2017)*, 2017.

[5] J. Chen. Flowchain: A distributed ledger designed for peer-to-peer iot networks and real-time data transactions. *Proceedings of the 2nd International Workshop on Linked Data and Distributed Ledgers (LDDL2)*, 2017.

[6] S. Goldwasser and Y. Lindell. Secure multi-party computation without agreement. *Journal of Cryptology*, 18(3):247–287, 2005.

[7] P. Jayachandran. The difference between public and private blockchain. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.

[8] J. Katz, A. Miller, and E. Shi. Pseudonymous broadcast and secure computation from cryptographic puzzles. 2015.

[9] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong. Zyzzyva: Speculative byzantine fault tolerance. *SIGOPS Oper. Syst. Rev.*, 41(6):45–58, Oct. 2007.

[10] D. Kraft. Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, 9(2):397–413, 2015.

[11] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/en/bitcoin-paper.

[13] D. Raggett. An introduction to the web of things framework. https://www.w3.org/2015/05/wot-framework.pdf.

[14] A. Ramachandran and M. Kantarcioglu, Dr. Using Blockchain and smart contracts for secure data provenance management. *ArXiv e-prints*, Sept. 2017.

[15] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami. Blockchain contract: Securing a blockchain applied to smart contracts. *2016 IEEE International Conference on Consumer Electronics (ICCE)*, 2016.

[16] Wikipedia. Asset. https://en.wikipedia.org/wiki/Asset.