IOTW - A Transaction Ledger Using Proof of Assignment (PoA) With Improved Security

Motivations

Blockchain is arguably one of the most disruptive technology in decades. Using distributed ledger architecture, blockchain technology is poised to transform our society in many ways; revolutionizing multiple industries including the financial system, supply chain and even our legal system. Yet, the blockchain technology has hit a virtual roadblock in the Internet-of-Things (IoT) arena, markedly limiting its applications in the ubiquitous smart appliances and electronic devices.

The most popular blockchain consensus algorithms used today are Proof of Work (PoW) [NAKA08] and Proof of Stake (PoS)[KING12]. Unfortunately, both PoW and PoS are inadequate for IoT applications because most IoT devices have very limited computing power, memory resources, and power budget.

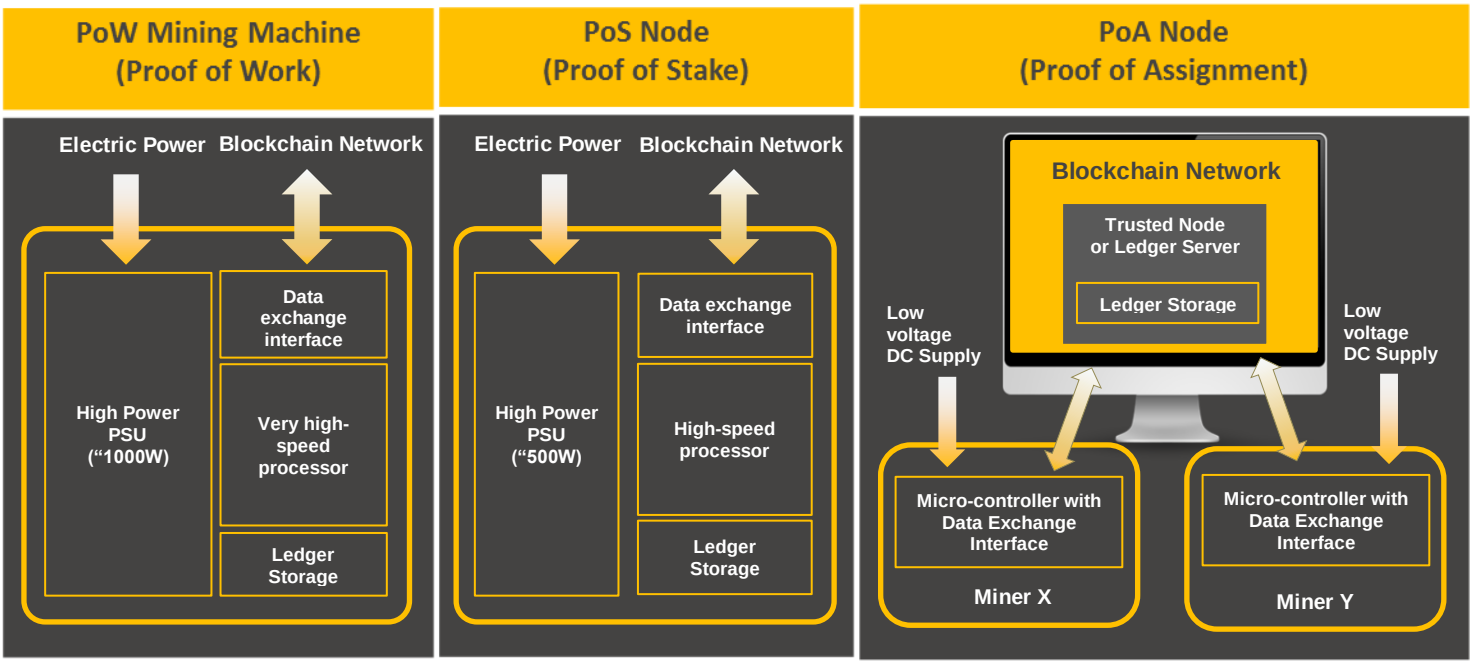
The PoW algorithm is used by many existing blockchains, including Bitcoin, in which miners compete to become the first provider of a cryptographical problem. The complexity of the cryptographical problem increases with the growth of the ledger size and in some use cases is already demanding power on similar levels as consumed by a supercomputer. It is not an environmentally friendly algorithm and consumes a lot of energy. Although PoW is useful for some applications, it is definitely not a suitable option for IoT applications.

In the PoS consensus process, a candidate is regularly elected among validators in the blockchain ecosystem. The PoS algorithm requires less power than the PoW algorithm because of the above election process. Nevertheless, it is still not a good choice for IoT applications, as each individual node requires substantial computing power and memory resources.

To this end, we have invented a very robust, secure and, scalable new **Proof-of-Assignment (PoA)** consensus algorithm which requires much less energy, making it suitable for IoT applications. PoA is designed to gracefully solve these IoT specific issues.

Concept of Micro Mining

In PoA, each IoT device is required to perform simple but very important cryptographic tasks, known as “Micro Mining.” Moreover, these IoT devices are not required to handle the transaction ledger, which is maintained by a Distributed Trust Node System.



While PoS alleviates some of the energy concerns, ledger servers involved in such a blockchain still need to have substantial memory capacity to accommodate the transaction ledger. This increases the cost, making it very costly for small IoT devices to become blockchain enabled. IOTW aims to remove such hurdles and enable the general adoption of blockchain by products used in our daily lives, fueling the growth of blockchain transactions.

Similar to PoS, mining devices of the IOTW blockchain require very little computational power in comparison to PoW. In addition, IOTW, using the PoA consensus algorithm, eliminating the need for mining devices to store the transaction ledger. This removes the

cost associated with large memory and therefore adds mining capability to simple and affordable IoT devices.

Instead of allowing every network node to participate in mining (as in PoW), or having a voting process to elect the appointed validator for a transaction (as in PoS), PoA elects a single candidate or a limited number of candidates to solve the cryptographical problem using a pre-agreed criteria (availability at the request for MicroMining and as well as historical data of Mining assignments) issues the task directly to the elected candidate(s). Therefore, no or limited competition exists in solving the cryptographical problem. Furthermore, the storage of the ledger is not a mandatory requirement for mining devices. Transaction ledgers are being stored in higher networks layer(s) such as trusted nodes or ledger servers. PoA reduces the requirements on computational power and memory capacity of the mining devices to a basic level. An average microcontroller, controlling the functionality of devices like electric fans, rice cookers, vacuum cleaners, air conditioners, printers, etc., can become a mining device on the IOTW blockchain, given that it has network access and sufficient program memory to incorporate the mining software. Thus, the term Micro Mining is adopted for the mining process in IOTW to distinguish it from other conventional forms of mining.

Since the cost of adding Micro Mining to any IoT enabled product is extremely low or near to zero and the incentive for products with Micro Mining capability can be realized during the operating life of the products, the adoption rate for IOTW is anticipated to be much more rapid than public blockchains today. This will bring the cost of blockchain technologies down and spawn off various applications.

The initial launch of IOTW blockchain network aims at creating a marketplace linking household appliance manufacturers, agents, services providers, and end users, which will be accessible via mobile phones, pads, and computers. The product manufacturers, agents, distributors and service providers will be strategic partners for IOTW blockchain and it is the aim of the IOTW blockchain to grow together with its strategic partners. For more details, please refer to the IOTW White Paper.

System Architecture

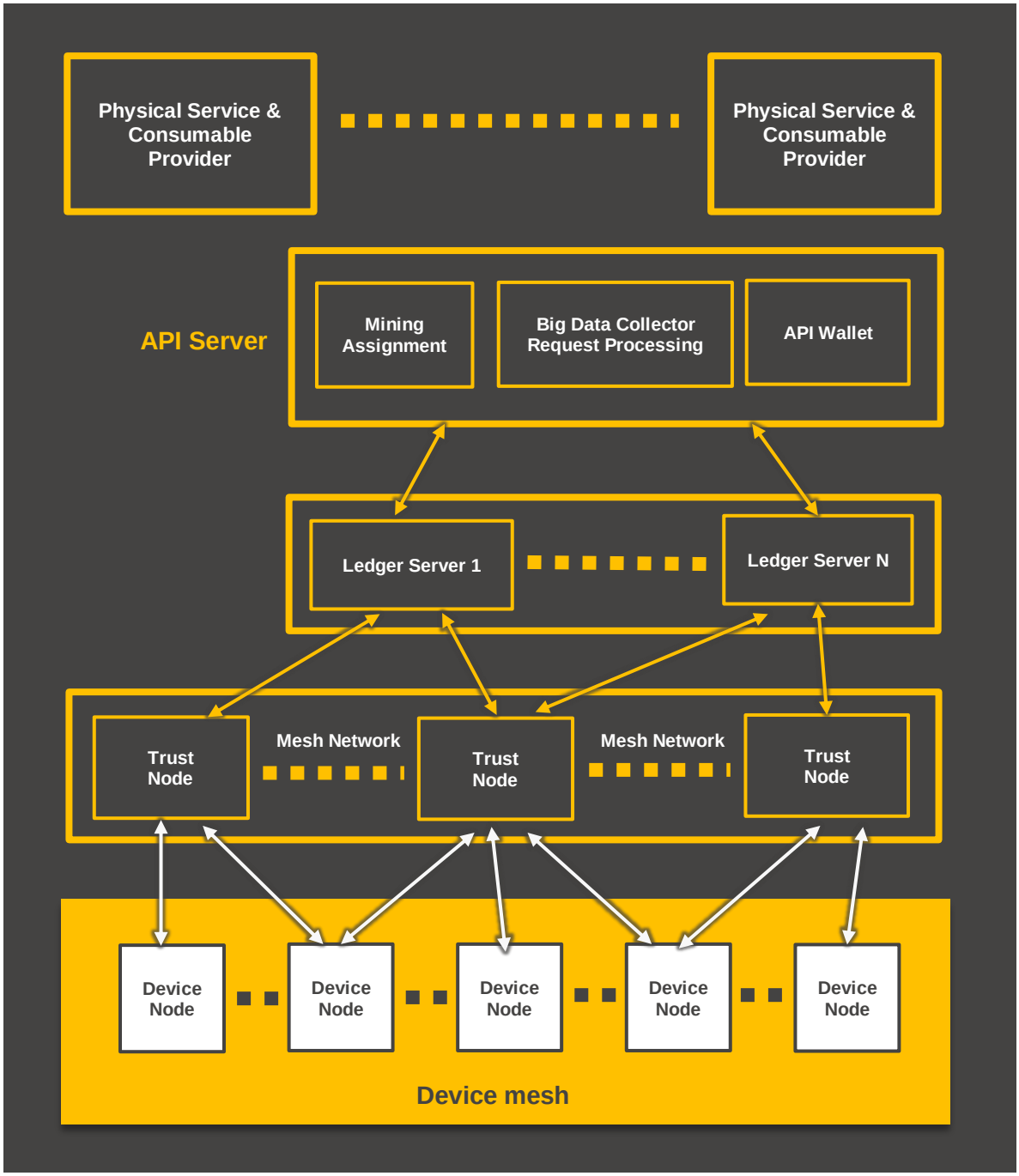
Today's public blockchains simply have a flat layer of ledger server mesh network under the API server.

The IOTW blockchain will have more network layer(s) below the ledger server mesh network. Mining devices will be linked to any one of trusted nodes of IOTW blockchain directly, or via another layer of trusted node mesh network. Mesh networks between mining devices and trusted nodes may also exist. Hence, the network architecture may vary from one to multiple layers of mesh networks.

It should also be noted that due to the simplicity of mining devices, Man Machine Interface (MMI) for transaction processing and direct association with wallet are generally not being built within mining devices. Instead, they are normally linked to user devices such as cell phones, tablets, or computers for communicating with the IOTW blockchain ecosystem.

Similar to existing public blockchains, there is an API server on top of the ledger server mesh network to link different categories of users together, as well as to wallets and exchanges. A big data bank can be built into the API servers collecting data, and carrying out analysis to generate useful information such as consumer behavior, best-selling products, product reliability and life, service response time, etc. Such information has the potential to become a source of income for the IOTW blockchain and a value add for the markets and community.

The following diagram illustrates a possible system architecture. It should be noted that the mining assignment block shown is within the API server. It is also possible that the mining assignment is within the ledger server mesh network controller.



PoW based consensus blockchain networks are normally more vulnerable to 51% takeover attacks, when the number of ledger server nodes is small. As number of ledger servers grow, blockchains become more and more robust against such attacks. Therefore, special care should be taken during initial launch of new blockchains. For IOTW, the whole system is controlled by AnApp Blockchain Technologies Limited in collaboration with strategic partners, serving also as owners of trusted nodes, or even trusted ledger servers. This means that the IOTW blockchain ecosystem will not be an open system at the beginning as a tradeoff for better system security.

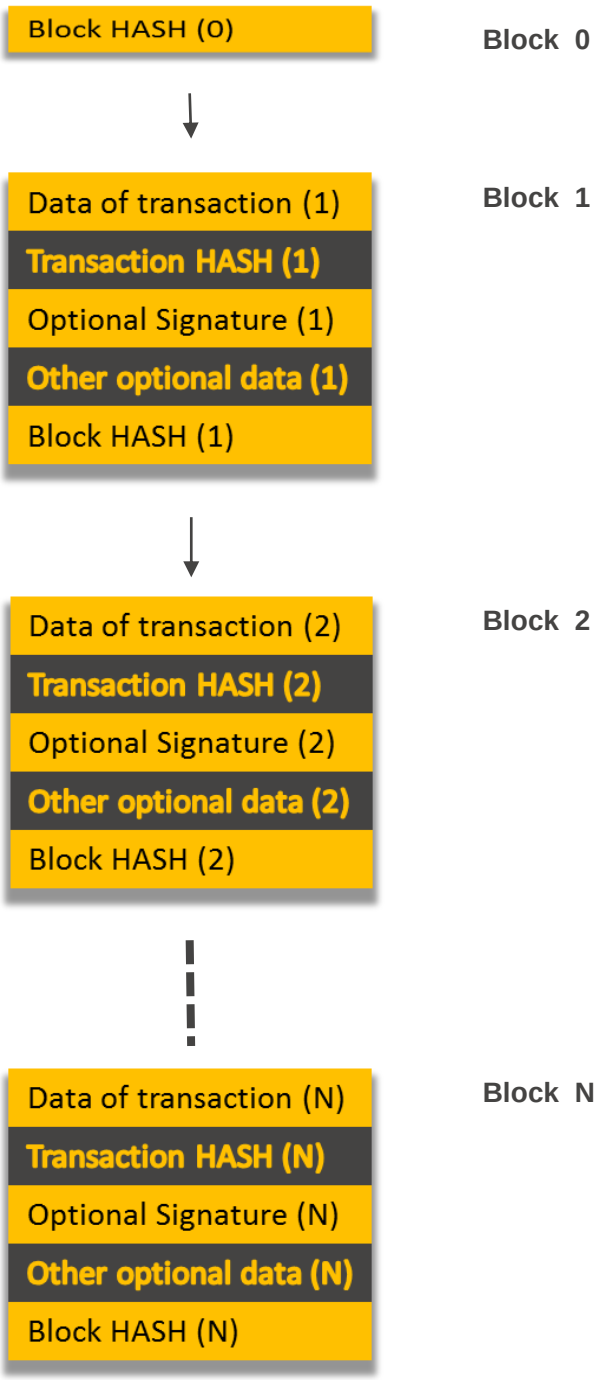
Transaction Execution

Transaction request can be raised by any devices in the IOTW blockchain ecosystem having a valid wallet for paying or receiving IOTW coins. A transaction request comprises of the transaction information in terms of the nature of transaction such as purchase or sale of goods and services, involved parties, delivery schedule, warranty terms, transaction amount involved, etc., together with a transaction HASH, and other optional data such as digital signature and time stamp.

Upon receiving new transaction request, the IOTW blockchain ecosystem assigns the job of computing the new block HASH to one or more mining devices. New Block HASH generated by mining device(s) is then validated by trusted node(s) or ledger server(s).

Once the transaction request is verified and validated, the newly generated block HASH will be appended to the transaction request to form a block included into blockchain. The new transaction is then appended to the last transaction block and the transaction amount involved will then be transferred between corresponding wallets.

The following diagram illustrates a typical ledger with N transaction blocks



Scalability and Sustainability

From the adoption point of view, blockchain offers very rapid transaction processing speed, such that tens or even hundreds of transactions can be entertained per second. This is a well-known scalability problem that every blockchain is attempting to tackle. Sharding is one of the most discussed method to drastically improve the capability in terms of transactions per second. We are investigation sharding, as well as other potential innovative solutions to improve scalability.

Starting from the formulation of the operating model of IOTW blockchain, recurrent income from transaction fees and service fees for big data is anticipated. Since IOTW aims at building up a mass network of IoT devices in hundreds of millions worldwide, income generated will become substantial once the blockchain ecosystem becomes well established. It is the target of the IOTW blockchain to become a sustainable ecosystem in the long run such that the transaction and service fees received can cover reward systems, systems management, maintenance and upgrade, as well as further development.

Security

Since transaction ledger is not being stored in micro-mining machines (IoT devices), the 51% hostile take over does not apply to this network layer. In the IOTW blockchain ecosystem, the key to security is to protect the ledger from attacks at the trusted server network layer. Theoretically, trusted servers are already more robust against attacks. In addition, we are developing another algorithm to improve the security of the IOTW blockchain ecosystem.

Instead of the validating a new transaction just through a verification from IoT micro-mining and validation by trusted nodes, at least one witness who is not the mining node will be invited to witness the new transaction using digital signature (private/public key pair). With such implementation, 51% attack needs to simultaneously attack both the transaction ledger as well as the associated blockchain of witnesses to gain hostile takeover. Hence, vastly improving the security of the IOTW blockchain ecosystem.

IOTW Blockchain Network Management

The initial assignment of IoT devices to the Ledger Server will be managed by AnApp Blockchain Technologies Limited in collaboration with strategic partners such as semiconductors and IoT devices vendors. When the ecosystem grows, a management standard steering committee will be formed by interested individuals and companies to oversee the overall IoT ledger sever assignment and general network management including its future development direction. Members of this committee will come from different backgrounds and represent multiple stakeholders who participate in IoT devices manufacturing and selling. AnApp founding members have established USB OHCI, 1394.A and participated in PCI SIG, wireless LAN standard development. AnApp has the skills and the necessary connections in the industry and community to kick start such committee.

Patents will be licensed out for free when the development and sales is for IOTW network ecosystems with some exception such as building mining farms. The steering committee and AnApp will have the right to take legal action against such violations or shut down such operations. The target is to put IOTW coin into the average person's hand through decentralised mining.

We will select appropriate security models to benchmark the figure of merit for the IOTW blockchain ecosystem before the public launch.

Existing Status & Future Works

We have been successfully running IOTW blockchain on 1,000+ IOT devices at the same time with a single Trust Node.

At this moment, a very preliminary demo of IOTW blockchain with two hundred mining nodes within a small room is implemented successfully. Transactions are being generated using either cell phone handsets or computers. The blockchain ledger can be viewed on a computer screen (for demo only and not the future working version). The demo will be upgraded shortly to 1000 mining nodes either in a small room or within small rooms at different sites. Most households do not have 200 IOT devices.

The software is fully scalable.Furthermore, the current implementation is to target for instant transaction and the ultimate target performance would be 1M transactions per second.

The green paper will be updated with details of instant transaction implementation once instant transaction patent is filed. For development tasks and target milestones, please refer to the IOTW White Paper.

Future development will focus on the following:

a) Implementation of a real IOTW blockchain ecosystem with user friendly Man Machine Interface (MMI)

b) Scale up the system capacity to accommodate practically unlimited number of users (as discussed previously)

c) Implementation of further security features to make the ecosystem more robust against the 51% attack (further discussion in following paragraph)

d) Development of data analysis of big data and launch of related services

Instead of the normal validation in PoW or PoS, IOTW implements another level of security by inviting one or more users to serve as witness(es) to co-sign transactions. Signature(s) of witness(es) is/are generated by private key and validation of such signature(s) are done using address of validating device which is encoded from elliptic curve public key encoded with hashing algorithm. This will greatly increase the difficulty for the 51% take over attack due to the need for tackling the witnesses blockchain within the limited time of transaction processing, simultaneously.

References

[BUTE13] Vitalik Buterin. Ethereum: A Next-Generation Generalized Smart Contract and Decentralized Application Platform, 2013.

[DWOR92] Cynthia Dwork and Moni Naor. Pricing via Processing or Combatting Junk Mail, 1992.

[JAKO99] Markus Jakobsson. Proofs of Work and Bread Pudding Protocols, 1999.

[KING12] Sunny King and Scott Nidal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012.

[LOMP82] Leslie Lamport, Robert Shostak and Marshall Pease. The Byzantine Generals Problem, 1982.

[NAKA08] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[WOOD18] Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger Byzantium Version, 2018.

[ZHAN15] Yu Zhang. An IoT Electric Business Model based on the Protocol of Bitcoin, 2015.

Important

The reader of this document should read this Warning page carefully and confirm that he/she would not be in violation of any laws before proceeding to the next page.
This document may relates to the promotion and offering of cryptocurrency and is intended for circulation in the Hong Kong Special Administrative Region of the People's Republic of China or such other jurisdiction that permits the promotion, offer and sale of cryptocurrency only.
In particular, this document is not for release, publication, distribution, directly or indirectly, in or into the United States, Canada, the People's Republic of China (excluding Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan) or any other jurisdiction where the offering of and/or the sale and purchase of cryptocurrency is prohibited. This document does not constitute and is not an offer to sell or a solicitation of any offer to buy digital token in places where the offering of and/or the sale and purchase of digital token is prohibited. The cryptocurrency referred to in this document have not been and will not be registered under the U.S. Securities Act of 1933, as amended or any state securities laws of the United States.
The responsibility to ensure compliance with the applicable laws lies with the reader of this document should he/she proceed to the next page. AnApp Blockchain Technologies Limited takes no responsibility and make no representation whatsoever in this respect. If you are in any doubt as to the content of this document, you should contact your professional adviser.