# IOTW

## ANAPP BLOCKCHAIN TECHNOLOGIES LIMITED

A Scalable Blockchain – Proof of Assignment Protocol

# IOTW

Highly secure IoT ecosystem,
enabling Instant transaction and green micro mining
from any connected device - no extra hardware,
no additional cost.

## Whitepaper

By: Fred Leung, Tony Chan, Kartik Mehrotra, and Peter Chan
2018

## Mission

To Develop an IoT Blockchain protocol using proof of assignment to integrate IoT devices with Blockchain such that a decentralized network of IoT applications and data exchange can be established.

## The Problem

Current consensus systems such as Proof of Work or Proof of Stake have drawbacks that make them difficult for adaptation to IoT devices.  For example,

- The Proof of Work system requires strong computational power and large amounts of memory on the end-node side, which are costly for consumers to adopt.  A "mining machine" for Bitcoin costs over USD 2000 per set.

- Mining under the PoW protocol is deliberately consumptive of power.  It is estimated that the Bitcoin network uses 0.14% of the global energy consumption and more power than several developing nations.

- As the PoW system gets bigger, the whole network slows down.

- The Proof of Stake system still requires large amounts of memory on the end nodes, and also large amount of tokens to be able to win the Blockchain reward.  The rich gets richer under the PoS system.

- Both PoW and PoS are leading to the centralization and accumulation of mining power into the hands of a few entities. Under PoW, giants like Bitmain's mining pools control close to 51% of Bitcoin's mining. Similarly, under PoS, original adopters of Ethereum who own large stakes can easily rake in all the fees from the network.

# Introduction

We have invented a completely new Blockchain protocol that

- Can run on most kinds of IoT devices without the need to change any hardware;

- Have a mining function to attract IoT device users to join up to the chain;

- Have a unique consensus protocol called "Proof of Assignment" that gives fair chance to all IoT devices to obtain mining rewards;

- Very light in overall power consumption; and

- Supports instant transactions even if the chain expands in size exponentially.

### Features of our new Blockchain architecture

- Divide the Blockchain network into different layers to reduce system requirement on the IoT devices (end nodes) side;

- End nodes do not have to have strong computational power or large amount of memory;

- All IoT devices can connect to our Blockchain without any hardware change;

- All the end nodes have equal chances of getting Blockchain rewards;

- The chain does not consume unnecessary power; and

- The chain supports instant transactions no matter how big it becomes.

From the Proof of Assignment consensus protocol, we have developed the "Micro-mining" protocol. Micro-mining is introduced so as to incentivize IoT device users to connect their devices to our Blockchain and provide usage data. In order to make it easy for IoT devices to connect to our Blockchain, we have also designed a new Blockchain architecture with end-nodes and trusted-nodes separated. Under this innovative new architecture, most of the IoT devices in the world, be them big or small, can run our micro-mining software without the need for any hardware change. For the first time ever, Blockchain and IoT devices can seamlessly work together.

We aim to connect every household in the world with Blockchain and collect their usage data for betterment of the whole mankind. This can be achieved through our easy to adopt Blockchain design, and a token reward system (IOTW tokens system). IoT device owners who join our Blockchain network will be rewarded with IOTW tokens. We shall establish a decentralized purchase network for the IOTW holders to purchase goods and services with their IOTW tokens directly from the device makers and service providers. This is a decentralized purchasing ecosystem to do away with all unnecessary middlemen and agents. The following pages will explain our technology and business case in more details.

# A High Instantaneous Throughput IoT Blockchain Architecture using Proof of Assignment consensus

## Motivations

Blockchain is arguably the most disruptive information technology (IT) in decades. Using distributed ledger architecture, Blockchain technology is poised to transform our society in many ways, revolutionizing our financial system, supply chain and even legal system. Yet, Blockchain technology has virtually hit a roadblock in the Internet-of-Things (IoT) arena, markedly limiting its applications in ubiquitous electronic devices and appliances in our daily lives.

The most popular Blockchain algorithms used today are Proof of Work (PoW) [NAKA08] and Proof of Stake (PoS) [KING12] algorithms. Unfortunately, both PoW and PoS are inappropriate for IoT applications because most IoT devices have very limited computing and memory resources, and power budget. To this end, we have invented a new Proof-of-Assignment algorithm that is suitable for IoT devices and is very robust, secure and scalable.

The PoW algorithm is used by many existing blockchains, including Bitcoin, in which miners compete to become the first provider of a cryptographical problem. It is not an environmentally friendly algorithm and consumes much energy. The complexity of the cryptographical problem increases with the growth of the size of the ledger size and is already demanding super computing power. Although PoW is useful for some applications, it is definitely not good for IoT applications.

In the PoS consensus process, a candidate is regularly elected among validators in the blockchain ecosystem. The PoS algorithm is less power hungry than the PoW algorithm because the above election process and the cryptographical problem solving do not require supercomputing power. Nevertheless, PoS is still not a good choice for IoT application because each node still needs to have substantial computing and memory resources.

Our Proof of Assignment (POA) algorithm is designed to gracefully solve these specific IoT issues.

| Miner of PoW (Proof of Work) | Miner of PoS (Proof of Stake) | Miner of PoA (Proof of Assignment) |

# Micro Mining

In the PoA algorithm, each IoT device is required to perform some simple but very important cryptographic tasks, known as "Micro Mining". On the other hand, these IoT devices are not required to handle the transaction ledger, which is maintained by a distributed Trust Node system.
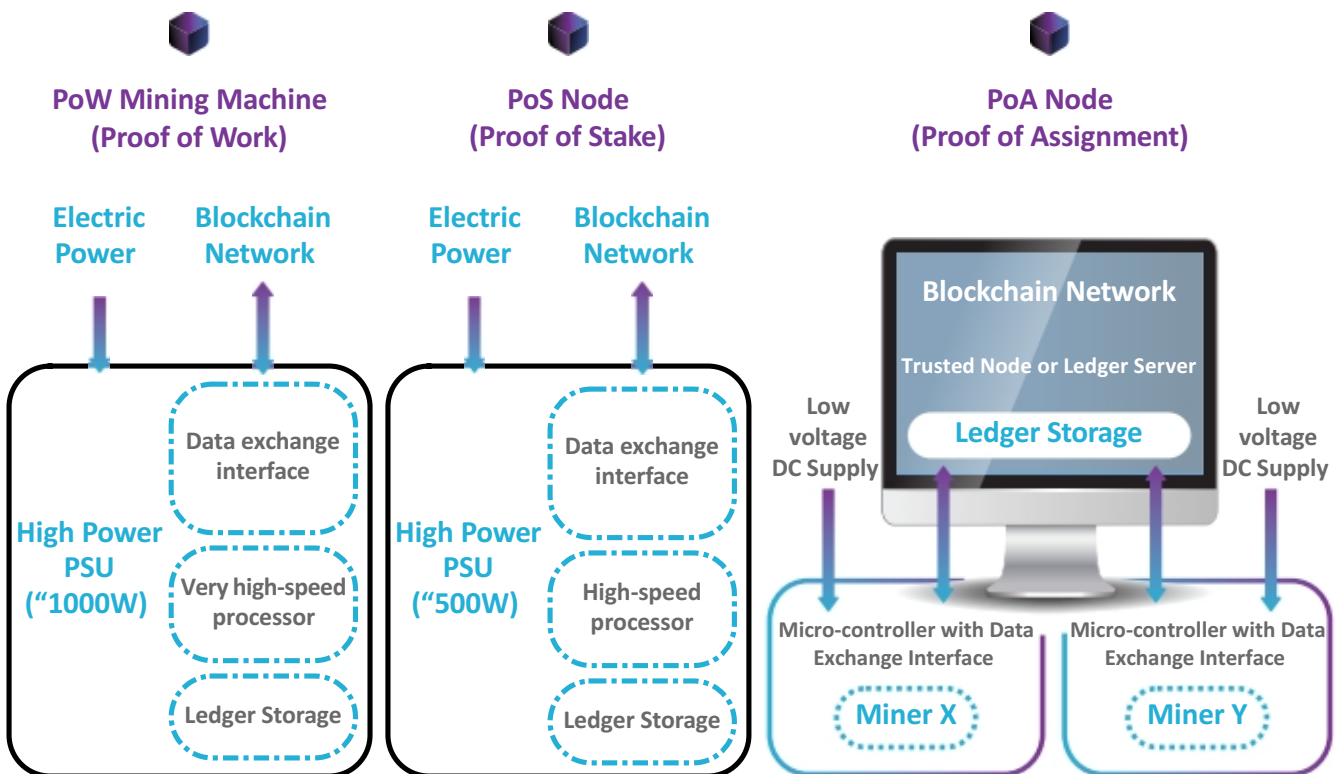


While PoS solves the energy wasting, ledger servers involved in such blockchain still need to have substantial memory capacity to accommodate the transaction ledger. The cost will then become not affordable for small IoT devices to become blockchain enabled. IOTW aims at removing such hurdle to enable the general adoption of blockchain in our daily used products. This will hopefully fuel the growth of blockchain transactions in our daily life.

Similar to PoS, mining devices in the IOTW blockchain do not require super computational power. In addition, IOTW removes the need for mining devices to store the transaction ledger. This removes the cost associated with the large memory and therefore adding mining capability to simple IoT devices will become affordable. The consensus algorithm behind the IOTW is proof of assignment (PoA).

Instead of allowing every network node to participate in mining in PoW, or having a voting process to elect the appointed validator for a transaction in PoS, PoA elects a single candidate or a limited number of candidates to solve the cryptographical problem by pre-agreed criteria (e.g. random, historic time connected to the system, among of cryptocurrency involved, etc.) and issue 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 servers or ledger servers. The PoA makes the requirement on computational power and memory capacity of the mining devices basic. An average micro-controller controlling functionality of products (e.g. electric fans, rice cookers, vacuum cleaners, air conditioners, printers, etc.) with network access and sufficient program memory to incorporate the mining software can become a mining device on the IOTW blockchain. Thus, the term Micro Mining is adopted for the mining process in IOTW to distinguish it from other conventional mining.

Since the cost for adding Micro Mining to any IoT enabled product is extremely low or near zero, together with the incentive of getting award during the operating life of the products with Micro Mining capabilities, it is anticipated that the adoption can be much more rapid than public blockchains today. This will bring blockchain technologies down to earth and spawns off various applications.

Initial launch of IOTW blockchain aims at creating a market place linking household appliance product manufacturer, agents, services providers, and end user. Accessing the IOTW blockchain via mobile phones, pads, and computers will also be supported. Product manufacturer, agents and distributors, service providers, etc., are strategic partners of IOTW blockchain and it is the aim of the IOTW blockchain to grow together with its strategic partners.

## Miner Selection Algorithm

To elect miner candidates from a large set of IoT devices, we can adopt the following two types of approaches. First, as for centralized approaches, we allow flexible design choices for selecting IoT mining device(s). For example, we can leverage the API server to perform the assignment allocation; or the API server can delegate the allocation task to a ledger server/trusted node. The assigning process can be random, where each IoT device has equal chance of being selected. Or, the assigning process might be weighted, so that each IoT device has different chance of being selected and is in proportional to their weights. In practice, we can use the reliability of the IoT devices, i.e., whether it has correctly performed mining in previous assignments, to build up their reputations as weights. Another possible approach is through generating public randomness and using it as a seed to select IoT devices, completely in a decentralized manner. Here we give one concrete instantiation using verifiable random functions (VRF). The public randomness seed can be generated via VRF, or via a multi-party computation protocol. Later, using seed, each IoT device (with public/private key pair <pk, sk>) can generate a specific hash value via (hash, $\Pi$) VRFsk (seed), where hash is a hash value and is a proof. Then, the IoT device can determine whether it is selected, e.g., via pre-defined characteristics of the n least significant bits in hash, and others can prove that the IoT device pk is indeed being selected via validating the given hash, and checking whether True VRFpk (hash, $\Pi$, seed) holds. Furthermore, as for selection criteria, we can either select IoT candidates randomly or in proportion to their weights on the blockchain, such as money units in their accounts.

# System Architecture

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

The IOTW blockchain has more network layer(s) below the ledger server mesh network. Mining devices may be linked to any one of the ledger servers 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, 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 with public blockchains today, 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 SPI servers collecting data, and carry 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 an income-generating source for the IOTW blockchain.

The following diagram illustrates 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.
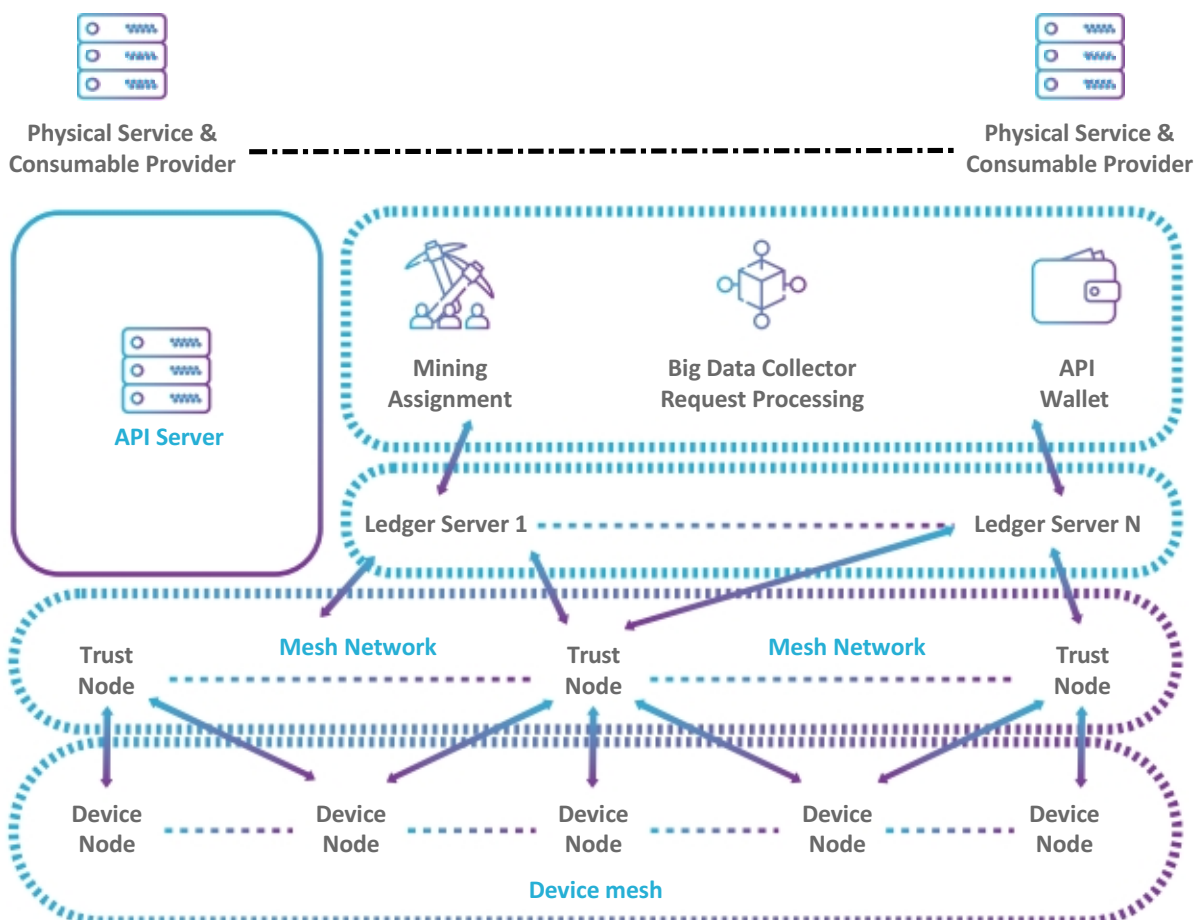
Blockchain ecosystems are normally more vulnerable to 51% takeover attacks when the number of ledger server nodes is small. As number of ledger servers grow, blockchains become more and more robust against such attacks. Therefore, special care should be taken during initial launch of new blockchains. 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. The makes the IOTW blockchain ecosystem not an open system at the beginning to trade for better system security.
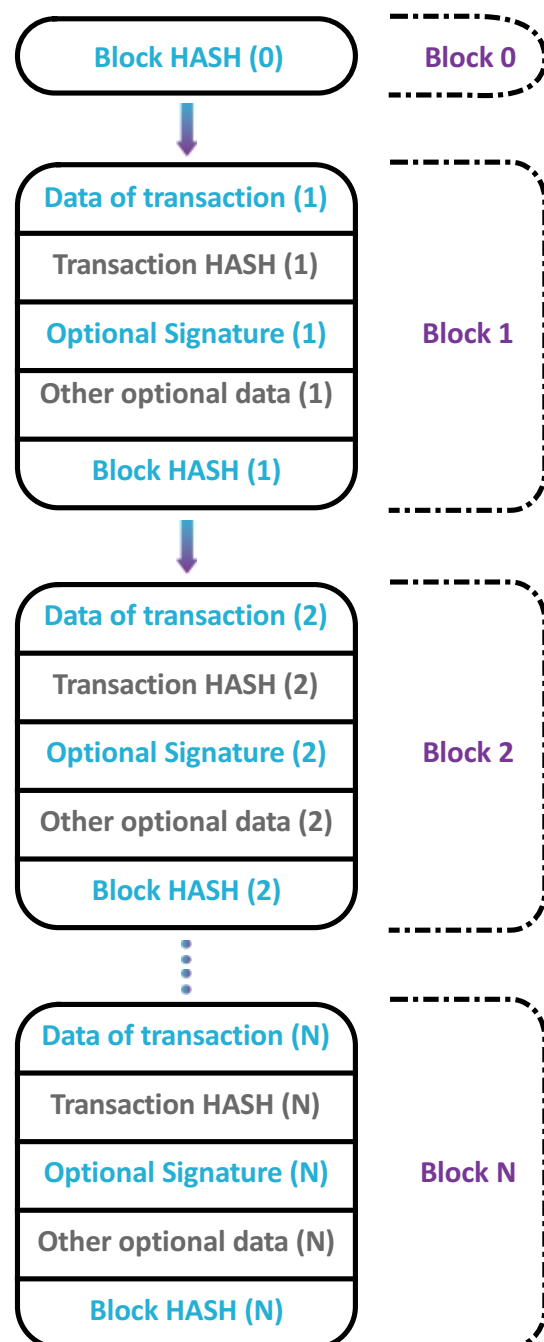
## Transaction Execution

Transaction request can be raised by any devices on the IOTW blockchain ecosystem having a valid wallet for paying or receiving of IOTW coins. A transaction request comprises the transaction information in terms of the nature of transaction such as purchase or selling 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 signature, day and time stamp, etc.

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

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

The following diagram illustrates a typical ledger with N transaction blocks

**Block HASH (0)**     **Block 0**

**Data of transaction (1)**

**Transaction HASH (1)**

**Optional Signature (1)**     **Block 1**

**Other optional data (1)**

**Block HASH (1)**

**Data of transaction (2)**

**Transaction HASH (2)**

**Optional Signature (2)**     **Block 2**

**Other optional data (2)**

**Block HASH (2)**

**Data of transaction (N)**

**Transaction HASH (N)**

**Optional Signature (N)**     **Block N**

**Other optional data (N)**

**Block HASH (N)**

# Security: Witnessing Protocol

Since transaction ledger is not being stored in micro-mining machines (IoT devices), the 51% hostile takeover 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 most robust against attacks. In addition, we are developing another algorithm to improve the security of the IOTW blockchain ecosystem.

Instead of validating a new transaction by just verification by IoT micro-mining and validating 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, this will greatly improve the security of the IOTW blockchain ecosystem. This is known as the witnessing protocol.

Security of the system will be growing with time as more devices get connected. We have a patented witness protocol that assumes a few devices from the pool of available ones will be picked up to sign and verify the transaction blocks. The block will be considered valid only if all devices will return the same coherent verification. In case of not coherent verification provided, all devices chosen for this verification will be blacklisted and removed from the pool. To further enhance security for single block, verifications originated from different geographical locations and different manufacturers can be chosen and connected to trusted servers residing on different cloud infrastructures (AWS, Google, MS).

Below, we give a more concrete analysis on the extra security strength brought by our witnessing protocol. Suppose we have n witness nodes being pre-selected in the setup stage. Assume that each witness node has a probability of p to be compromised by the adversary. Here the compromise probability p is directly related to the deployed security practices on how we protect the witness nodes. Then the probability (k) that exactly k out of n witness nodes have been compromised follows the binomial distribution (k;n,p), as given by the formula:

$$(k) = (k;n,p) = (nk) (1-p)-k$$

To put the above math formula in to contexts, if we pre-select the trusted nodes as witnesses, which are necessarily well-maintained in our system, then we can expect that the probability p would be extremely small. If we use a threshold based witnessing scheme, which demands t out of n witness nodes' signatures to audit the block, then the probability that no more than t witness nodes have been compromised by external attacker is given by the formula:

$$\sum_{k=0}^{t-1} (k) = (0) + (1) + (2) \ldots + (t-1)$$

Thus, if we follow the standard blockchain threat model (Byzantine), and set t = 1/3 witness nodes, then the above formula gives us overwhelmingly high probability that the adversary cannot control more than t witness nodes. While for witnesses serving by IoT mining nodes, we can expect that the probability p might rise. Nevertheless, we can integrate a combination of IoT mining nodes and trusted nodes as witnesses, and emphasize that the attacker has to compromise both the trusted nodes and selected IoT witness nodes at the same time to disrupt our ecosystem.

## IOTW Blockchain Network Management

The initial assignment of IoT devices to Ledger Server is 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 form by interesting individuals and companies to oversee the overall IoT ledger sever assignment and general network management, and its future development direction. Members of this committee come from different stakeholders who participate in IoT device manufacturing and selling chain. AnApp founding members have founded USB OHCI, 1394.A and participated in PCI SIG, wireless LAN standard development. AnApp has the skillset to push start such a 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 farm. The steering committee and AnApp will have the right to take legal action against such violation or shut down their operation. The target is put IOTW coins into common people's hand through mining.

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

## 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. Transactions are being generated using either cell phones or computers at the moment, but will soon be on other connected devices such as light bulbs and air purifiers as well. The blockchain ledger can be viewed in a computer screen (for demo only and not the future working version). The software is fully scalable.

Furthermore, the current implementation is target for instant transactions. The ultimate target performance would be 1M transactions per second. Our recent alpha testing of the platform resulted in 3,000 transactions per second for long distance network transactions and 100,000 transactions per second for local network transactions

Future development will focus on the following

- Implementation of a real IOTW blockchain ecosystem with user friendly MMI

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

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

- 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 user(s) to serve as witness to co-sign transactions. Signature(s) of the witnesses are generated by private key and validation of such signature(s) is done using the public key. This will greatly increase the difficulty for the 51% talk over attack due to the need to tackle simultaneously the witness's blockchain within the limited time of transaction processing.

# Mining Algorithm Comparison

| | Proof of Work (PoW) | Proof of Stake (PoS) | Proof of Assignment (PoA) |
|---|---|---|---|
| Compensation | Greater mining leads to higher rewards | Compensation increases as more people get paid | The more the mining nodes are, the more rewards we get |
| Crypto Currency | Bitcoin and many others | NEM、PeerCoin, etc Etherueum will be adopted in the future | IOTW |
| Computation Power Required | Extremely high | Lower than PoW | Extremely Low |
| Power Consumption | Extremely high | Lower than PoW | Extremely Low |
| Instant Transaction | ✖ | A few seconds | Less than one second |
| IOT Device | ✖ | ✔ | ✔ |
| Centralization | Mining is becoming more centralized | Ming can potentially be centralized | Mining is 100% decentralized |

# Business Model: B2B2C

Collecting usage data from IoT devices used to be very difficult. There are over 15 billion IoT devices scattered around the world, and they are too simple to run complicated blockchain software. Yet they contain so much information about people's daily lives. To enable and encourage IoT device users to connect to the blockchain network and share their usage data, we have invented the micro-mining system.

## 1 Getting Existing Devices Connected

People's behavior is hard to change. To get IoT device users to connect to our blockchain, we need to incentivize them. This is done through our micro-mining function. For existing IoT devices, we will work with different device makers to embed our system codes into their next firmware update. When the IoT device owners upgrade their firmware, their devices will be able to connect to our blockchain and start micro-mining to get blockchain rewards. The way of giving out blockchain rewards under the Proof of Assignment consensus protocol has been explained in the previous chapter. Once they get IoT, they will start to obtain IOTWs as they continue to connect their devices. If the users are willing to share their usage data, they will obtain extra IOTWs.

## 2 Partnering with Goods and Services Providers

In order to create value for the IOTW tokens, we need to have goods and services providers willing to take IOTWs as payments. We expect certain fluctuations in the value of IOTWs initially, and goods and services with high margins would be able to withstand such fluctuations in their payments. As such we are discussing with sellers of luxury goods, overstock items, digital contents such as music and videos, and online games to take IOTW as their payments. We shall make announcements when such discussions are concluded.

In the long term, as more and more devices are IoT to our chain and more and more households have IOTWs, the price of IOTWs is expected to stabilize. Then we expect more ordinary sellers of goods and services to be willing to take IOTWs as payments.

## 3 Collecting and Selling Usage Data for Device Owners

With micro-mining functions and IOTW rewards, IoT device users are motivated to connect their devices online and sell their usage data. Device makers, research institutes, government agencies, and other organizations can purchase such data from us with IOTW tokens. The IOTW tokens are limited in supply, but usage data are continuously being generated, and organizations will have regular needs of such information. Therefore, as more and more data are being generated, the demand for IOTW tokens will become higher and higher, creating a strong support for the value of IOTW tokens.

## 4 Instant Transactions Made Possible

We have installed our beta software into 1,000 Expressif wireless LAN chipsets and run a number of demonstrations to interested audiences in Malaysia, China, Hong Kong, and the US. The Expressif family of chipsets has cumulative sales of over 100 million units, and is still shipping millions of units per month. This is a clear demonstration of our software's lightness in very simple chipsets that can be widely found in many IoT devices.

## 5 Increasing Target Market of IoT Devices

In order to further increase the number of IoT devices for our blockchain, we have invented a Digital Power System chipset ("DPS chipset") that is a low-cost solution to replace traditional analog power systems in small appliances with digital power systems while giving them connectivity at the same time. We believe the DPS chipset will be able to see adoption by a certain number of device manufacturers for saving costs while increasing device functionality. We have already filed a patent for the DPS chipset design. We plan to file a few more patents for this new product.

## 6 Scalability & Sustainability

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

Starting from the formulation of the operating model of IOTW blockchain, recurrent income from transaction fees as well as service fees for big data are anticipated. Since the IOTW aims at building up a mass network with millions of IoT devices 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 transaction and service fees received can cover reward system as well as system management, maintenance and upgrade, as well as further development.

## 7 Decentralized Data Hosting

IOTW will develop and expand a decentralized data hosting platform for IoT device manufacturers. IoT device Manufacturers currently host data on centralized servers while paying high fees that hinders their scalability. Device manufacturers can end up paying up to $4 per device in a year, resulting in millions of dollars spent on data hosting. IOTW uses a decentralized network of devices and efficiently utilizes the existing storage and compute of devices to host Data for such IoT device makers. IOTW also partners with decentralized data hosting platforms to leverage their technology and provide a cost effective and efficient data hosting capabilities to partner IoT manufacturers. As a result of this, we are able to significantly reduce data hosting costs by up to 95% to $0.1 - $0.2 per device a year. This will inevitably allow for reduced prices of devices and increased access.

# IOTW Ecosystem
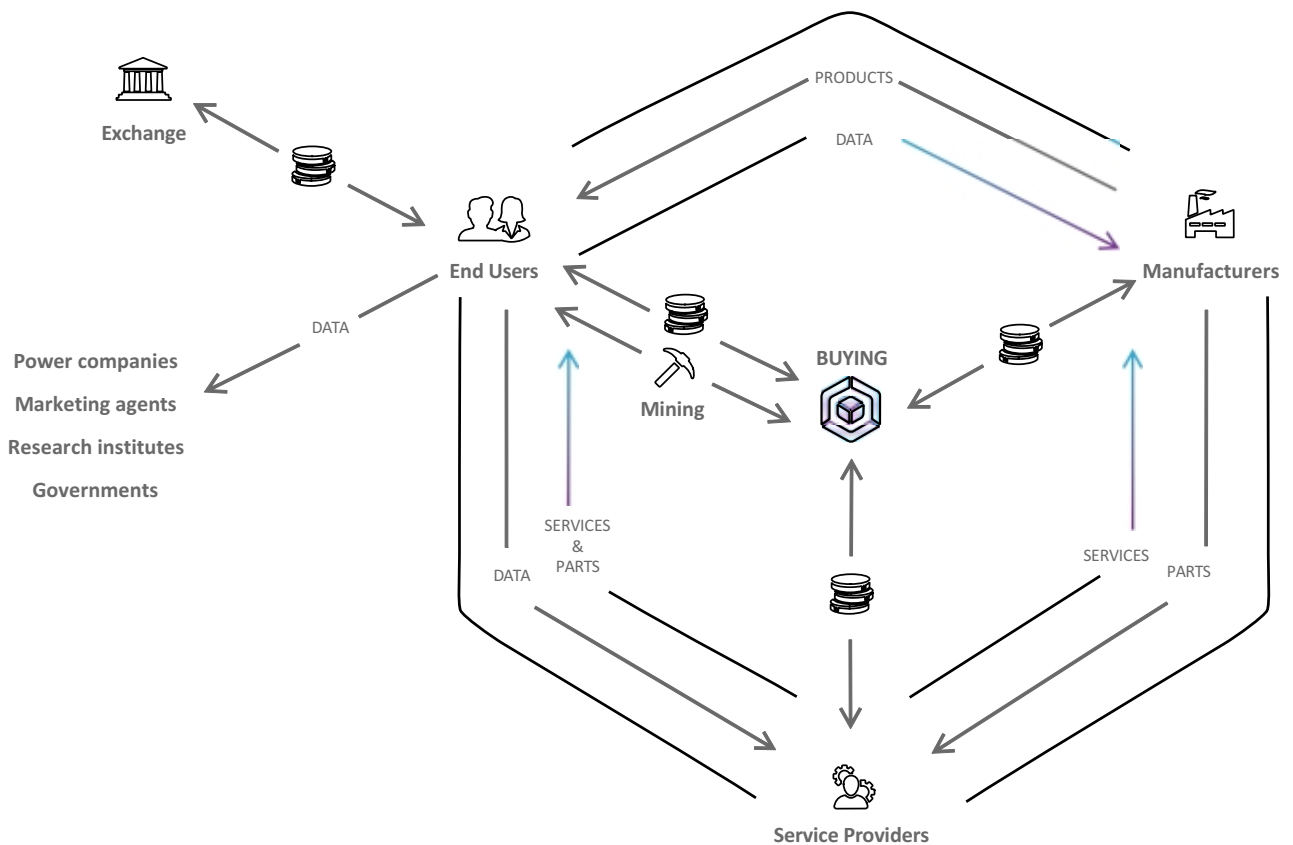


A ● Device users obtain rewards for mining and sales of usage data for IOTW

B ● Manufacturers and service providers purchase usage data with IOTW

C ● Goods and services providers sale through our online mall accep:ng IOTW as payment methods

D ● We will take a percentage as processing fee out of each IOTW transac:on.

# Competitive Analysis

| | IOTW | IOTA | IOTex |
|---|---|---|---|
| Specific hardware/CPU required | ✖ General purpose | ✔ Must run on their own CPUs/boards | ✔ |
| Mining | ✔ | ✖ | ✔ |
| Instant transaction | ✔ | ✖ | ✔ |
| Reward system flexibility | ✔ | ✖ | ✖ |
| System construction costs | 1/100s of normal | Expensive | Expensive |
| Security | High | Low | High/Medium |
| Mass deployment partner in semi-conductor, IoT hardware industry | ✔ | ✖ | ✖ |
| Application | Decentralized E-commerce platform, Payment system, Big Data Collection, Other enterprise usages | Micro-transaction | IoT information exchange with privacy |
| Token Utility | Payment, Micro-transaction, Purchase of Big Data | Micro-transaction | Unclear |

# Patents

We have both software and hardware patents. Our software patent relates to our innovative Proof of Assignment method of mining. We shall provide open license for software and product developers to develop and ship Proof of Assignment apps in IOTW devices.

| Patents | Filing Date |
|---|---|
| Input Current Profile Control Circuit (for reduction of THD and silicon EMI filter) | February 2018 (filed) |
| An Energy Efficient Mining Algorithm (PoA) | April 2018 (filed) |
| System And Method For Securing Blockchain Transactions (for improving blockchain security against attack) | June 2018 (filed) |
| Further software patent for blockchain application | October 2018 (expected) |
| EMI Cancellation Techniques (for silicon EMI filter) | October 2018 (expected) |
| Method to enhance light load efficiency | December 2018 (expected) |
| Further hardware patent on EMI Cancellation Techniques (for silicon EMI filter | January 2019 (expected) |

# IOTW

## Timeline
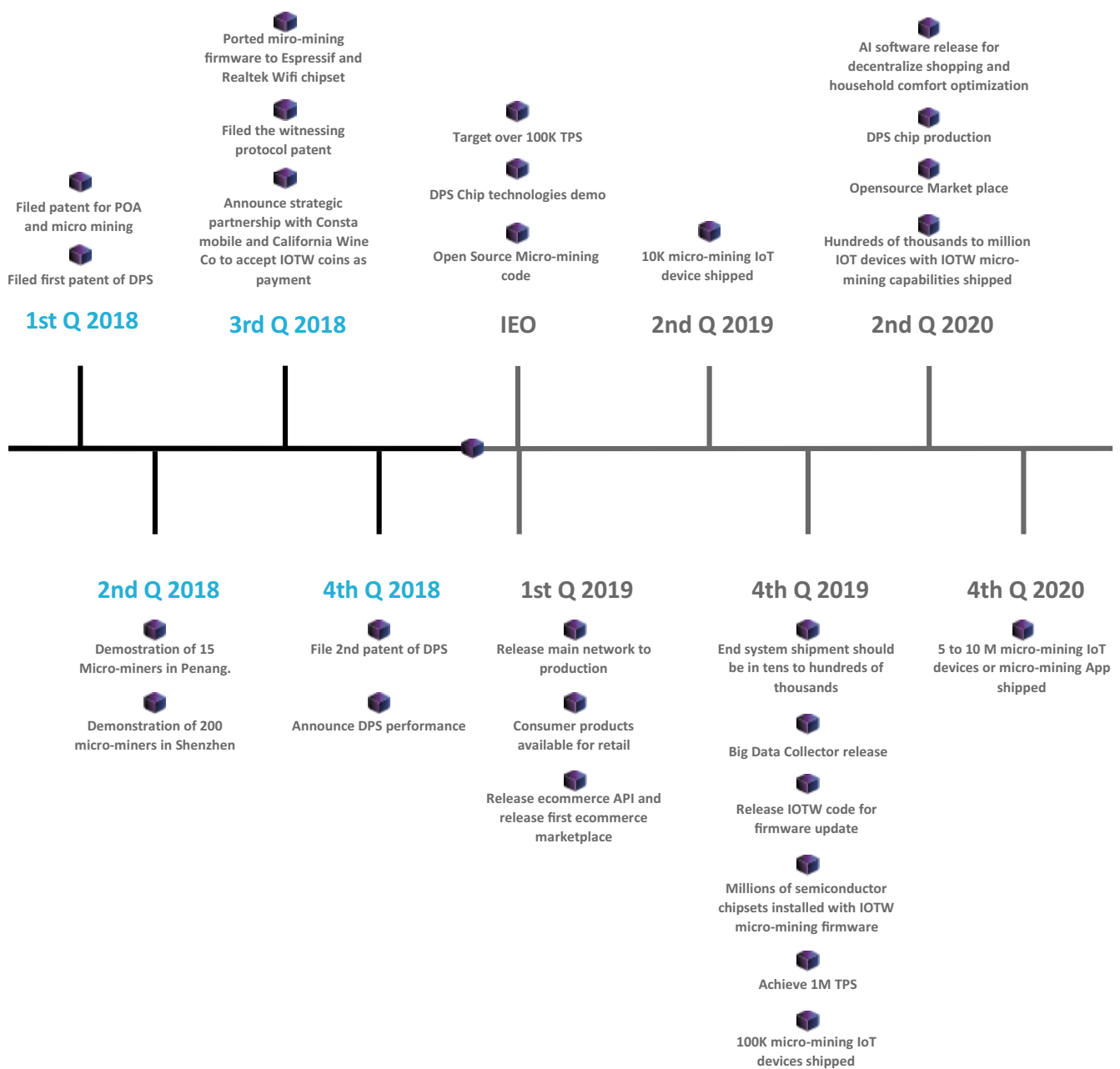
We have both software and hardware patents. Our software patent relates to our innovative Proof of Assignment method of mining. We shall provide open license for software and product developers to develop and ship Proof of Assignment apps in IOTW devices.

**Ported miro-mining firmware to Espressif and Realtek Wifi chipset**

**Filed the witnessing protocol patent**

**Target over 100K TPS**

**AI software release for decentralize shopping and household comfort optimization**

**DPS chip production**

**DPS Chip technologies demo**

**Opensource Market place**

**Filed patent for POA and micro mining**

**Announce strategic partnership with Consta mobile and California Wine Co to accept IOTW coins as payment**

**Open Source Micro-mining code**

**10K micro-mining IoT device shipped**

**Hundreds of thousands to million IOT devices with IOTW micro-mining capabilities shipped**

**Filed first patent of DPS**

### 1st Q 2018    3rd Q 2018    IEO    2nd Q 2019    2nd Q 2020

### 2nd Q 2018    4th Q 2018    1st Q 2019    4th Q 2019    4th Q 2020

**Demostration of 15 Micro-miners in Penang.**

**File 2nd patent of DPS**

**Release main network to production**

**End system shipment should be in tens to hundreds of thousands**

**5 to 10 M micro-mining IoT devices or micro-mining App shipped**

**Demonstration of 200 micro-miners in Shenzhen**

**Announce DPS performance**

**Consumer products available for retail**

**Big Data Collector release**

**Release ecommerce API and release first ecommerce marketplace**

**Release IOTW code for firmware update**

**Millions of semiconductor chipsets installed with IOTW micro-mining firmware**

**Achieve 1M TPS**

**100K micro-mining IoT devices shipped**

# IOTW

### 1 ◈ Fred Leung, Founder & CEO

- BS, Electrical Engineering & Master, Computer Engineering.
- Founder of a number of semi-conductor design companies in Hong Kong
- 30 years' experience in semiconductor industry with full exposure to chip set design, production, sales and marketing
- Co-inventor of Proof of Assignment for blockchain application
- Created the world's first AMD CPU chipset for notebook as working at Acer Labs and pushed Acer Labs' IPO in Taiwan. Set up wireless division in Chung Nam Electronics with profitable products accepted by Dell, Lexmark, Korean Telecom. Owns 10 chip design patents.

### 2 ◈ Marcin Dudar, Founder & Chief Blockchain Officer

- 20 years' experience in embedded software for security, semiconductor, set-top box and internet industry with chip-full exposure to DVBS set-top box IC firmware, DVBS & internet set-top box control and security software, internet digital picture frame software, video server database, etc.
- Blockchain software expert.
- Co-inventor of Proof of Assignment for blockchain application
- First person to decrypt Nintendo to create Gaming DVD in Acer Laboratories Inc. CTO of NixPlay. Built US's number one Internet Picture Frames. Built both the hardware and software infrastructure with 30 engineers.

### 3 ◈ Peter Chan, Founder and CTO

- M.Sc in Electrical & Electronic Engineering.
- Founder of Mosway Technologies Limited. 37 years' experience in semiconductor industry with exposure to setting up wafer fab, testing laboratories & IC design.
- Set up the first wafer fab in HK for Elcap Electronics Ltd, experience design in ROM, SRAM, DRAM and a series of computer chips, e.g. UART, USART, PPI, etc.
- Set up and ran an accredited electromagnetic compatibility (EMC) testing Centre in the Hong Kong Productivity Council

### 4 ◈ Tony Chan, Founder & CFO

- Bachelor of Business Administration, Master of Accounting Science.
- Member of American Institute of CPAs (AICPA), Chartered Management Accountant (CMA), Chartered Financial Analyst (CFA)
- Over 20 years of financial markets experience, including front line positions at the investment banking divisions of major international investment banks including ING Barings, Credit Suisse, Standard Chartered Bank, and Rabobank, focusing on IPOs, cross-border mergers and acquisitions, and fund-raisings

## 5 🔷 Dr. Patrick Hung, Founder & Control System Advisor

- Ph.D. in Electrical Engineering from Stanford University
- Hong Kong University of Science and Technology Consultant. Stanford University, Consulting Assistant Professor.
- Co-founder / CEO, Alta Sicuro Technology -- cloud and data security.
- Principal, Velosti Technology -- fabless IC Design House on high- performance, high-security & low-power solutions.

## 6 🔷 Kartik Mehrotra, Head of Business Development

- UC Berkeley graduate in Economics and technology entrepreneurship
- Early investor in Ethereum, Bitcoin, Stellar, Neo and Zcash.
- Hedge Fund advisor at G2H2 Capital.
- Previously, Consultant at Deloitte, consulted for ICOs and Blockchain companies.

# 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.

[STATISTA] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)