µNEST

Trusted data is the cornerstone of all future applications

2018-6-5
Ver.1.0

Neo MA
n@iotee.io

Table of Contents

Background

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. Gartner, Inc. forecasts that 20.4 billion connected things will be in use worldwide by 2020. Nowadays, no matter from smart home to smart building, or from sharing economy to smart mobility, and from smart parking to smart energy, we cannot ignore IoT even in a single minute.

At present, the realization of “Industry 4.0” proposed by the German government and the “Made in China 2025” plan proclaimed by the Chinese government should be based on well developed IoT industry. Internet could not meet the requirements of the whole industry at the moment nor in the future. There will be much more CPUs, Sensors, processors, memory than ever before, generating tons of data all the time from the fields of industry related manufacturing, supply chain, smart meters, testing and the like.

In recent years, many countries proposed the concept of Smart City and have been striving to put into practice in all kinds of “Smart” living areas like agriculture, communications, healthcare, government administration, education, smart grids, smart retail, and entertainment, etc. The city makes the life better, the better life comes from “SMART”, which is supposed to be built on cutting-edge technologies and IoT will be the essential one to contribute to the wonderful scenery of human being in the future.
Last but not least, The M2M (machine-to-machine) interaction has also, and will, more and more draw the attention to all parties due to its natural characteristics. It may revolutionize our current payment system and payment habits step by step.

Current Issue and Pain Point

Though IoT is everywhere, surrounding us in our lives, the massive data generated from it hasn’t been treated and processed carefully, especially in the field of **privacy** and **security**.

Almost all the time, our personal privacy data is collected by “big companies” and hackers for various commercial purpose illegally and FREELY. Recently, a report released by Consumer Watchdog, an American consumer protection organization, showed that the patent applications from “two giants” revealed how its smart sound box “eavesdrops on” users. According to the organization’ s research, the patent applications of the two giants can be found that these devices could be used as monitoring devices for collecting a lot of information and for advertising as well. The research warns that in the near future, the smart sound box can monitor all kinds of voices in the family. The new version of smart home products can even collect user data and sell products to the relevant people. It seems mankind have no place to hide. Meanwhile, the deployment, upgrading and maintenance of the IoT system itself is also lack of security management, which has become a bottleneck for large-scale commercialization and development of IoT. For example, in 2016, the botnet Mirai that launched the largest DDoS (Distributed Denial of Service) attack in the world is resulted from comprised unsafe home cameras and home routers. Data collection, transmission, processing, storage and so on will involve **data integrity matter**, which brings various challenges to the deployment, upgrading and maintenance of the IoT.

The infrastructure of today’ s IoT is almost all in c/s mode. This mode is **centralized** which has the drawback of the single point failure. For example, the Top2 shared bike company often has a system failure that a large area of bikes cannot be unlocked. Along with the number of terminal devices increasing, the entire system faces scalability challenges. Another challenge of centralization we’ re facing is that, today, the PKI (Public key Infrastructure), which is the cornerstone of current cybersecurity, has been fragmented. Kinds of powerful organizations can get totally legitimate certifications for MitM (Man-in-the-Middle) attacking purpose.

Although big internet corporations and organizations are “harvesting” personal privacy data all the time, they cannot share or trade it between themselves. The data becomes **Information Silo** due to various barriers. For example, the patient needs repeated inspection by different medical facilities due to lack of trusted medical records sharing mechanism between medical institutions. Also the Information Silo phenomenon in vehicles’ life-cycle costs tons of dollars every year, all because it cannot be shared among auto manufacturers, 4S shops, insurance companies, vehicle maintenance points and end users, which resulting in serious information asymmetry, operating costs rising, and maintenance fraud. In second-hand market of vehicles, the tampered odometer cases are not new to us anymore.

Hackers also gain illegal profits through the endless stream of technical means to obtain personal and industrial IoT data.

With the re-emergence of AI, the data source for AI model training is a crucial part of AI scenarios, and it is no exaggeration to say that this is the most important precondition. Garbage in garbage out, without complete, unpolluted data, AI model training will become a "joke” , not to mention the AI applications in real life.

Thus, IoT means everything about data, who could truly protect the security of the data?

Our Proposal

IoT + Blockchain, builds the cornerstone of all future applications by providing trusted, integrity and completed data, which enables value exchange and efficient collaboration in a non-trusted environment.

A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. The Harvard Business Review describes it as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, food traceability or voting.

The first blockchain was conceptualized in 2008 by an anonymous person or group known as Satoshi Nakamoto and implemented in 2009 as a core component of bitcoin where it serves as the public ledger for all transactions.
IoT and blockchain have so many matching points that we think they are made for each other. In particular, the deep dependence of applied cryptography makes blockchain technology one of the feasible and preferred solutions to solve the security problems of IoT. Smart contract technology also brings new dawn to M2M interaction.

IoT + Blockchain projects status quo

At present, there is not a shortage of IoT + blockchain projects on the market, but we see that all these projects have different levels of deficiencies. This is also the most important reason why we are determined to do another IoT + blockchain project.

Some high market cap project, which employs DLT (Distributed Leger Technology) with DAG (Directed Acyclic Graph) as the underlying technology trying to address issues such as IoT’s scalability and M2M interaction by eliminating "transaction fees". But up to today, due to DAG's weak consensus, their test network still requires a centralized "coordinator" as a facilitator to complete its whole network’s transactions. The facilitator is a closed source blackbox, about which nobody knows at all. In the meanwhile, the “triad chip” R&D keeps secret to the audience, too. Last but not least, its homebrew hash algorithm has been proved unsecure.

A certain Telehash based IoT project, which uses bitcoin network as payment channel, leverages the special RF equipment to build up technical barrier. While on the other side, the homemade RF is also regarded as a double-edged sword since it brings potential difficulty for network deployment, maintenance and upgrading in real mass production environment. Along with bitcoin prices’ continue increasing, transactions through

bitcoin network make their transaction fee expensive and unaffordable, which is a big hurdle for the use of massive data on IoT.
Some consortium blockchain from a big corporation is only on framework stage with various access restrictions. The solution portfolio is too expensive to build even a PoC (Proof of Concept) for normal developers.

Another IoT + blockchain project based on Ubuntu Core and Ethereum is still at the conceptual stage. Ethereum's expensive transaction cost, network high latency and frequent fatal smart contract issues have left the project with an uncertain future.

There is also some traceability project named after IoT + Blockchain, but they put source data on-chain from cloud through layers of traditional IoT architecture system. The system design obviously cannot guarantee the data integrity.

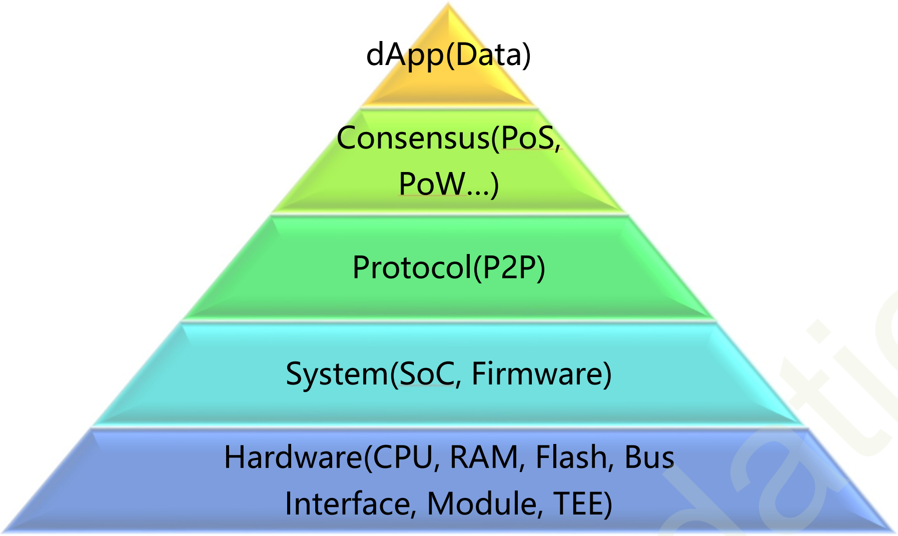
Although projects above have tons of problems, the combo technology of IoT and Blockchain is still very attractive to the world. While for ordinary hardware or software developers, the threshold is extremely high. Even it’ s not easy to verify an idea of IoT + Blockchain in quick and sound way.

Here comes μNEST!

Infrastructure of μNEST pub-blockchain project

Our proposal is to lower the entry barriers for IoT + Blockchain integrated technology and allow normal developers to quickly deploy PoC. Therefore, we will develop a pub-blockchain along with hardware, which is dedicated to IoT in order to make up for the shortcomings of today's projects. We put the security of IoT to another high level while decreasing the transaction fee of the blockchain at the same time.

IoT is about everything of data and trusted data ensured by blockchain will be the cornerstone of all future applications, enabling value exchange and efficient collaboration in a non-trust environment. Our project, μNEST, will be the trust of a chain and the chain of trust.



Pic 1

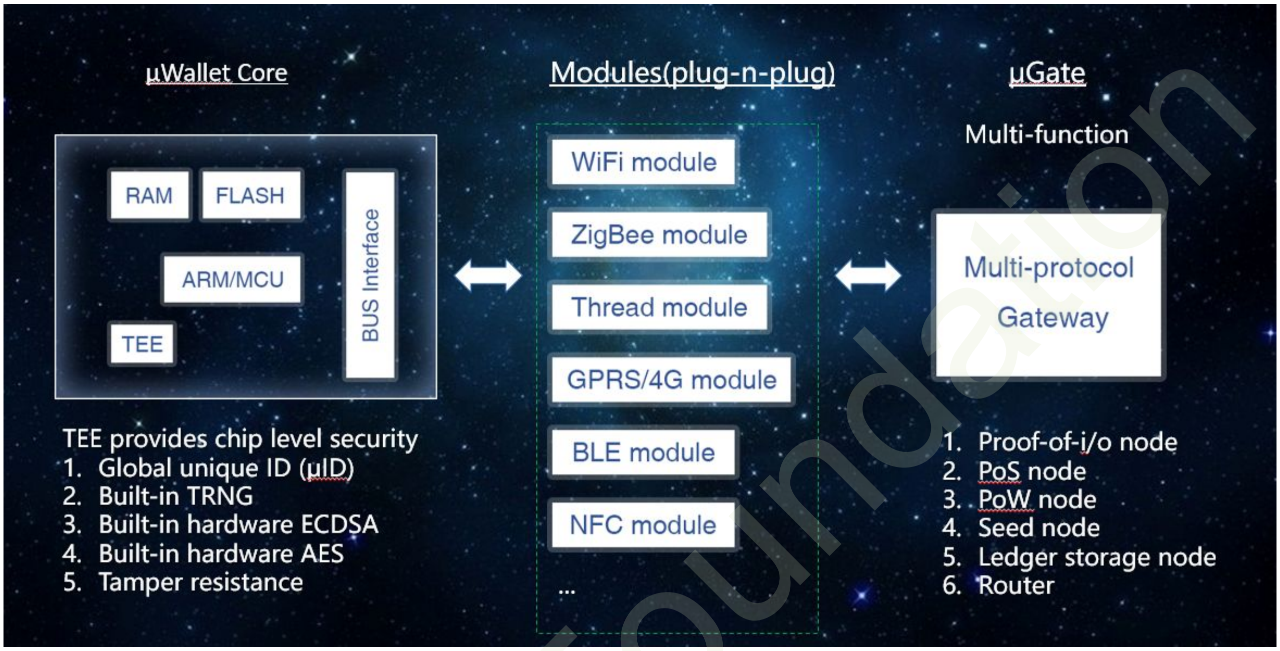
As shown in picture no.1, **µNEST fuses IoT and Blockchain together. It builds the trust chain from the hardware level of TEE (Trusted Execution Environment)** to consider and solve security issues. The whole system’ s trust can be guaranteed from chip level. Starting from TEE, this trust chain provides integrity checks for the system layer (SoC), firmware, and driver layer to prevent these layers from being vandalized and replaced. The p2p protocol layer, consensus layer, smart contract and distributed application (dAPP) layer of the blockchain ensure the functionality and role of value exchange in unfamiliar environments without the need of third-party trust.

The most import benefit of the whole trust chain is data integrity which is mathematically verifiable.

µ NEST core technology

By TEE technology, µNEST builds the trust without having to rely on 3rd parties root trust. As shown in picture no.2, µNEST's smallest hardware PCBA is called **µWallet Core** that is composed of a microprocessor (MCU or ARM), RAM, Flash, TEE and Bus Interface. The TEE provides chip level security for the entire µNEST. It has a built-in and the global unique hardware ID along with other elements designed for security, such as TRNG (True Random Number Generator), hardware ECDSA (Elliptic Curve Digital Signature Algorithm), hardware AES (Advanced Encryption Standard), etc. And the TEE is tamper resistance. From a blockchain perspective, µWallet Core is a naturally safe hardware wallet. No matter IoT or Blockchain, today, they still need to access the Internet to achieve specific functions.

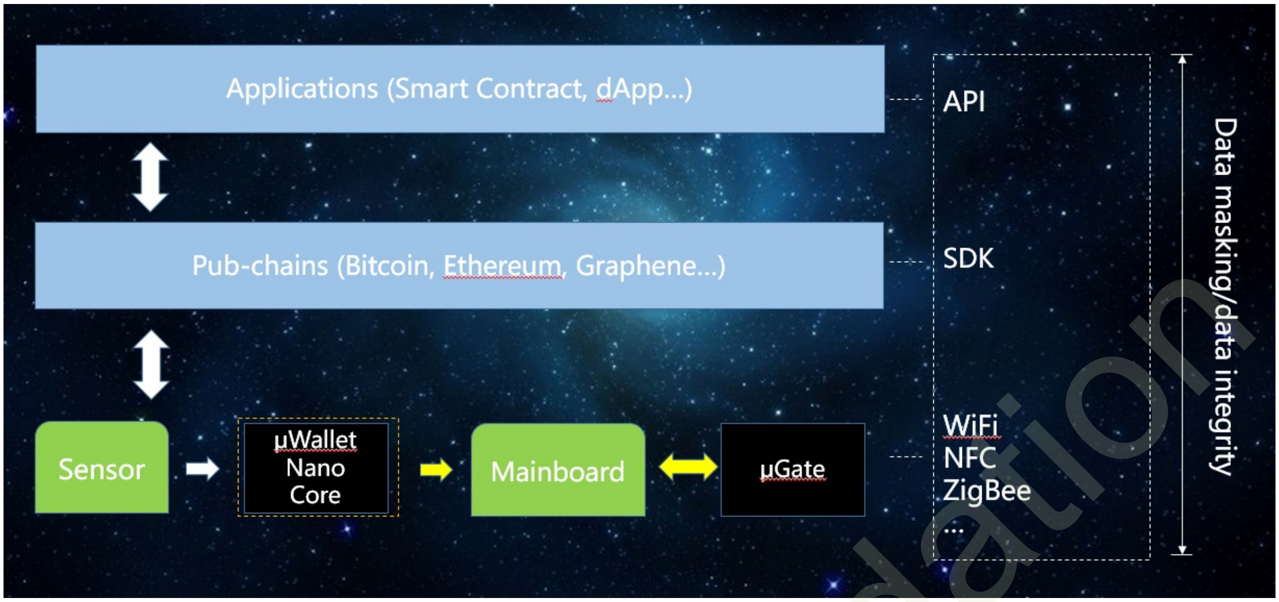
For such reason, we design another piece of hardware, which will be a multi-protocol and multi-function gateway. It could work as a normal router to Internet, a full-node of blockchain, a seed-node of blockchain and a “miner” of blockchain. We call it **μGate**.



Pic 2

In the connection between μWallet Core and μGate, we make the modular design of PnP(plug-n-play). We will use mature mass production modules from kinds of mature manufacturers, including but not limited to WiFi module, ZigBee module, Thread module, GPRS / 3G / 4G Lte / 5G / NB-IoT modules, Bluetooth Low Energy (BLE) modules, Near Field Communication (NFC) modules and more.

μNEST application architecture


Applications (Smart Contract, dApp...)
Pub-chains (Bitcoin, Ethereum, Graphene...)
Sensor
μWallet
Nano
Core
Mainboard
μGate
API
SDK
WiFi
NFC
ZigBee
...
Data masking/data integrity

Pic 3

In real life IoT scenarios, just as described in picture no.3, in order to ensure the integrity and high level security of the entire IoT data, we recommend designer to keep the μWallet Core as close to the sensors as possible. At the same time, we μNEST also provide SDKs and APIs to enable ordinary developers to quickly implement PoCs with the given structure of μNEST, normal developers could build their own secure applications that have the math-proven data integrity and data masking advantages. Obviously, high security is a costly consideration and μWallet Core can be eliminated in some specific scenarios that are very cost-effective to implement without of the highest security requirement. System security begins with the μGate layer.

Functionally, μWallet contains two important parts, μID and Status. Where μID is the global unique ID, all things and people can have unique, naturally distinguishing and identifiable eigenvalue as ID. Every single person has some unique features that can be distinguished from each other such as fingerprint, voiceprint, iris, facial features, etc. For things, this unique feature can be the MAC, TEE serial number, building mailing address, or a vehicle license plate number, barcode, QR code and so on. Status is the attribute of all things or human beings at some moments and in some places. It contains time stamp, space (such as GPS), degrees (such as health, satisfaction), status (availability for example), value (price, commissions), degree (temperature or humidity) and so on. μWallet is the entry point of all applications based on μNEST and plays a crucial role in the overall system as well as the basis for M2M payment.

As mentioned above, multi-protocol gateway (μGate) has a dual role, in which the mining node from the perspective of the blockchain can either be the witness node of the dPoS consensus algorithm or the μNEST unique mining node - Proof-of-i/o node. The Proof-of-i/o is our patent pending “mining” algorithm. It will calculate the network i/o, the storage i/o of μNEST network, together with the weight of μGate’ s uptime. The Proof-of-i/o is mainly an incentive method in bootstrap period and the uptime of μGate nodes will benefit the whole p2p network, too. It is designed to motivate more people to participate in μNEST's underlying network, making the whole network more stable and distributed. We will descript the Proof-of-i/o algorithm in other paper in detail.

μNEST underlying consensus algorithm

We will employ the improved version of dPoS (delegated Proof-of-Stake) as μNEST’ s underlying consensus model. All blockchain is actually a deterministic state machine that establishes transactions. Consensus is a process of agreeing on a sequence of transactions and filtering of invalid transactions. There are currently many different consensus algorithms that can make packaged transactions, while dPoS is proven to be the most robust, secure, efficient and decentralized one by years of reliable operation of multiple blockchains. dPoS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates. Deterministic selection of block producers allows transactions to be confirmed in an average of just 1 second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference. For more details, you may check the wiki of it.

μNEST unmatched features

- Light but secure mobility wallet App both for iOS and Android;
- Soft router with supporting to PoW, PoS, dPoS, xBFT, etc.
- Ultra-low-cost hardware implementation benefiting from our 15yr industrial experience;
- Well tailored and power efficiency IoT solutions;
- Modular design for plug-n-play applications and easy for mass production;

- Rich hardware interfaces（UART，SPI，I2C）and software SDKs、APIs, seamless access to the mainstream public chains;
- Optional national cryptograph algorithms（SM1，SM2，SM3）;
- High availability and high reliability.

Business Scenarios

This section enumerates only a few scenarios of µNEST, the vastness of µNEST is not limited to this.

- **“shooot”, an APP for digital photos and GPS info. Sharing** (Right verification and transaction for photo, real-time geographical information sharing)

The invention of camera let people keep and hold the “moment”. The function of photograph has also changed with time flying and technology progressing. The copyright and value of digital photos become a disturbing factor problem to today’s social life.

The advances in technology and law have made some progress on the issue of the verification of rights, while the issue of eradication of disputes has not been solved. µNEST gives out its own application examples from both the technical and the economic aspects. By combining µNEST’s µID and Status technology, the APP shooot could take the unique physical info from device as the µID, and other meta info of the photo and device as Status. The original author could also add other patterns to the photo as Status, e.g. the copyright requirement he or she wants to deal with the photo, free for use or with certain selling price. The µID and Status of the photo will get on chain, the original photo will be securely saved with privacy being masked. When original authors share, contribute their work to “shoot”, or get "Likes", the original author can get different token incentives. µNEST’s distributed matchmaking engine can help the original author sell their art works and even bidding. With blockchain, all footprint of the art works could be recorded with time stamp. The creative µID and Status technology solves the drawbacks of merely doing hashing for photos and avoids the waste of computing resources for image recognition deep learning algorithms.

This scenario can also be extended to similar scenarios such as real-time geographic information sharing and trading. For example, when someone wants to see the recent aurora borealis of Fjord Norway, he or she can make a request be broadcasted in μNEST, there happen to have a tourist in Fjord willing to share the immersive picture or video, who could upload it onto μNEST. Based on the visitor's existing μID and Status information, as well as obeying the smart contract relating to transactions, the two can use token to complete the information exchange trading.

The above two examples are essentially applications that belong to "Right Verification and related Transactions", which verify the original owner's exclusive ownership of the work's copyright, and ensure the interactions surrounding the copyright permission or assignment smoothly and correctly. In the future, third-party companies could develop their own blockchain-based "Right Verification and related Transactions" applications based on APIs and SDKs provided by μNEST. At the same time, we will also provide mathematically proven underlying data masking techniques as well as anti-cheating algorithms to safeguard the rights and trading / interaction process of eco-participants.

- **New world of smart home and intelligent equipment**

Currently, smart home system security and privacy of personal data has been highly criticized. On the one hand, with the progress of society and technology, the public demand for intelligent home automation is on the rise. On the other hand, the centralized solution does not place smart home’ s security in an enough important place (for example, the Mirai bot event). And the big company’ s products are collecting user private data all the time, which has become the industry "open secret". In the future, μNEST-based hardware and software ecosystem could be a good solution to such problems. Multi-protocol routers provided by μGate can be used as a home gateway for security, which solves the problem of smart home security by "coordinating" interoperability among different protocols such as WiFi, ZigBee, and Mesh. At the same time, we provide APIs and SDKs to facilitate third-party companies (such as smart home and smart hardware providers) to make math-proven products and applications with secure private data protection. In such case, user data is masked and securely stored in μGate’ s local storage space to achieve a "distributed storage" style.

Therefore, while using the smart home or intelligent equipment products developed on μNEST, customers can clearly know the data has been desensitized in the acquisition process, personal privacy will not be violated. Also, customers could choose which application data be sold to the vendors for the token activation. In the future, in all areas of the “data market”, users, vendors, third-party companies or other data demanders will be able to make transparent, secure and desensitized data transactions through μNEST. Similarly, intelligent equipment manufacturers, such as sports bracelet manufacturers, based on μNEST technology, can develop products that attract customers in security and privacy protection aspects. Customers can choose to sell the multi-dimensional and desensitized data related to personal sports to manufacturer or third parties to get token incentives. For producers or third parties, they can not only get supporting for business decision / market expansion based on the desensitized and sound data, but also feed their professional research and analysis data back to the community or sell them to get token incentive, promoting the healthy development of both business and μNEST eco system as well.

- **Digitalization application scenarios: Sharing economy**

One pain point in the sharing economic scenario is the “handover” problem of shared objects in untrusted environments. In our opinion, the core of the sharing economy is that the state of shared objects in untrusted environments varies with time and position, as well as locking and unlocking status. This can be abstracted as a state machine + lock.
The backbone blockchain of μNEST is the state machine recorder, and μWallet is the lock. The μID and Status of the shared objects will be broadcasted to μNEST’s blockchain according to a certain algorithm, the filed in Status including availability, price, arear, frequency, etc. The demanders can broadcast fields (regions, times, etc.) of their own μID and the "demand" in the Status and the price range they are willing to pay. The μNEST’s distributed matchmaking engine will match the transactions and use the smart contract to track the locking status of the μWallet. After usage, smart contracts call M2M payment to complete the transaction.

Whether sharing bicycles, sharing house rental locks, sharing charging equipment, sharing umbrellas, personal belongings, everything can be shared "object", by μID / μWallet being tagged, can participate M2M payment scenarios in μNEST eco system. We also provide standard APIs and SDKs for developers.

Of course, μNEST's unique μID + Status technology can also be used in diversified financial scenarios such as asset digitization.

Not limited to the above mentioned scenarios, various applications developed based on μNEST underlying architecture can also be widely used in various fields of smart life in future cities such as V2X, traceability, supply chain, smart home, smart travel, smart tourism and smart energy, etc. Meanwhile, μNEST will enter the AI field at the right time.

μNEST project summary

- Innovative features:

  Solve IoT security issues, data integrity and privacy issues, to achieve multi-party value interaction and efficient collaboration in a non-trusted environment. Different from most "similar projects" on the market, all the μNEST underlying technologies are mathematically verifiable, and the hardware and software are open source, with a wide range of industry coverage, cost-effective and maneuverability.

- Target customers:
  Personal Developer, Startup, Small and Medium Business
- Basic Products:
  μWallet, μGate Miner, Public chain for IoT, μGate-based APIs, SDKs
- Eco system establishment:

  - C-side users:
    Cryptocurrency Hardware Wallet μWallet User
    μGate” Miner” Users (Marketing, Maintaining μNEST initial network robustness)
    Application users (desensitized data based on μNEST technology for token activation)
  - Personal Developers / Startups:
    In the future, μNEST foundation will reserve a fixed proportion of token to support PoC on μNEST. For different application scenarios, μNEST will provide a certain standard SDK / API interface (to reduce IoT + blockchain innovation

access threshold, reduce development and operation costs, increase productivity and business flexibility).

- SME:

  Provide µNEST-based solutions for different application scenarios, hardware and software technology architecture and implementation

  Provide complete first-hand information for business decision-making / expansion through transparent, secure and desensitized "Data Trading"

  Desensitization of corporate data to feed the community to promote cross-industry data exchange, to achieve multi-party collaboration and improve production efficiency
- Open source community technology maintainer
- Cryptocurrency investors

µ represents one part per million, and NEST stands for colorful applications. µNEST' s vision is to become the "Nest" for future life. Based on µNEST's solid underlying technical support, people can enjoy the comfortable and warm life brought by various safe and efficient intelligent applications.

Roadmap

~3m

- Testnet getting online
- µGate PoC
- Proof-of-i/o algorithm PoC
- Fund-raising

~12m

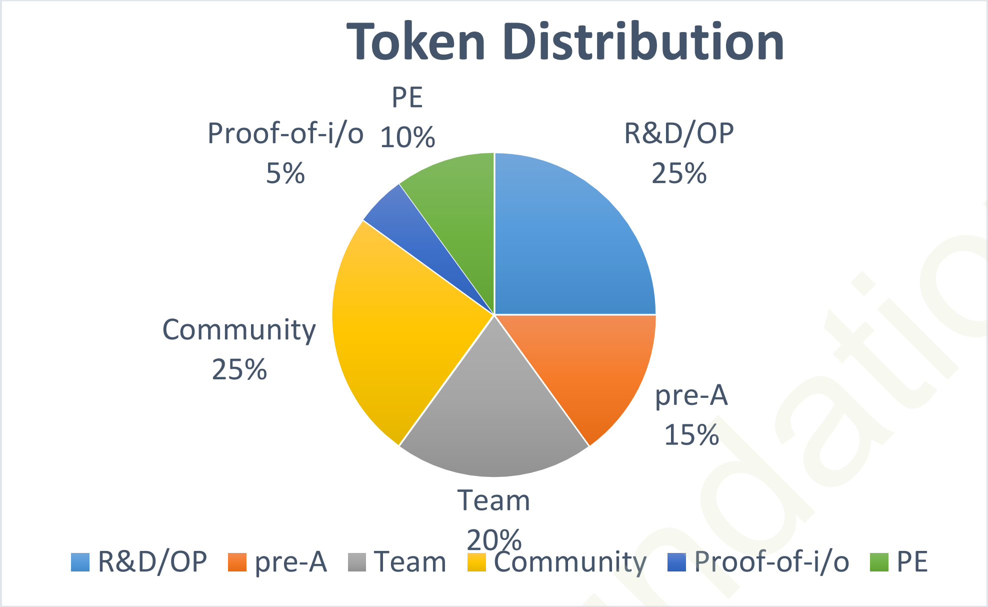
- µWallet hardware PoC
- µWallet software (mobility App , PC side , Mac side , Linux side)
- µGate pilot-run
- µGate API , SDK
- Smart contract
- "Shooot" App
- Testnet code auditing (security , reliability)
- Mainnet getting online
- M2M payment (PoC)
- Community build-up

~36m

- Fulfilled at least 5 projects (traceability, v2x, sharing economy, etc.)
- Smart city
- AI
- Breaking even

Token Distributions

μNEST has total 7billion tokens, code name NEST.



20% of it for start-up team member, core developers, advisors, etc. and will be unlocked in 3 years;

5% by Proof-of-i/o and will be “mined” up in 3 years;

15% of it will pre-A fund raising;

25% of it will be used for community build-up, bug bounty, code audit, hackathon, etc.

Team Member

Neo MA (Founder , CEO/CTO)

Technical geek, graduated from Zhejiang University and Fudan University. Used to work in F500 such as GE, etc. 15yr+ industrial MP experience and 20yr+ applied crypto experience. 2nd prize award in Smart Terminal Category of Wanxiang Smart City Global Blockchain Challenge. Rich experience in leading smart hardware solutions building for start-ups.

Esther ZHANG (Co-founder , COO)

Graduated from Tongji University. Owned 10yr+ Marketing/Sales experience at IBM and Cisco. Joined Wanxiang Blockchain in 2016 as BDM for Chainbase accelerator expansion.

Bo Zhang (Chief Architect)

Famous cryto guru, graduated from Huazhong University of Science and Technology, used to work in Huawei, Nsfocus and 360. More than 20 years applied cryptography experience, good at C / C ++, proficient in the application of cryptography-related technology. Chief board master of Kanxue forum known as **Blowfish**.

Chen Gang (Sr. C++ Developer)

Technical expert, graduated from East China Normal University in CS. Served in HP for 10+ years, working on enterprise applications. Having almost 20yr+ experience in software engineering.

LGX (Sr. C++ Developer)

Famous "white hat", who has 20yr experience in cyber counter-strike. Nsfocus' early member, used to work for a very big cyber-security company as the chief architect. Expert in GNU/Linux, TCP/IP. Good at high reliability and high availability system building. Creator of very famous anti-DDoS solution for a "giant" internet company.