DRAFT VERSION 0.6.0
AnyLedger: Embedded wallet for decentralized IoT

Bogdan Djukic, Lorenzo Pieri

bogdan@anyledger.io, lorenzo@anyledger.io

HTTP://ANYLEDGER.IO

ABSTRACT: We introduce an open source programmable embedded wallet which connects the physical world to the blockchain. Every physical asset will be able to exchange value and interact with smart contracts. This novel capability is provided by a platform composed of an embedded wallet, a broker and a wallet fleet manager. Once connected to a sensor or to an existing IoT device, the embedded wallet is able to communicate to the broker which acts as a bridge to a specific blockchain ecosystem. With the growing number of IoT devices which now can become individual wallets, there will be need for wallet fleet orchestration. The wallet fleet manager delivers end-to-end decentralized IoT wallet fleet orchestration which eliminates the need for centralized trust brokers.

Contents

1 Introduction

The Internet of Things (IoT) represents an extension of the Internet to everyday objects, in which digital and physical world are deeply merged together. In the realm of IoT, we include entities as industrial machinery, electronic appliances, wireless sensors, cars, transport systems, wearables, smart meters or any other everyday object with enhanced digital capabilities ([1], [2], [3]). The exponential growth of the IoT will lead to more than 20 billion devices being connected to the Internet by 2020 [4], while long term prediction is that we will see more than 100 billion IoT devices by 2050 [5]. During this expansion period, there is another major technological trend that will emerge: blockchain.

Blockchain is a data structure composed of a series of transaction groupings called blocks [6]. These groupings are linked together in a simple line or a chain topology. Each block has a parent and a child to which it is cryptographically linked. Blockchains are truly remarkable and novel concepts since they achieve decentralized consensus on which new block will be added at the end of the current chain. Substantially, a blockchain is a tamper-proof peer-to-peer ledger which is removing the need for different actors to trust each other, since trust is embedded in the data structure itself. Once a block is added, it is computationally infeasible and financially not viable to alter the state of the blockchain. The security is inherited from applying state of the art cryptographic algorithms.

The role of a wallet for blockchain is analogous to a physical wallet which stores banknotes. In case of the blockchain, a wallet represents a digital entity which does not directly contain value but rather gives access to funds to the owner of the private key.

In summary, blockchain is the concrete implementation of the decentralized trust. It is more than just a mathematical data structure based on public-private key cryptography, it is a complete paradigm shift in how people can communicate and transact with each other. There is no more need for trusted third parties or intermediaries anymore. Furthermore, the whole history of every transaction is fully transparent.

When combining the decentralized software (blockchain) with the decentralized hardware (IoT), we are able to have a glimpse on how the future will be: fair, automated and peer-to-peer.

1.1 IoT and Blockchain need each other

The Increasing presence of IoT will have a great impact on our daily lives, but to unleash its full potential many challenges must be solved [7]. For instance, it is estimated that 70% of the IoT devices have security vulnerabilities [8]. The crucial point is that IoT devices are generically constrained in power and memory, therefore they are forced to run lightweight encryption algorithms and to lower security standard if they want to stay also affordable. One of the best candidates to address security challenges is the blockchain. Fundamentally, the blockchain solves an identity problem. How to be confident that the party that is being transacting to is who it claims to be and has the claimed resources? While in Bitcoin case, this question can be identified with the double spending problem, for IoT devices it is about device permissions, cybersecurity and data access control. Concrete examples of malicious exploits are masquerading attacks, man-in-the-middle, replay attack,

Denial-of-Service, clone-ID and Sybil attack [2]. In a world full of sensors talking to each other, how can a single sensor be sure that the other party is legitimate?

Current IoT solutions have centralized access control. For instance, remote device management of IoT devices in a smart home scenarios is currently done by a third party centralized trust broker. The issue with IoT centralization is twofold: firstly the presence of a trusted third party and of privileged nodes constitutes a single source of failure within the ecosystem. Secondly the system is not scalable, since a single cloud platform creates a bottleneck limiting the maximum number of connected devices.

The blockchain has the potential to decentralize the whole IoT infrastructure which will result in improving connectivity and speed and creating a secure peer-to-peer IoT network. Security is perhaps the most crucial benefit of the blockchain, since it eliminates man-in-the-middle attacks and spoofing. Notice that to achieve this security level a deep integration at the hardware level is required. That is indeed the approach that we introduce with AnyLedger, as it will be explained later.

While it may not sound obvious, for blockchain to be connected to the physical world, we need reliable and secure IoT. A prototypical good use case of the blockchain is in the supply chain: goods are shipped over very long distances, with different means of transport and many different actors that do not necessarily trust each other. While the benefits of a shared ledger for the supply chain are clear, who is exactly going to put the correct information inside the blockchain? We should not rely on human intervention, since this would defy the purpose of a trustless environment. Therefore IoT devices must be resilient and tamper-proof as much as the blockchain, in order to reliably store data on the blockchain.

1.2 IoT Blockchains and What is Missing

Blockchain space is moving very fast and there are already planned or semi functioning solutions for applying blockchain in IoT. The desirable features of a blockchain based IoT are low latency, low fees and minimal energy requirements for nodes, even though this last property is not crucial, since nodes can be hosted remotely, outside of the IoT devices themselves.

Solutions built purposely for the IoT include IOTA [9], IOTEX [10], IoT Chain [11] and HDAC [12]. The main promised innovations consist in a lightweight consensus algorithm, allowing power constrained devices to become nodes with fast confirmation times and low fees.

Other promising scaling solutions are Lightning Network based implementation for Bitcoin and other cryptocurrencies [13]. These are additional off-chain layers on top of the blockchain (Layer 2 solutions), which allow close-to-zero fees transactions and low latency bi-directional channels between nodes.

Therefore, what is missing? These projects are exciting and highly promising, but they rely on hardware and software infrastructure that has not been builded yet. AnyLedger builds exactly such infrastructure layer.

1.3 Executive Summary

We introduce a programmable embedded wallet which connects the physical world to blockchain. Physical assets will be able to execute financial transactions and interact with smart contracts. IoT devices using AnyLedger technology can generate public blockchain addresses, sign and verify transactions.

AnyLedger platform is composed from hardware and software stack. The core of the platform is the firmware of the embedded wallet, which will be compatible with a great number of hardware IoT devices already existing on the market. In line with our vision of spreading the usage of blockchain technology for the benefit of everyone and making sure that our platform aligns with highest security standards, the complete embedded wallet implementation will be open sourced.

AnyLedger embedded wallet employs the highest standards of security, such as Trusted Execution Environment (TEE), Secure Boot and encrypted connectivity. The firmware, which is purposely built to leverage the hardware and software security of TEE, safely generates and manipulates private-public key pairs. It represents a collection of lightweight wallets with minimal impact on memory and battery footprint and exposes all basic blockchain functionalities. A thin broker, called AnyLedger Hub, connects the IoT devices to the blockchain, exposing it to full node capabilities. The Energy (ENE) token powers every single device, additionally adding another layer of security. Only devices with ENE token sent by AnyLedger Hub are authenticated as trustworthy and benefit from access to AnyLedger Hub capabilities according to the token balance.

The last piece is the wallet fleet manager, which allows customized orchestration of the wallet fleets.

AnyLedger platform is blockchain agnostic, it will be able to support any implementation on the market, both public (for instance Ethereum, Bitcoin or Stellar) and private (for example HyperLedger [14]).

Given the flexibility of over-the-air AnyLedger firmware update capabilities, any blockchain innovation can be just encapsulated in a firmware update and deployed on a global network of sensors.

1.4 Our Vision

AnyLedger delivers a bridge between the complexity of the physical world and the immutability of blockchain. Our mission is to build an affordable, flexible and powerful add-on for every IoT device. To do so, we are proposing a cutting-edge hardware that is compatible with large number of IoT devices and a software stack that is blockchain agnostic.

This solution is ready for the upcoming future in which:

- devices are everywhere, small and low powered.
- IoT devices are uniquely identifiable, resilient and stable, while allowing instant and remote feature or security modifications.

- IoT devices are acting autonomously in a distributed architecture thanks to smart contracts.

For the existing markets, we see at least four different waves of innovations that AnyLedger can empower in the near future:

- Supply Chain and Logistics

  Blockchain can be used in the supply chain industry and logistic, particularly for international trades. Smart sensors running AnyLedger would be able to automatically record the entire history of every shipment on the blockchain and execute Smart Contract that sender and receiver agreed upon at the beginning of the shipment. Logistic companies can choose to be automatically paid with currency put in escrow inside a Smart Contract and unlocked after confirmation of delivery. In exchange, they attract new customers and get discounted tariffs from insurance companies. Goods would be monitored from the production plants to the small shops, giving a complete history (provenance) of the product to the end customer.

- Payment Systems and Sharing economy

  Enabling payments for every physical object will create new business models. Imagine decentralized marketplaces in which sensor owners are getting paid to share their collected data or objects paying fees just once entering geo-fenced areas. These technologies will also bring the sharing economy to new levels. Bikes and cars will become available to be shared everywhere inside the city, industrial machinery and tools such as 3D printers and construction equipment will be rented according to the time usage. Previously, the sharing economy was powered by centralized solutions big enough to build their own payment networks. The future sharing economy will use a peer-to-peer model since it will become easy to for objects to exchange financial value.

- Machine-to-machine communication

  Fast machine-to-machine communication allows easy sharing of data and value for interactive applications. Electricity can be distributed by smart grids and be able to create a dynamic decentralized marketplaces between energy producer and consumers. Self-driving cars will communicate securely between each other and would be able to automatically pay tolls, parking and fuel. Smart traffic systems will be enabled to decrease the traffic real time by incentivizing cars to run across roads with less pollution, traffic and noise. Smart factories, also known as Industry 4.0, and smart homes will be finally a reality.

- IoT Security

  Some connected devices require very high standard of security, either because they are very expensive, potentially dangerous or life-critical. Examples are industrial machinery and medical devices. AnyLedger leverages the blockchain to assure firmware

integrity, device authentication, tamper proof over-the-air updates and device lifecycle management.

Another interesting opportunity is the birth of a truly decentralized IoT. We can imagine IoT devices autonomously paying the computing power and memory storage that remote cloud-services, connected themselves trough the blockchain, can remotely offer. Interesting projects in this direction are Golem [15] and Filecoin [16].

Finally, it is worth remembering that the majority of world physical assets, worth hundreds of trillion dollars, are not tradable right now. The blockchain could allow the tokenization of all these assets, allowing seamless exchange of value and goods, without the need of a trusted third party. This usage will be particularly powerful in areas like real estate and art.

The most exciting applications of AnyLedger are the ones that we cannot even fully grasp at moment. The AnyLedger embedded wallet will be built to be open source and we are confident that the community of developers and makers will figure out the next big thing.

2 General Architecture

The structure of the remaining part of the document will be as follows. First of all, we will cover the general architecture of AnyLedger. Then, we will outline the hardware specifications of AnyLedger embedded wallet. Following that section, the concept of AnyLedger Hub will be explained in more details.

Security is a transversal topic that will be touched in all the sections. This is indeed a signature feature of AnyLedger. Security is built-in from the ground up in both hardware and software layers. AnyLedger will be reusing tried and tested security models rather than developing new designs and thus increasing the potential attack vectors. We are committed to carry out scheduled penetration testing for our software and hardware stacks.

2.1 AnyLedger One

AnyLedger One is an open source programmable embedded wallet. Once an IoT device is integrated with AnyLedger One and it starts using dedicated SDK, it will get all the benefits of decentralization and distributed ledger technologies. In particular, AnyLedger One exposes IoT devices to smart contracts and an ability to execute value transactions. To be able to connect to the blockchain, a device must contain AnyLedger One firmware, which must be installed on a compatible secure hardware component. There are two possible routes for using the firmware:

1. Using AnyLedger One, a secure hardware component built directly from AnyLedger on which is installed the firmware. IoT companies can insert the AnyLedger One in their devices.

2. Install the firmware on a hardware component satisfying the specifications detailed in the next sections. AnyLedger is committed to be compatible with the highest number of existing devices, in order to spread the diffusion of AnyLedger Hub.

In summary, AnyLedger firmware is a software add-on that can be flashed together with the main application code provided by the client. The platform exposes all the cryptographic functions necessary to make the main code secure regarding interactions with external devices, blockchains and servers. Critical points like device onboarding and device update are also hardened. The end result is a resilient, decentralized and flexible IoT infrastructure.

AnyLedger One is the first of a series of models that will be offered by AnyLedger. We generically refer to them as AnyLedger wallets, meaning firmware plus compatible hardware.

AnyLedger Hub comprises a broker which allows the communication of the device with the blockchain and a wallet fleet manager. More in detail, the broker exposes all necessary APIs for communication with specific blockchain stack and represents a secure bridge from IoT device and targeted blockchain node. This broker is crucial, since it allows the platform to outsource demanding tasks from the IoT devices to the cloud or remote blockchain nodes.

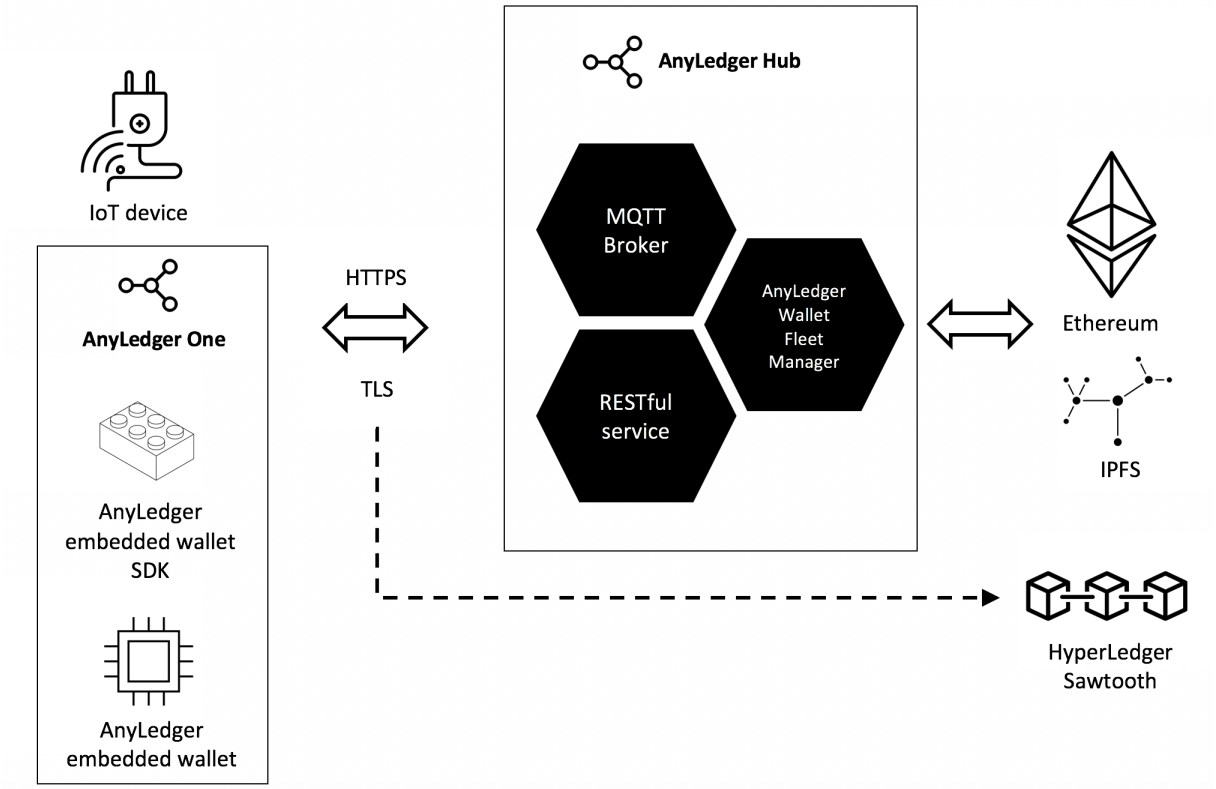

Figure 1. AnyLedger general architecture. The IoT device using AnyLedger firmware is able to interact with the blockchain.

In its initial phase, AnyLedger embedded wallet will be supporting Ethereum, ERC20 tokens and HyperLedger blockchain projects. Subsequent implementation will include Stellar, due to its low transaction fees which makes it an interesting candidate for financial exchange scenarios between IoT devices, Bitcoin and IoT blockchains.

Some companies maybe not willing to use the full services of AnyLedger Hub for instance for privacy reasons. In this scenario, as shown in figure 1 using HyperLedger as an example, AnyLedger wallet will interact directly with the RESTful service provided by the private blockchain implementation.

AnyLedger uses the ENE token to power up all devices using the AnyLedger firmware. As explained more in detail in section 6, the functionalities of the ENE token include authentication and access to premium services inside AnyLedger Hub.

In order to provide a scalable and decentralized storage solution, AnyLedger Hub will be exposing Interplanetary File System (IPFS) end points. Again, companies more worried about privacy may want to use a private cloud server at this point.

A typical company using IoT sensors is expected to maintain a large number of devices. AnyLedger wallet manager offers complete real time control over the IoT fleet through a web and a mobile interface. Users can remotely browse the status of their devices, the balances, analytics and perform actions that will be described later in more detail.

3 Hardware and Firmware

3.1 Hardware Architecture

This section of the white paper will cover AnyLedgers hardware architecture in more details. Security challenges in IoT environment have two dimensions. One is securing the IoT devices against attacks directed at the organization or its owner. The other dimension is protecting against unauthorized use of the device itself. This section will cover the latter part.

During the architecture design phase, we have identified three possible paths one can take in designing an embedded wallet:

1. Single microcontroller unit (MCU). This is the approach taken by Trezor hardware wallet [31]. It has the lowest level of security compared to the other ones since its architecture is based on a single general purpose MCU. This results in a wide hardware-based attack surface.

2. MCU with Trusted Execution Environment (TEE) support. The benefits of TEE are described in more details in the section down below. TEE gives a very advanced security model and it is especially designed to target mobile and IoT devices. On the other hand, targeted attacks on TEE based MCUs which is done in specialized laboratories will result in a compromised security.

3. MCU with Secure Element (ARMs SecurCore technology [32]). Hardware wallets coming from Ledger are based on this architecture [33]. The wallet functionality is divided between general purpose MCU and a dedicated crypto chip (Secure Element). Vulnerabilities are not very common but there is the additional cost of an extra chip.

AnyLedger will balance between the level of security being offered and the overall cost of the hardware platform. That is why we have chosen second option. We believe this will satisfy most of the use cases from our potential users.

3.2 Hardware platform

Fundamentally, we consider AnyLedger to be a software organization. In order to deliver our services to a broader set of developers, we will be using hardware as a delivery vehicle and as a way to speed up the early adoption. For instance, in one of the early prototypes, AnyLedger already used Particle Photon as a references board, while in the future AnyLedger will deliver a programmable embedded (hardware) wallet based on nRF52840 [34] system-on-a-chip (SoC) product from Nordic Semiconductors[1].

[1]The latter SoC design will give our embedded wallet a powerful 32-bit ARM Cortex-M4F [35](with TrustZone capabilities for trusted execution [36]). Built-in cryptographic hardware accelerator (Cryptocell-310 [37]) brings security model built from the ground up with support for cryptographics libraries, key management and secure boot.

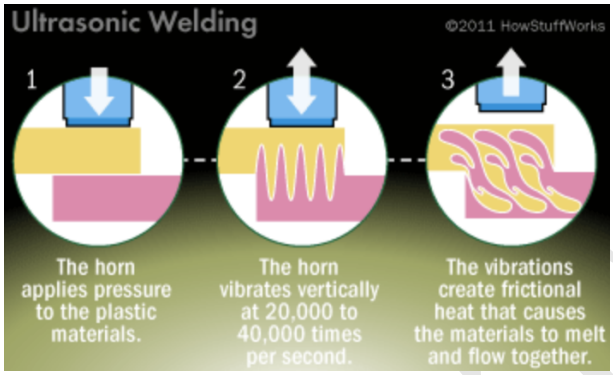

Figure 2. Ultrasonic Welding procedure. Source: HowStuffWorks [38]

3.2.1 Secure Casing

In order to increase the level of security of our embedded wallet in the scenario of physical exposure, we will apply the process of plastic ultrasonic welding around nRF52840.

This procedure brings tamperproof hermetic plastic seals and waterproof capabilities to the embedded wallet, making it more robust for outdoors use cases.

3.3 Secure Boot

AnyLedger hardware stack is relying on ARMs TrustZone Secure Boot feature which is critical to device integrity throughout its lifecycle. Secure Boot is a mechanism to build and maintain a complete chain of trust for the whole software stack running on the embedded system. It is based on the concept of firmware fingerprinting. In particular, Secure Boot prevents malicious code from loading and running by authenticating all firmware images.

AnyLedger embedded wallet SDK will notify subscribers with an event in case boot sequence has been compromised.

3.4 Trusted Execution Environment

Trusted Execution Environment (TEE) is an emerging standard for the security of mobile and IoT devices. It represents a secure and trusted component of the processing unit and lowers the possibility of dictionary and side-chain attacks [17]. TEE is an isolated/safe area of processing unit which guarantees confidentiality and integrity for the code and data loaded into it. Embedded processing unit which supports TEE is split into two parts: Rich Execution Environment (REE) and Trusted Execution Environment (TEE).

REE enables applications to be ran under the control of operating system from the embedded device. TEE exists as a separate and isolated space on the processing unit which is running Trusted Apps (TAs). TEE runs in parallel with the REE, but it has exclusive access to the underlying secure hardware and provides trusted processing. TEE exposes a set of strictly controlled APIs in order to communicate with untrusted REE. A concept of shared memory (which is inherently untrusted since it resides on REE) is used to share

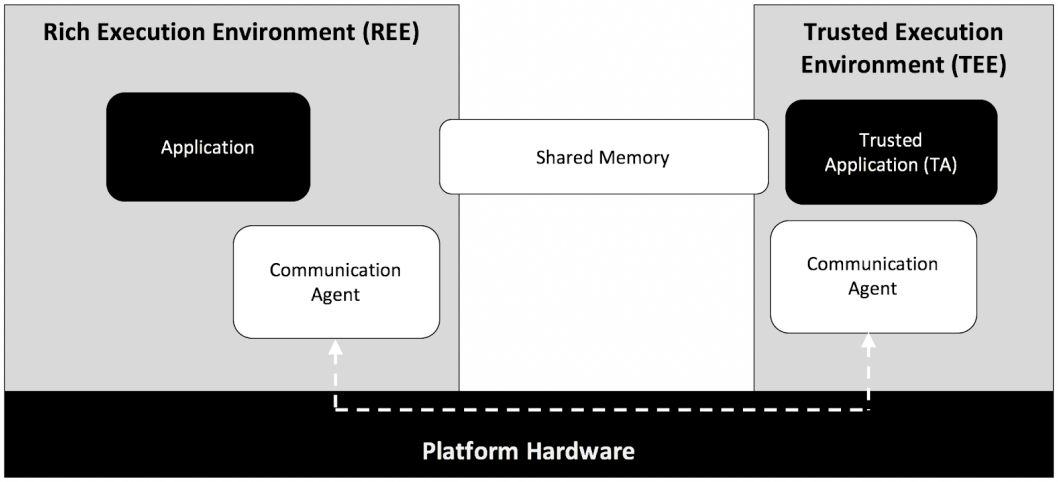

Figure 3. Trusted Execution Environment architecture

the data between REE and TEE. Sensitive data is available only from the safe zone (TEE) and protected from the outside world (REE).

TEE takes a critical role in the Secure Boot process since it is loaded after ROM and it is capable to verify the content of REE before it is loaded.

In the context of AnyLedger embedded wallet, TrustZone will be used for private key generation, private key storage and transaction signing. It is essential that the AnyLedger TA remains with the small footprint in order to lower the risk of potential security critical bugs and make source code auditing more straightforward. We will put additional effort in making AnyLedger wallet platform independent and not force developers to use our reference platform. Therefore, special focus will be put on abstracting the Random Number Generator component, cryptographic algorithms and networking stack which will be platform specific.

3.5 Private key, Public key and Address

Private-public key cryptography is the main security concept behind blockchain. The private key gives its owner access to the funds and an ability to sign transactions. AnyLedger makes sure that private key is only accessible to the embedded wallet. The private key is created the first time once the embedded wallet is powered up. The private key is 256 bit long non-deterministic number (in the case of Ethereum and HyperLedger Sawtooth). True Random Number Generator (TRNG) will be used for generating this long number. TRNG will be supported by underlying hardware platform (nRF52840). The private key will not be directly accessible to the IoT device which integrates AnyLedger embedded wallet: once generated, the private key is not exposed to the embedded wallet SDK but rather kept as a secret in TEE, or rather AnyLedgers Trusted App (TA). The private key has two main purposes. First one is to sign transaction payload which can be then verified that it came from the original sender. Second one is to generate an address which uniquely defines IoT

Figure 4. Private key, Public key, Address creation procedure

device and can be used in Smart Contract interactions and financial value exchanges.

Transaction signing capabilities and unique address will be exposed through the embedded wallet SDK. Private key, public key and address generation will happen in TEE as a part of AnyLedger TA. TA will also be responsible for handling transaction signing and as a result it will be returning encoded payload. This encoded payload will be then broadcasted to dedicated blockchain network through AnyLedger Hub or directly to HyperLedger Sawtooth (since it is private blockchain deployment).

Notice that previous implementations and proof of concept of blockchain in IoT where at the two extreme: either they were using "full nodes" on the IoT devices or they were completely outsourcing the key generation to remote nodes, while the IoT devices where just collecting and sending data. The first approach can be applied only to very powerful devices, that is the great minority of the whole IoT landscape. The second approach is not secure. AnyLedger approach is both secure and low power footprint, since it just signs the transaction on the device itself and the private keys never leave the TEE.

3.6 Secure Access

Transaction signing and related embedded wallet functionality will only be accessible if IoT device authenticates itself successfully against AnyLedger embedded wallet SDK.

3.7 Other Firmware Specs and Features

Additionally to the blockchain and security functions explained above and in section 5, the fimware leverages state of the art functionalities based on the LWM2M layer for device management. Explicitly, the firmware is a Real Time Operating System (RTOS) able to run on very low powered devices and with capabilities such as Firmware Updates over-the-air (FOTA) and device lifecyle managment.

4 AnyLedger Hub

Given the power and space constraints of microcontrollers today, it is infeasible to run blockchain full nodes on embedded devices. This is due to the requirements for the full nodes to usually (depending on the underlying blockchain implementation) keep the complete transactional history and execute Proof-of-work.

This is why our hardware device is only focused on the lightweight wallet capabilities, whilst the heavy work is done remotely. In order to enable broadcasting of signed transactions from embedded wallet to the specific blockchain network, we will be offering a broker service (AnyLedger Hub). As already described in general architecture, we are introducing novel approach of exposing different blockchain endpoints through MQTT (widely used industry standard for machine-to-machine communication). MQTT is offering a very lightweight (compared to HTTP) publish/subscribe protocol whose channels will be secured through TLS. Transactions signed by the embedded wallet on IoT device will be therefore transported as payload of MQTT message and further down broadcasted to targeted blockchain network. Similarly, for more powerful IoT endpoints AnyLedger Hub will be exposing HTTPS based RESTful service which has same same broker responsibilities as MQTT. In order to support a broader range of IoT devices, we will be considering the support for other communication protocols like CoAP in the future.

A common misconception is that blockchain is not suited for IoT applications since it cannot deal with the huge amount of data generated by billions of devices. Actually raw data is not stored on the blockchain, what is stored is just an address (a hash) linking to the data. In order to support our vision for decentralized nature of IoT devices, AnyLedger Hub will be exposing Interplanetary File System (IPFS) node through MQTT endpoint. This will enable IoT devices to store any kind of data (i.e. sensor data) in distributed and decentralized fashion. Data stored on IPFS will be encrypted by default. If we look at blockchain as a truth machine and embedded wallet as a root of trust, combining embedded wallet and IPFS will deliver unique way to guarantee authentication and integrity of the data coming from specific IoT device or a sensor.

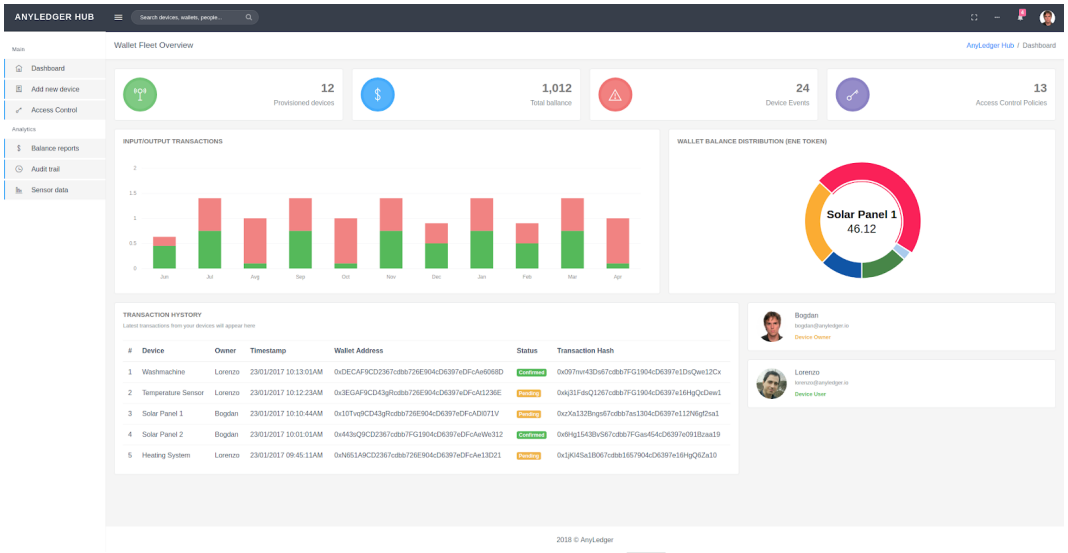

Figure 5. AnyLedger Wallet Fleet Manager dashboard

5 AnyLedger Wallet Fleet Manager

With the growing number of IoT devices around us and with AnyLedger empowering them to become individual wallets, there will be an increasing need for managing multiple wallets for households, factories or governmental agencies (institutions). AnyLedger Wallet Fleet Manager is part of AnyLedger Hub general architecture and it is responsible for orchestrating multiple wallets. In the next sections we will go over its basic functionalities.

5.0.1 Provisioning new IoT device

Once AnyLedger One gets physically attached to the targeted IoT device, in order to expose it to the blockchain infrastructure, it needs to go through the process of provisioning (onboarding). This process of adding new IoT device coupled with AnyLedger One to AnyLedger ecosystem is done using AnyLedger Wallet Fleet Manager. The provisioning process itself will be done using the AnyLedger One SDK and involves the usage of the ENE token.

5.0.2 Wallet Management

The newly provisioned IoT device will have a specific amount of ENE token being assigned after the onboarding process is completed. Additional amounts of ENE token can be added by the wallet top-up functionality.

5.0.3 Distributed IoT device management

AnyLedger Wallet Fleet Manager enables owners to define a specialized configuration mappings which can be used for enabling/disabling features on targeted IoT devices. This capability of distributed device management can be used also to initiate remote data wipings and disconnecting of IoT devices in scenario of theft or malfunctioning.

In order to keep the existing wallets on AnyLedger One up-to-date with the latest security updates, owners will be able to kick off authenticated firmware updates for their wallets. Furthermore, additional wallets can be deployed from the same place.

5.0.4 Distributed Access Control for IoT

Access control today faces big challenges in IoT. Delegating access control logic to a third party creates a security risk and requires strong trust relationship between the parties involved. Therefore, we strongly believe that IoT devices need a decentralized access control model which fits to distributed nature of IoT devices themselves [18–22]. We propose an IoT access control framework based on blockchain.

Once provisioned, the IoT device will be assigned with a single owner or multiple owners, depending on the use case. When defining additional ownership of the IoT device, the original owner is able to define different access control levels for IoT device resources/data. These access control rules represent entitlements between a specific user and resources/data published by IoT device. Enabling IoT devices to be able to interact with entitlements given by access control procedure opens some interesting scenarios. For example, the IoT device would be able to request entitlements for another IoT device or even go through the delegation process where it could obtain necessary access through a third party (another IoT device or a user from AnyLedger Hub).

5.0.5 Wallet Fleet Analytics

AnyLedger Wallet Fleet Manager is offering analytics capabilities in order to simplify the process of orchestrating a large number of wallets. It provides an overview for wallet balances, device ownership, transaction history, basic sensor data analytics, AnyLedger One firmware update audit history, role and region groupings.

5.0.6 Multisignature embedded wallet

In order to deliver an additional layer of security, AnyLedger will combine physical security of embedded wallet with the resilience of multisignature to offer the highest level of security for IoT devices. AnyLedger Wallet Manager will have an option to create a multisignature wallet for IoT device with the device owner(s) and optionally to any trusted party.

Multisignature transactions, also known as M-to-N transactions, require the signature of at least M parties out of N possible signers to be broadcasted to the blockchain. In this language, a normal transaction is a 1-to-1 transaction. Multisignature wallets, that is wallets supporting multisignature transactions, are more secure than traditional wallets since they delocalize the private key storage to multiple owners. One can argue that this is the ultimate security measure, superior even to single signature hardware security itself, since now a malicious attacker must steal multiple private keys.

Bitcoin offers multisignature in its core implementation ([23],[24]), and indeed the technology has a very good track record since very few incidents and hacks were reported. In Ethereum, multisignature can be implemented as a Smart Contract, even though there is no standard yet [25]. There are several open source implementations (Grid+ [26], Gnosis [27] or from individual developers [28]) which have stood the test of time. AnyLedger will

be looking up to these open source implementations in order to deliver robust and secure multisignature scenarios.

Multisignature will have a capability to be parametrized in such way that IoT device could behave more as an autonomous economic actor. This involves setting a threshold spending limit below which IoT device can sign and execute value transactions without owners approval.

6 Token Economics

AnyLedger platform is supported by the Energy Token (ENE). The ENE token acts as a simple access control mechanism and is needed to enjoy the full functionalities of the AnyLedger platform. In particular, every IoT device can be in different states according to the amount of ENE sent to the device. The token is designed with the intent of aligning the interest of token holders and users of the platform, in line with the principles of mechanism design [29, 30]. More details will be found soon in the companion Business white paper.

References

[1] Qusay F. Hassan, Atta ur Rehman Khan, Sajjad A. Madani, *Internet of Things: Challenges, Advances, and Applications*

[2] Rajkumar Buyya, Amir Vahid Dastjerdi, *Internet of Things Principles and Paradigms*

[3] Sabina Jeschke Christian Brecher Houbing Song Danda B. Rawat, *Industrial Internet of Things*

[4] Gartner 2017, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, https://www.gartner.com/newsroom/id/3598917

[5] https://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf

[6] Andreas M. Antonopoulos, *Mastering Bitcoin*

[7] Nitesh Dhanjani, *Abusing the Internet of Things Blackouts, Freakouts, and Stakeouts*

[8] http://www8.hp.com/h20195/v2/getpdf.aspx/4aa5-4759enw. pdf

[9] https://iota.org/

[10] https://iotex.io/

[11] https://iotchain.io/

[12] https://hdac.io/

[13] https://lightning.network/

[14] https://www.hyperledger.org/

[15] https://golem.network/

[16] https://filecoin.io/

[17] https://fenix.tecnico.ulisboa.pt/downloadFile/1689244997256880/Thesis.pdf

[18] Ouaddah, Aafaf and Elkalam, Anas Abou and Ouahman, Abdellah Ait, *Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT*

[19] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Jianxiong Wan, *Smart Contract-Based Access Control for the Internet of Things*

[20] Aafaf Ouaddah Anas Abou Elkalam Abdellah Ait Ouahman, *FairAccess: a new Blockchain based access control framework for the Internet of Things*

[21] Aafaf Ouaddah Anas Abou Elkalam Abdellah Ait Ouahman, *Harnessing the power of blockchain technology to solve IoT security and privacy issues*

[22] Oscar Novo, *Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT*

[23] https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

[24] https://github.com/bitcoin/bips/blob/master/bip-0017.mediawiki

[25] https://github.com/ethereum/EIPs/issues/763

[26] https://blog.gridplus.io/toward-an-ethereum-multisig-standard-c566c7b7a3f6

[27] https://github.com/gnosis/MultiSigWallet/blob/master/contracts/MultiSigWallet.sol

[28] https://github.com/christianlundkvist/simple-multisig

[29] http://complexitylabs.io/token-economics-book/

[30] Y. Narahari, *Game Theory And Mechanism Design*

[31] https://trezor.io/

[32] https://www.arm.com/products/processors/securcore

[33] https://www.ledgerwallet.com/

[34] https://www.nordicsemi.com/eng/Products/nRF52840/(language)/eng-GB

[35] https://developer.arm.com/products/processors/cortex-m/cortex-m4

[36] https://www.arm.com/products/security-on-arm/trustzone

[37] https://www.nordicsemi.com/eng/Products/ARM-CryptoCell-310

[38] https://science.howstuffworks.com/ultrasonic-welding2.htm