RISC-V

RISC-V Blockchain Special Interest Group

Trusted RISC-V Architecture in Blockchain Infrastructure

White Paper

Release 1.0 Jan. 10th 2023

Table of Contents

Section I: Introduction to Blockchain

1.1 Blockchain Overview

Blockchain technology has been the center of world's attention for a while. As one of the fastest developing technologies, it penetrated every field of human life, innovatively integrated with other industries. Nowadays, cross-innovation happens between blockchain and other technologies such as internet of things, big data, cloud computing, artificial intelligence and 5G, etc. The "blockchain +" is becoming a promising trend in the real economy.

Blockchain technology is a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. It has specific features such as permanent tamper-free data records, establish automated execution of prior agreement with set conditions, data accessible but not replicable, data protection across domains and easily establish network of the willing without heavy IT and legal costs, which allow it to work in many industries other than finance transactions. Blockchain technology is a disruptive innovation, it gave us a new trust based problem-solving and cost-reducing solution.

Recent years, thanks to the cross-innovation, blockchain is speeding up its application in many areas, in order to improve efficiency, to tackle new challenges, to realize new business value streams, and etc. In Metaverse, every participator, including human and device, will collaborate deeply with next-generation identity, which is supported by Decentralized Identity (DID)/Verifiable Claims. Blockchain technology helps to securely verify every participator's identity and claims, and still ensure sensitive information not being mis-used. In industry like manufacturing and logistics. There are outstandingly successful using cases in digital equity, public welfare, healthcare, industrial internet, supply chain management, digital economy, and digital media, from where we can see a great potential in blockchain application.

1.2 Blockchain Infrastructure with RISC-V

Blockchain is a new mode of application that innovatively integrating and utilizing peer-to-peer network, cryptography, timestamp, Merkle tree, distributed storage, smart contract technologies.

The architecture of blockchain has 9 layers:

- The base installation layer contains the essential operation system and hardware.
- The underlying component layer enforces the recording, verification, and transmission in blockchain system.

- The ledger layer is responsible for data storage in blockchain system.
- The consensus layer keeps the consistency of data recording in all network nodes.
- The smart contract layer ensures the business logic, because of which blockchain system can allow flexible programming and data implementing.
- The interface layer is for packaging the functional modules, it fits all kinds of using cases and services in blockchain.

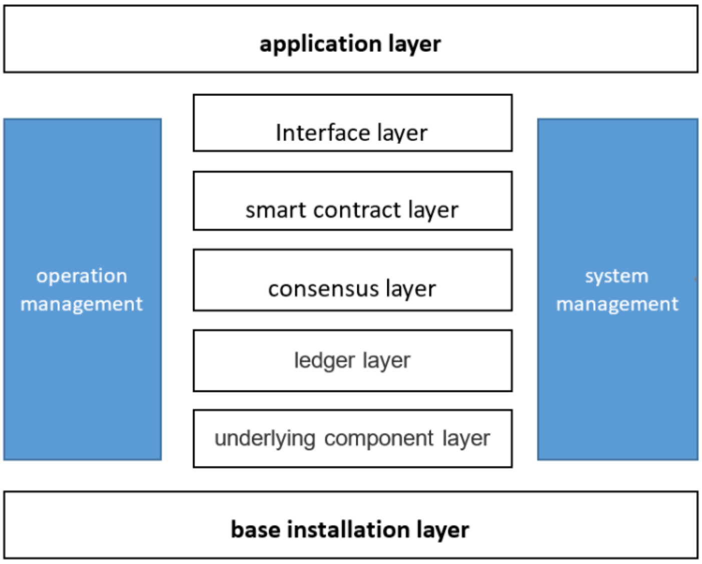


Figure 1 Blockchain Technology Architecture

The base installation of blockchain consists of different kinds of network data processing equipment such as data storage and consensus server, data transmission router and gateway, applying smart contracts computer and smart phone, data collection perceptive devices. Blockchain network consists of several blockchain nodes, can be labelled as full nodes and light nodes. Full nodes records and maintain complete block ledgers and generate new block ledgers according to certain consensus rules, light nodes do not follow the consensus rules, and do not store the complete block ledgers but only the head of the blocks, light nodes only ask for full information at making transactions or search transactions. The devices that have strong computing power, large storage capacity and strong communication capability can all be nodes in blockchain network, ensure data interaction. In many blockchain using cases, internet of things plays a very important role, which is responsible for environment perception and data collection. Some devices have ability limitation that hard to access to the blockchain network directly as nodes, they can only access blockchain through existing nodes.

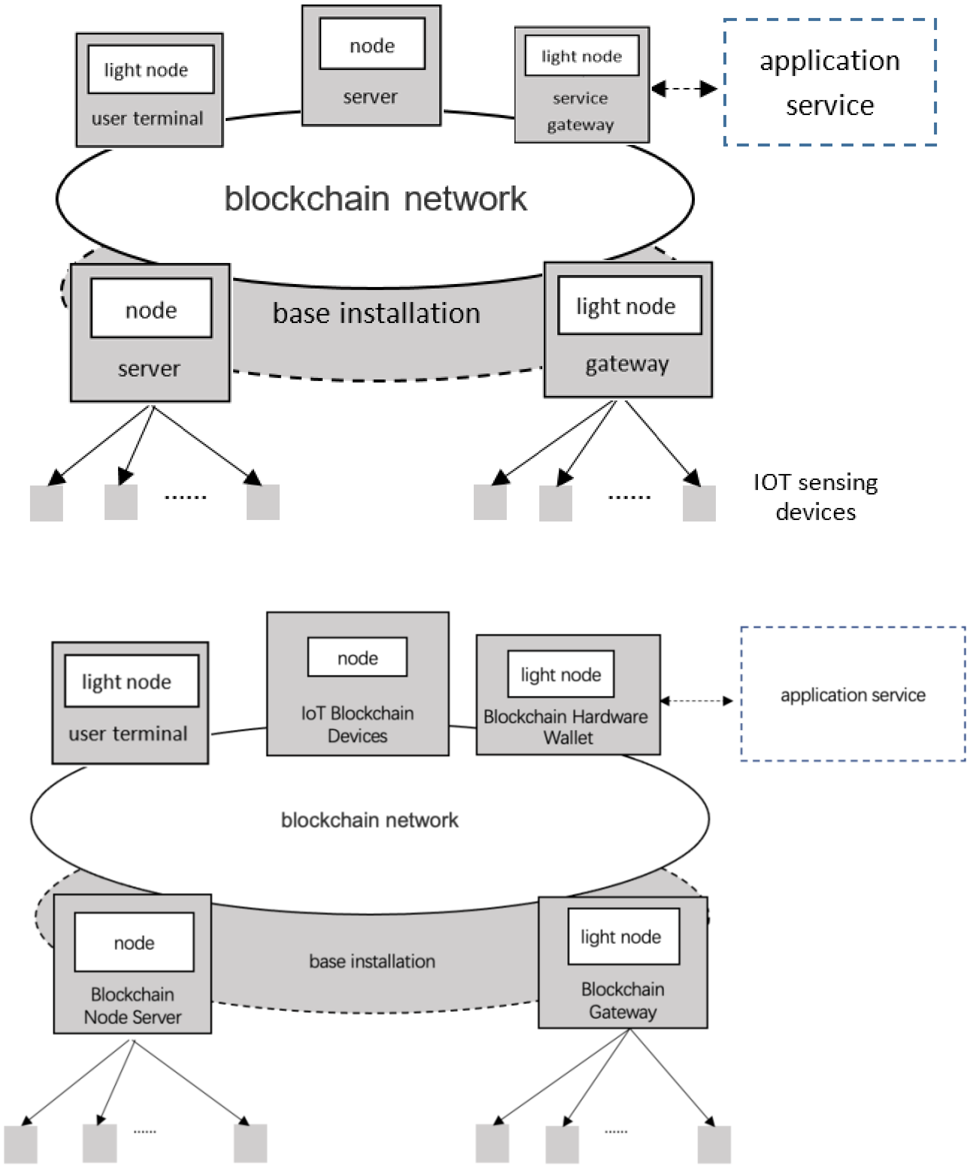


Figure 2 Blockchain Reference Network Architecture

Blockchain technology ensures the data on it are tamper-free, and easy to trace to the source, but it cannot ensure the authenticity of original data. Most of the data comes from all kinds of devices which lead to an important issue is the trustworthiness and security of the devices. The key is to keep a high security of chips. The new CPU architecture RISC-V is open-sourced, modular, and simple, it is wildly used by chip companies and will become the core technology in blockchain base installation. Ensure the security of chips will lead to the success of the original data authenticity.

1.3 Security Challenges

Several key challenges arise to manage securely the distributed ledgers that are tied to the device:

- Securely binding the distributed ledgers to a clearly identified and immutable information throughout the life of the device.

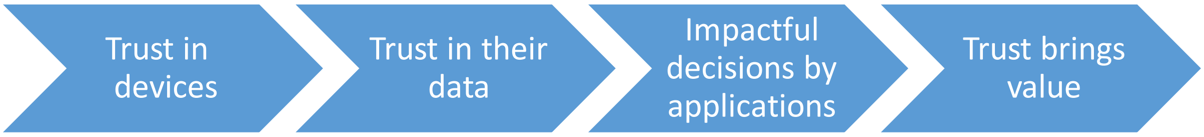
- Ensuring that modifications and additions to the distributed ledgers are only performed by authorized actors.
- Ensuring that the distributed ledgers can only be accessed and read by actors with the appropriate authorizations.
- Integrating the adequate security and cryptography mechanisms to protect the distributed ledgers against cyber-attacks.
- Enabling the required flexibility in the system to allow for the regional and local regulations on privacy and security.
- Enabling the audit of the distributed ledger to verify it as it goes through its lifecycle.

The device industry is characterized by the fragmentation of its target markets, functions, specifications, supply chains etc. So, it is hard to incent the vendor invest on the security design. And the consequences are:

- Most of IoT devices which collect, store, and transmit data to the chain are lack of data protection methods
- The benefits of that cannot be balanced since the countermeasure of security increases the cost of implementation.
- The lack of specialists in security field is a big problem in companies especially for small businesses and startups.

1.4 Objectives and Value Proposition

Blockchain service and applications receive data from the IoT devices. They make decisions impacting the safety of the system and its users. They send instructions to the IoT devices with large potential financial and safety implications. The data plays a key role, and it is fundamental that it is trustworthy. If the data cannot be relied upon, it is not worth much, and in some cases cannot be acted upon. Trust in the data brings value to the systems. Trust in the data is built upon a security architecture that will start with the devices. Trusted devices enable trusted data.



Across the industry, chipmakers, device vendors, and blockchain service providers all see the need of data security improvement. So, the objectives of this article are:

- To define the requirements of security in different blockchain using cases.
- To propose trusted architectures for different RISC-V using cases.
- To reduce the costs of countermeasure of security and the complexity of chip designing through reference designs.
- To get better combinations of security and costs of RISC-V chips in blockchain with IoT field.

Section II: The Cryptographic Algorithms

2.1 The Cryptographic Algorithms of Blockchain

Cryptography is one of the core technologies in blockchain, which empowers blockchain to keep the information anonymous, immutable, and honest, is an indispensably important part of blockchain.

There are many cryptographic algorithms using in blockchain, these are the basic ones:

- **Hash Algorithm**

A hash is a mathematical function takes input of any length and produces a fixed-length encrypted string in a very short time. The hash algorithm is normally used to check data integrity and secure a variety of cryptographic systems and protocols. In blockchain, the most used hash algorithms are SHA, Blake, RipeMD, Keccak256 and SM3.

- **Digital Signature Algorithm**

Digital signature algorithms are widely used in blockchain. The signature is encrypted using the private key and decrypted with the public key. Because the keys are paired, decoding it with the public key verifies that the proper private key was used to sign the document, thereby verifying the signature's provenance. In blockchain the most used digital signature algorithms are Secp256k1, NIST P-256, Ed25519, SM2.

- **Encryption Algorithm**

An encryption algorithm is designed to encode a message or information so that only authorized parties can access data, and data is unreadable by unintended parties. In blockchain the most used encryption algorithms are AES, SM4, mainly to protect private keys.

2.2 The value of hardware chips supporting cryptographic algorithm

Hardware chips supporting cryptographic algorithms can secure application expansion.

Security

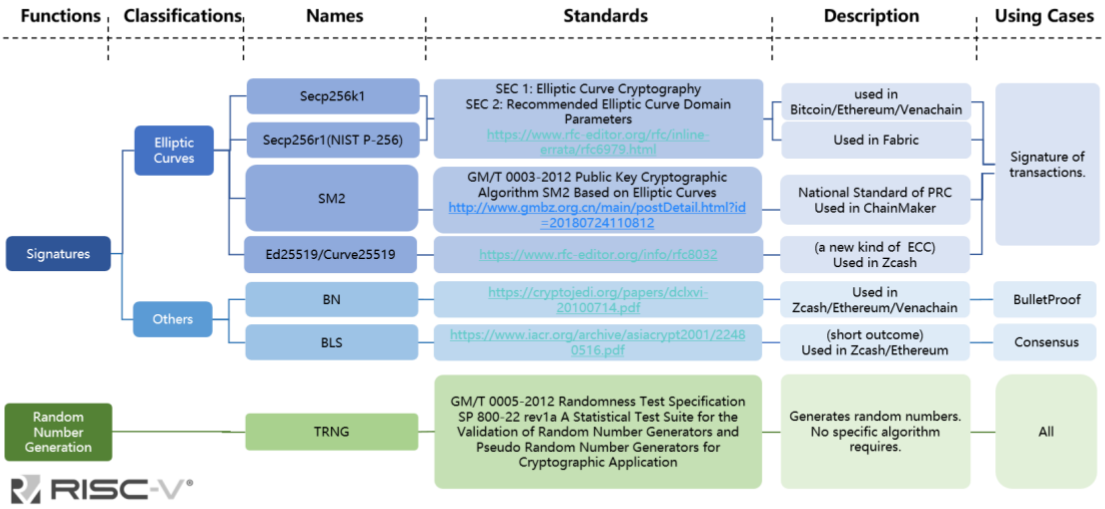
Hardware chips supporting cryptographic algorithm can elevate the level of security. All the data will be encrypted and decrypted inside of hardware chips so that no data will be disclosed. Hardware chips produce true random numbers from inside, greatly reduced the risks of producing pseudo random numbers from the software side.

Performance optimization

Hardware chips supporting cryptographic algorithms can largely improve computing processing performance and code running efficiency, leverage the developing efficiency, reduce the volume of code and CPU, memory and other occupied resources at code running time.

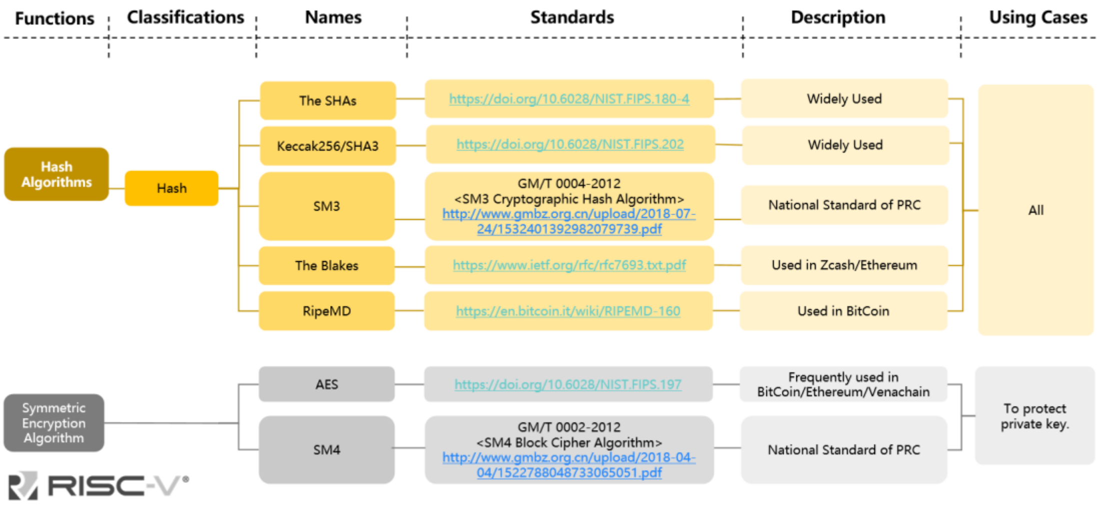
2.3 Supporting cryptographic algorithms

Below are the cryptographic algorithms that we strongly suggest using in hardware chips, to improve computational efficiency, security, and optimization of blockchain applications.



Functions	Classifications	Names	Standards	Description	Using Cases
Signatures	Elliptic Curves	Secp256k1	SEC 1: Elliptic Curve Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters https://www.rfc-editor.org/rfc/inline-errata/rfc6979.html	used in Bitcoin/Ethereum/Venachain	Signature of transactions.
		Secp256r1(NIST P-256)		Used in Fabric	
		SM2	GM/T 0003-2012 Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves http://www.gmbz.org.cn/main/postDetail.html?id=20180724110812	National Standard of PRC Used in ChainMaker	
		Ed25519/Curve25519	https://www.rfc-editor.org/info/rfc8032	(a new kind of ECC) Used in Zcash	
	Others	BN	https://cryptojedi.org/papers/dclxvi-20100714.pdf	Used in Zcash/Ethereum/Venachain	BulletProof
		BLS	https://www.iacr.org/archive/asiacrypt2001/22480516.pdf	(short outcome) Used in Zcash/Ethereum	Consensus
Random Number Generation		TRNG	GM/T 0005-2012 Randomness Test Specification SP 800-22 rev1a A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Application	Generates random numbers. No specific algorithm requires.	All

Figure 3 **Cryptographic algorithms**



Functions	Classifications	Names	Standards	Description	Using Cases
Hash Algorithms	Hash	The SHAs	https://doi.org/10.6028/NIST.FIPS.180-4	Widely Used	All
		Keccak256/SHA3	https://doi.org/10.6028/NIST.FIPS.202	Widely Used	
		SM3	GM/T 0004-2012 <SM3 Cryptographic Hash Algorithm> http://www.gmbz.org.cn/upload/2018-07-24/1532401392982079739.pdf	National Standard of PRC	
		The Blakes	https://www.ietf.org/rfc/rfc7693.txt.pdf	Used in Zcash/Ethereum	
		RipeMD	https://en.bitcoin.it/wiki/RIPEMD-160	Used in BitCoin	
Symmetric Encryption Algorithm		AES	https://doi.org/10.6028/NIST.FIPS.197	Frequently used in BitCoin/Ethereum/Venachain	To protect private key.
		SM4	GM/T 0002-2012 <SM4 Block Cipher Algorithm> http://www.gmbz.org.cn/upload/2018-04-04/1522788048733065051.pdf	National Standard of PRC	

Figure 4 **Cryptographic algorithms**

Section III: Security Analysis

3.1 Blockchain Hardware Components

The world of the Internet of Things (IoT) is characterized by a very large number of devices extracting data from their operational environment and reporting information to analytics systems in their network or in the cloud. Other devices will perform operations based upon instructions sent to them by applications. These devices reside beyond the edge of the network. Some of them are capable of direct access to the backend, some others report their data through an edge node that passes the data to the analytics systems. The data is usually the information about the environment (e.g., temperature, speed). It can also be metadata that describes the operations of the devices or the system.

IoT Blockchain Devices

IoT blockchain devices are IoT devices with blockchain access capabilities. Such IoT devices can extract data from their operational environment (e.g., temperature, speed) and reporting information to blockchain. If the IoT device has sufficient computing, storage, and wide area network communication capabilities, it can directly access the blockchain. Otherwise, the IoT device must access the blockchain through a blockchain gateway. IoT devices neither participate in blockchain consensus nor store blockchain ledgers. So, they are not blockchain node servers. IoT devices must have the capabilities of hashing, signing and encryption.

Blockchain Hardware Wallet

Blockchain hardware wallet holds and manages the blockchain key pairs and related information related to the blockchain access. The hardware wallet is a secure enclave for the sensitive credentials. The host can sign the blockchain transactions with the hardware wallet. Hardware wallets must have the capabilities of hashing, signing and encryption.

Blockchain Gateway

Blockchain gateway provides relay functionalities for IoT blockchain devices to access the blockchain node server. The blockchain gateway may aggregate the data and manipulate the format of the data. The blockchain gate should have good network communication capabilities. Gateways usually neither participate in blockchain consensus nor store blockchain ledgers. So they are not blockchain node servers. Blockchain gateway devices must have the capabilities of hashing, signing and encryption.

Blockchain Node Server

Blockchain node servers compose blockchain network. They store the blockchain ledger and provide blockchain services to the outside world. Blockchain node servers have 2 major types: light nodes and full nodes, based on whether they participate in the blockchain consensus. Full nodes that support consensus require more computing power, more storage space, and better networks. Blockchain node servers must have the capabilities of hash, signing, encryption, and consensus algorithms.

3.2 Key Assets to Protect

System Software

System software refers to the basic software stack of blockchain devices, such as firmware and operating system or runtime environment. System software usually has the highest access authority to equipment resources, so it plays a vital role in equipment security.

Device configuration

Current date/time. TLS certificate verification requires knowledge of the current date and time to determine if the current time falls within the certificate’s current validity time. Trusted blockchain node servers, because BSD devices and BWD devices do not have the ability to participate in the blockchain consensus, it is necessary to trust the data or services provided by the blockchain node server.

Blockchain device secrets

To authenticate the blockchain devices to the remote service and verify identity of remote service, the blockchain devices must possess secret. For example, the root certificate list and the secret that be used to mutual authenticate between the external entities and the blockchain devices.

Wallet secrets

The blockchain wallet secret usually is private key. The private key is what grants a blockchain user ownership of a given address. When you send transaction from a blockchain wallet, the private key be used to sign the transaction, which indicates to the entire blockchain network that you have the authority to the address you're operating.

Sensor data

Sensor data is the output of a device that detects and responds to some type of input from the physical environment, for example, temperature, speed etc. Sensor data may be used to provide information or input to blockchain. Sensor data shall be delivered without modification or tampering.

Communication

Data or assets are communicated from block sensing device and blockchain node server or vice versa. between components of the blockchain system environments. Based on different device capabilities and network conditions, communication may be completed through many transmission nodes. For example, BSD collects environmental data, transfers the data to BWD for transaction creation and digital signature, and then transfers transaction to the blockchain node server via the BGW device. The safety of the entire communication link is of paramount importance.

Blockchain Ledger

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains several transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. Because a lot of key data is stored on the blockchain ledger, its security and trustworthiness are of utmost importance.

3.3 Threat Models

3.3.1 Attack Types

We apply STRIDE to all entry points to help us identify the threats to blockchain device including threats from hardware attacks, for example exploiting debug interface or tampering of local storage, as well as software and lifecycle attacks.

Physical attack

For unattended IoT devices placed outdoors, attackers can obtain key information and fake device identities through physical attack methods such as probes, side channels, or disassembly.

Man-in-the-middle attack

For mobile blockchain devices, attackers can intercept and tamper with data sent and received by blockchain devices by setting up pseudo base stations or wireless gateways to conduct man-in-the-middle attacks.

Software Attack

Attackers can download and install malicious applications on open operating system blockchain devices to obtain key assets (such as client secrets and keys) and sensor data or execute instructions that exceed their own authority.

3.3.2 Attack Methods

The following list is intended to act as an aid to architecture, design and implementation efforts surrounding enterprise projects that use these technologies：

- **Smart Contract Injection**

  The Smart Contract engine is an interpreter for a (sometimes novel) programming language and a parser of data related to the decisions the engine needs to make. The hazard in this situation is when executable code appears inside smart contracts to subvert the contract language or data. Implementers need to consider sanitizing inputs to smart contracts, proper parsing, and error handling.

- **Replay Attacks**

  Not only is there a threat in transaction processing and validation, but also in node behavior, authentication, and the securing of confidential messaging. Adding nonces to check against prior transactions is critical.

- **History Revision Attacks**

  Blockchains that rely on fault-tolerant consensus models do well when there are many participating nodes processing, competing, and collaborating on the next block. When the number of nodes drops, or if there is predictably cyclic behavior, lulls can be leveraged in a history revision attack where a new branch is created, effectively deleting a previously accepted transaction. Designers should consider how to best guarantee minimum support and the diversity of nodes.

- **Permanence Poisoning**

  Due to the permanence of blockchains and the cost to fork, it's possible to sabotage a chain with even claims of illegal content to draw the ire of regulators and law enforcement.

- **Confidential Information Leaks**

  Permanence increases the risk of data being exfiltrated out of the chain. Even encrypted data is at risk for future threats against those algorithms or brute-force attacks. Designers need to make sure that they understand the data being stored, how it is protected, who owns it and how it could be re-associated with any pseudonymized users.

- **Participant Authentication Failure**

  Are transaction creators cryptographically signing their transactions? Is that signature verified by the protocol? Is transaction receipt confirmed (non-repudiation)? Are sessions managed? Architects need to consider the proof of possession of private keys in the verification and authentication of participants.

- **Node Spoofing**

  Nodes are the entities that create and agree on the next new blocks in a chain. Nodes should be authenticated like any other user or system, and authentication must be verified, with multiple votes prohibited. Designers who fail to look for voting irregularities open their implementation to risk**.**

- **Node Misbehavior**

  Nodes that behave incorrectly, intentionally circumventing fault-tolerance mechanisms, or trojan nodes (nodes in public chains that follow the standard protocol but have non-standard implementations) are problematic. Transaction propagation non-compliance is another concern—where nodes don't convey transactions quickly to other nodes, nodes consistently act in opposition to other nodes, or verifications align consistently within small fiefdoms. In addition, architects need to consider what happens to the chain operations when the chain, the nodes or a subset of the nodes is subject to a denial-of-service attack.

- **Untrustworthy Node-Chain Seam**

  The cryptographic difference between what was intended by the participant, what happens in the node, and what happens on the chain must all be consistent. Architects should enforce a design such that the node is unable to modify a transaction (signing and hash verification), skip a transaction (non-repudiation) or add new transactions (source verification).

- **General Security Hazards**

The hazards fall into this meta-category of general security concerns that have specific implications in the blockchain/DLT realm. Architects, designers, and implementers all need to take heed of these practices and work to ensure a complete solution:

- **Unproven Cryptography**

  Look for best practices and proven cryptography in cipher suites, hash algorithms, key lengths, elliptical curves used, etc.

- **Non-Extensible Cryptography**

  Should a foundational algorithm aspect of the chain become compromised, can the chain easily migrate to another suite/hash/key pair? Is there a mechanism and process among node operators to agree and deploy this quickly?

- **Security Misconfiguration**

  Be aware of all code libraries used, stay abreast of the latest security information about deployment technologies such as Docker, and ensure that defaults present in test systems are not available in production systems. Ask if there are any components with known vulnerabilities, determine whether any open ports or file-system permissions may be at risk, and understand protection mechanics for private keys.

- **Insufficient Logging and Alerts**

  If something goes wrong, are there sufficient methods in place to capture actions that occurred (voting, smart contracts, authentication, authorization)? Project managers must ensure that alerts have been added to the code, that the correct recipients have been added at deployment time, and that procedures for constant monitoring and updating of those recipients take place.

- **Weak Boundary Defense**

  Development teams need to be aware of, and shore up, defenses so that there are no exploitable holes in client code or node software, smart contract engines, mobile applications, web applications, chain viewers or administrative tools.

3.4 Security Requirements

Attacks need to be considered within the frame of their cost and the value of the targeted data. The higher the value of the targeted data, the stronger the protection required for this data. For valuable data, the security and the protection need to be strong and robust: it must withstand numerous repeated attacks. One needs stronger and more robust protection for banking applications than for meters tracking the weather. We need to capture that the value of the data and the regulations of the industry will define the level of security and the robustness of the security solutions.

Anti-physical attack mechanism

The blockchain device itself has an anti-physical attack mechanism or a sub-module (such as a secure element) that contains the anti-physical attack capability, and the key functions of the blockchain device are placed in the secure element for execution. Anti-physical attack mechanism can be used to defense Physical Attack, also can be used to provide support to Man-in-the-middle Attack and Software Attack.

Secure Channel

The communication between the blockchain device and the server node must be carried out through a secure channel (such as the TLS protocol), and at least a one-way authentication mechanism is provided to ensure that the server node accessed by the blockchain device is trusted. Secure channel can be used to defense Man-in-the-middle Attack.

Application Management

The open operating system of the blockchain device needs to have a mechanism to verify the authenticity and integrity of external application files to ensure that only applications from legal sources can be installed on the blockchain device. Application management can be used to defense Software Attack.

Root of Trust

Blockchain devices need to have a root of trust mechanism. The root of trust includes computing engines, secret data, and code logic for providing root of trust services. The root of trust is the cornerstone of blockchain device security and needs to be strictly protected to prevent software attacks and some or all hardware attacks. In addition, the root of trust needs to be provisioned in a safe production environment. Root of Trust can be used to provide support to Man-in-the-middle Attack and Software Attack.

Physical Memory Isolation

For blockchain devices that support multiple application execution capabilities, a physical memory isolation mechanism is required. Physical memory isolation needs to ensure that application process resources are isolated from others. For devices with high security levels, isolation from the operating system is also required. The memory isolation mechanism includes all resources related to memory management, such as caches, memory management units, buses, and so on. Physical memory isolation can be used to defense Software Attack.

Section IV: Architecture

4.1 Overview

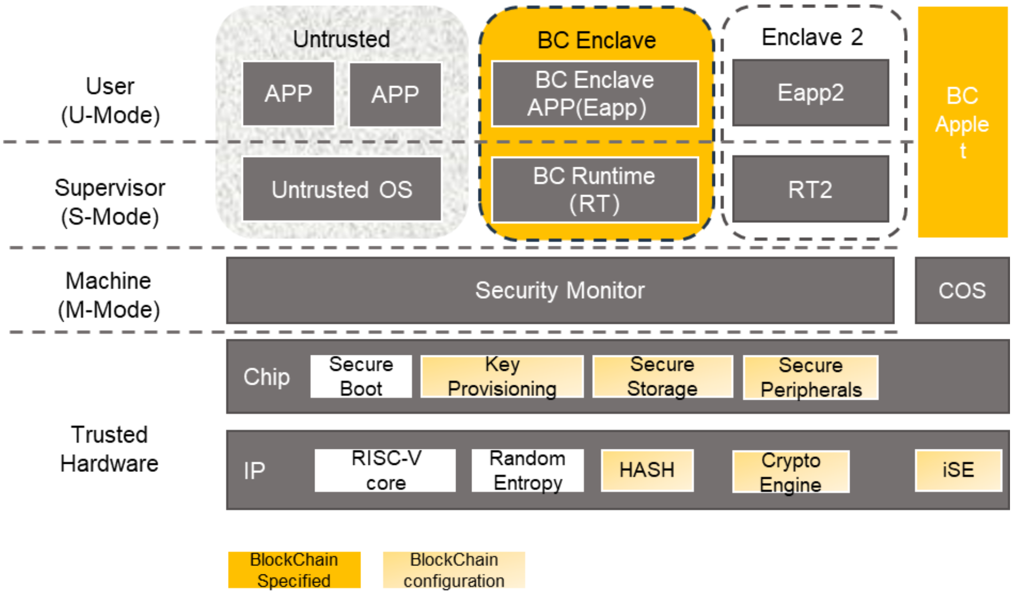


Figure 5 System Architecture

4.2 Root of Trust

The security of the blockchain must be enforced as soon as the chip boots after power-up. It is the first task to be undertaken, in that it is liable for the system trustworthiness across all subsequent operations. The requirement is therefore for the chip to leverage an existing "root-of-trust" IP. The functionalities of this IP are the following:

- Platform integrity, both from physical and logical standpoints. First, this requires a verification of the presence of the IPs, and of their proper functioning (e.g., thanks to self-tests); second, a verification of the integrity and authenticity of the firmware is required. This starts with the root-of-trust own firmware, and if validated, it extends to the system firmware as well. This is referred to as a two-level "secure-boot" stage.

  After this verification that the platform is genuine and in an acceptable state, the root-of-trust keep tracks on this information and releases the "host", that is the blockchain main function. The blockchain application can thus safely start at this stage, with the assurance that the platform has not been manipulated anyhow.
- Prior to being used, a root-of-trust shall be initialized. This step is called the provisioning. It consists in the

programming within the root-of-trust of a master-key (and of its associated applicative firmware). The traditional provisioning scenario is that of credentials injection: the configuration elements are securely provided from the outside. However, a novel paradigm is emerging, which consists in master-key extraction from the device, leveraging a Physically Unclonable Function (PUF). These two processes are explained below:

- Injection is straightforward: the master key is generated from the outside of the chip and are copied in a trusted facility.
- Extraction is different in that the master key is already resident inside of the chip. It is extracted from the silicon by a so-called "key rebuilding" process, which occurs upon each boot. The advantages are twofold. First, the master key vanishes as soon as the device is no longer powered, which allows to proactively fight invasive attacks. Second, the master key is only concealed within the chip itself and is not present in an external device. As a corollary, there is no requirement that the provisioning facilities be trusted.

After the root-of-trust has released the host, its mission is completed. The subsequent services are those of "confidential computing", typically embodied as a Trusted Execution Environment (TEE). The root-of-trust can be managed by an integrated Secure Element (iSE). The TEE can as well leverage the iSE for some of its security critical subfunctions.

4.3 TEE

TEE, the Trusted Execution Environment ensures the chips' systems, terminal parameters, safe data, and user data cannot be tampered with or illegally acquired, to fulfill the safe requests of smart devices and Internet of Things.

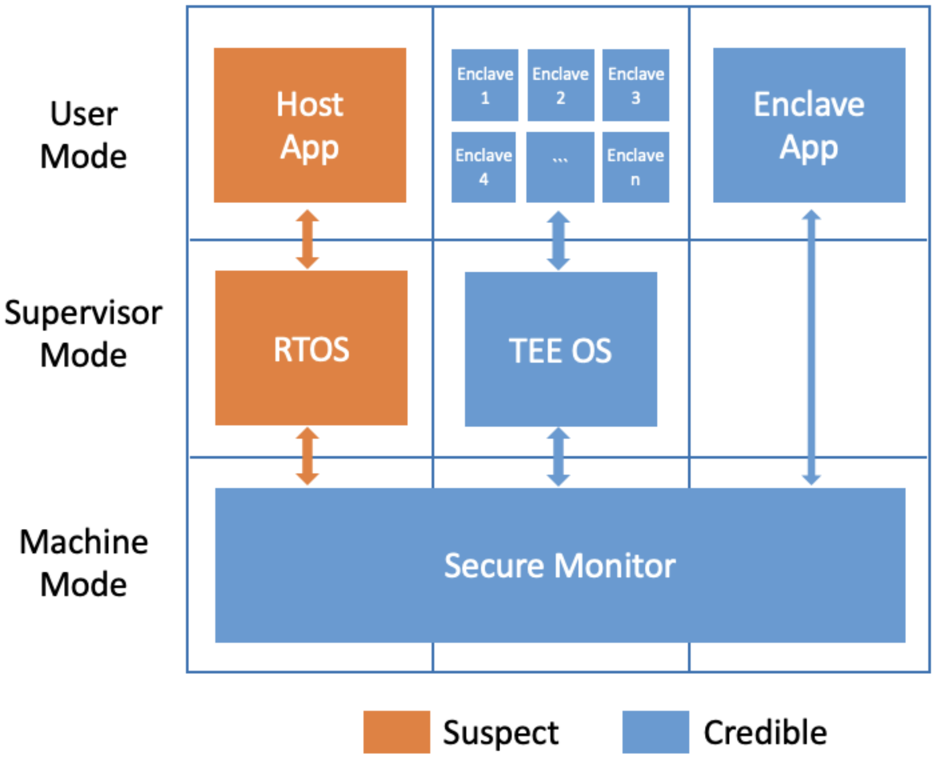


Figure 6 RISC-V TEE Secure Architecture

On the hardware security side, RISC-V standard architecture supports two properties of security scaling capability: physical memory protection (PMP) and privileged mode for different levels (M/S/U-mode). PMP can divide processors' access addresses into several minimum four-byte alignment areas, different areas can allow different RWX and control different levels of privileged mode, as well as PMP 's configuration register can only configure at machine mode. Different levels of privileged technologies can divide the operating state of processor into machine mode, supervisor mode and user mode. Machine mode can be used to run security-related programs, together with PMP technology, machine mode can insulate several separate memory intervals and can intercept interrupts and exceptions with the relevant configuration registers. Supervisor mode and user mode can be used to run in the separate memory intervals insulated by machine mode to make sure the safety of systems and data.

The processor's machine mode will used to run a lightweight secure monitor program which adopted a formal verification design method, used the PMP technology for physical address intervals management, interrupts and exceptions management, the program can also provide remote proof and functions such as in Enclave App runtime management and isolation as well as secure data interaction technology (Picture). Each separate Enclave App runs on supervisor mode or user mode, different Enclaves are isolated from each other and not directly accessible to each other, to prevent the risk of data tampering. With this solution, normally the Host Enclave App will be running as the REE, at the mean time Host Enclave App can create and run multiple preset Enclave Apps as security services, such as to access and process private data and pass the desensitized and processed data or results to Host Enclave App through Secure Monitor.

- TEE on RISC-V consists of following components.
- Secure monitor which is extended with TEE related features.
- TEE services which provide basic security capabilities, such as secure storage service， attestation service and cryptography service.
- Secure enclaves, which run security-sensitive logic.
- Untrusted components, which run untrusted operating system and untrusted apps.

Memory protection

TEE shall provide the ability to create isolated memory regions. In this architecture, secure monitor is extended to configure PMPs to achieve required scheme of isolation.

Blockchain code and all runtime data shall only reside in dedicated and isolated memory regions. Each PMP region shall be appropriately configured to provide minimized privileges. Sections in blockchain software with different accessibilities must be placed in different PMP regions.

Isolation of interrupt

In this architecture, an interrupt could be configured to be visible to an enclave or the untrusted component. Once configured, the interrupt is only visible to the given component. Secure monitor is extended to manage the status and route of interrupt.

By default, all interrupts are visible to untrusted components. Secure monitor shall provide ABI calls that would allow the software to control the visibility of an interrupt to current component.

Secure storage

TEE shall provide abilities of secure storage to store persistent data provisioned or generated during the execution of blockchain software. Secure storage service must provide confidentiality and integrity.

Security of peripheral devices

Blockchain software shall be able to leverage hardware random number generator or hardware components with similar ability to supply entropy for any required cryptography functions, such as key generation or signing.

The components which supply entropy shall be dedicated to the BC enclave or the secure monitor shall provide ABI calls that would prevent the multiplex of the hardware components while they're being used by the BC enclave.

Provision and attestation of the device

To securely identify a device, the device must be provisioned with a hardware secure unique ID and a device unique key pair from asymmetric cryptography algorithm.

The value of hardware secure unique ID shall be derived from the hardware random entropy and be stored in the secure storage. The keypair shall be generated on the device or imported from a trusted external source, i.e., HSM. The keypair shall be stored in the secure storage.

During the manufacture of device, hardware secure unique ID and the public key of the key pair shall be registered online in a secure channel so that it could join the blockchain network securely.

To attest a device, the device must be provisioned with a model unique key pair from asymmetric cryptography. The key pair shall be stored in the secure storage. Secure monitor shall provide ABI that would allow an enclave to attest its runtime state to the remote server.

4.4 Integrated Secure Elements

RoT and TEE rely on the capability of chip assets to be safeguarded, and managed. This is the function of an integrated Secure Element (iSE), whose (immutable) hardware parts and (flexible) software parts are described below. A typical architecture for an iSE is depicted in Fig. 2.

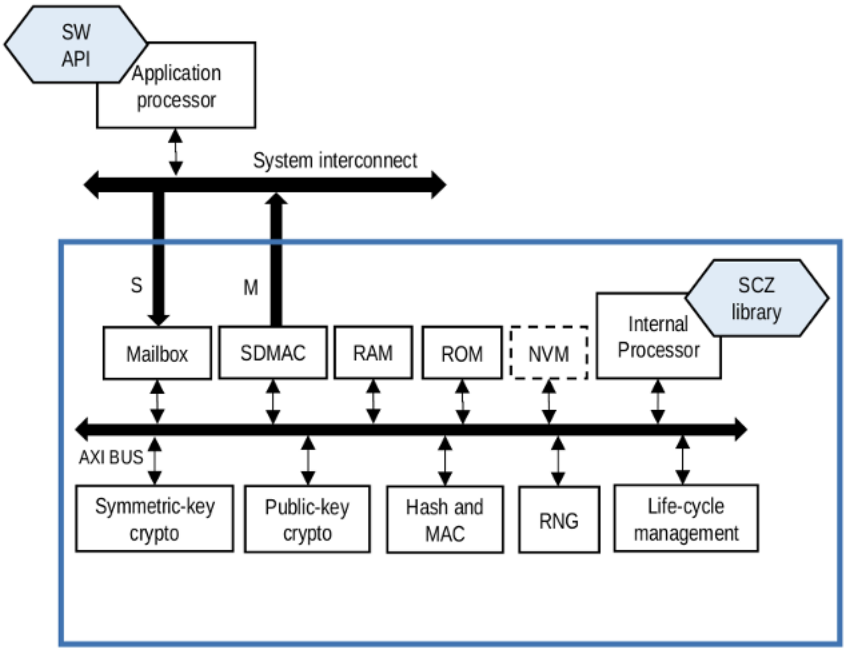


Figure 7 An Integrated Secure Element

4.4.1 Hardware

The iSE is an enclave, which is isolated from the host system (i.e., the blockchain chip). The assumption is that the host can be corrupted, hence a protocolar isolation between host and iSE. In practice, this is enforced by a mailbox: an API is used to request the mailbox, and the mailbox analyses the requests before they are processed. Incorrectly formatted or otherwise invalid requests are discarded. Such architecture incurs some performance loss but is safe in terms of worst-case assumptions on the platform reliability.

Internally, the iSE has some Non-Volatile Memory (NVM) storage for the keystore, the capability to generate keys with a Random Number Generation (RNG), and basic cryptographic primitives. In addition, it communicates with the host (data to encrypt/decrypt/sign/etc.) through a Secure Direct Memory Access Controller (SDMAC), which is only configured from within the iSE. Eventually, the iSE can handle its life cycle, each cycle being associated with some rights or restrictions on the resources managed by the iSE.

4.4.2 Software

The iSE software is responsible for offering security services, such as:

- Platform integrity verification (see Root of Trust section §4.2).
- Key management and cryptographic services.
- (optionally) User management and mapping between roles and permissions.

A more detailed description is provided in this paper. (Sylvain,2021)

The iSE software can be patched through a Secure Firmware Update Over-The-Air (SFUOTA) mechanism. Obviously, a firmware version can only be replaced by a version with a greater version number.

4.5 Physically Unclonable Function

Physical unclonable function (PUF) is a hardware security technology, which uses physical device variations to generate unique device responses that cannot be cloned for a given input. On a higher level, PUFs can be considered similar to human Biometrics - silicon fingerprint， they are the unique identifier of each piece of silicon.

Due to deep submicron manufacturing process variations, every transistor in an IC has slightly different physical properties. These variations lead to small but measurable differences in terms of electronic properties, such as transistor threshold voltages and gain factor. Since these process variations are not fully controllable during manufacturing, these physical device properties cannot be copied or cloned.

Importantly, although these variations may be random between different IC, once known, they are deterministic and repeatable. PUF generates a unique encryption key for each IC by taking advantage of this internal difference in IC behavior.

The silicon fingerprint is turned into a cryptographic key that is unique for that individual chip and is used as its root key. This root key is reliably reconstructed from the PUF whenever it is needed by the system, without a need for storing the key in any form of non-volatile memory. So, when the device is powered off, no secret key is present in any form of memory; in effect, the root key is “invisible” to attackers, which makes storage of keys with PUFs very secure.

Section V: Detailed Use Cases Implementation

5.1 Bio Tech

Due to the peculiarities of traditional beef cattle assets, such as difficulty in value determination, income assessment, ownership confirmation, post-loan management, risk management, and easy abnormal extinction, such assets are often not collateral recognized by financial institutions. The problems of difficult and expensive financing for beef cattle breeding companies have not been effectively resolved.

Using customized beef cattle collars combined with blockchain technology, each beef cattle can be given a unique identity, and the key growth data of beef cattle during the beef cattle breeding process will be left in the blockchain, helping financial institutions solve worries of beef cattle asset supervision for the future. At the same time, the digital animal husbandry bills generated using blockchain technology can be used as collateral recognized by financial institutions after the authority has registered and confirmed their rights. The generation and destruction of digital animal husbandry bills are synchronized with the beef cattle breeding process, and the digital twins are used to realize the digitization of beef cattle assets.

Beef cattle collars empowered by blockchain have improved the degree of informatization for beef cattle breeding companies on the one hand, and on the other hand provided credible financial data service for financial institutions, which can efficiently allocate financial resources to the beef cattle industry that has lagging financial services.

Beef cattle collars need to have anti-physical attack mechanisms and a root of trust. Because beef cattle are high-value financial assets, their security depends on the continuous tracking of beef cattle biological information. It is necessary to ensure that attackers cannot forge the biological information of beef cattle. Therefore, beef cattle collars need to have an anti-physical attack mechanism to ensure that attackers cannot extract the root of trust and forge biological information of beef cattle.

5.2 Gateway

In many industrial sections, surveillance systems provide various value-added solutions, such as AI-based video analysis (proactive surveillance, autonomous risk recognition, video classification, etc.). While to unleash the great potential of this solution requires strong collaborative computation and data sharing, no matter done by 3rd party service provider or MPC. Under this situation, private and sensitive data leaking is a big obstacle, especially considering growing serious cyber-attacks, untrusted 3rd parties (cloud provider, application provider, etc.) involved, and requirement of regulatory compliance (GDPR, PIPL, and etc.). Blockchain is acting as a promising collaborative networking by keeping data integrity through its data replication and consensus executed by smart contract, but data confidentiality is not guaranteed. TEE takes the place to provide secure execution environment. It is keeping data confidentiality and blockchain execution safety. Within TEE, execution worker utilizing AI algorithms is used for inference by feeding video captured data and meta data. Meanwhile, privacy policy is strictly to comply based on smart contracts. The data provider can utilize blockchain and smart contracts to define and enforce which functions can be evaluated against which data and who is granted to access the results, and it keeps transparency and control. At the same time, history-based policies make sure that executions don't repeats partially or entirely to reveal confidentiality through correlation, as each activity are logged, and decision of execution is to rely on timestamp transactions within blockchain.[1]

Blockchain gateway devices need to have a root of trust, anti-physical attack, secure channel, application management and physical memory isolation mechanisms. The root of trust enables the gateway device to authenticate its identity to the outside world and to verify the legitimacy of external entities. The anti-physical attack mechanism enables the gateway device to effectively resist external attacks and protect sensitive data inside the device. Application management ensures that only legitimate applications can run on gateway devices. The physical memory isolation mechanism isolates multiple applications running on the gateway device from each other, preventing internal data leakage. Secure channel ensures secure communication between gateway device and external associated devices.

5.3 NFT

In automotive industry, it is evolving fast towards vehicle networking. On this long journey, some Metaverse related use cases will be realized in the quite near future. It helps us investigate Metaverse not from buzzword way.

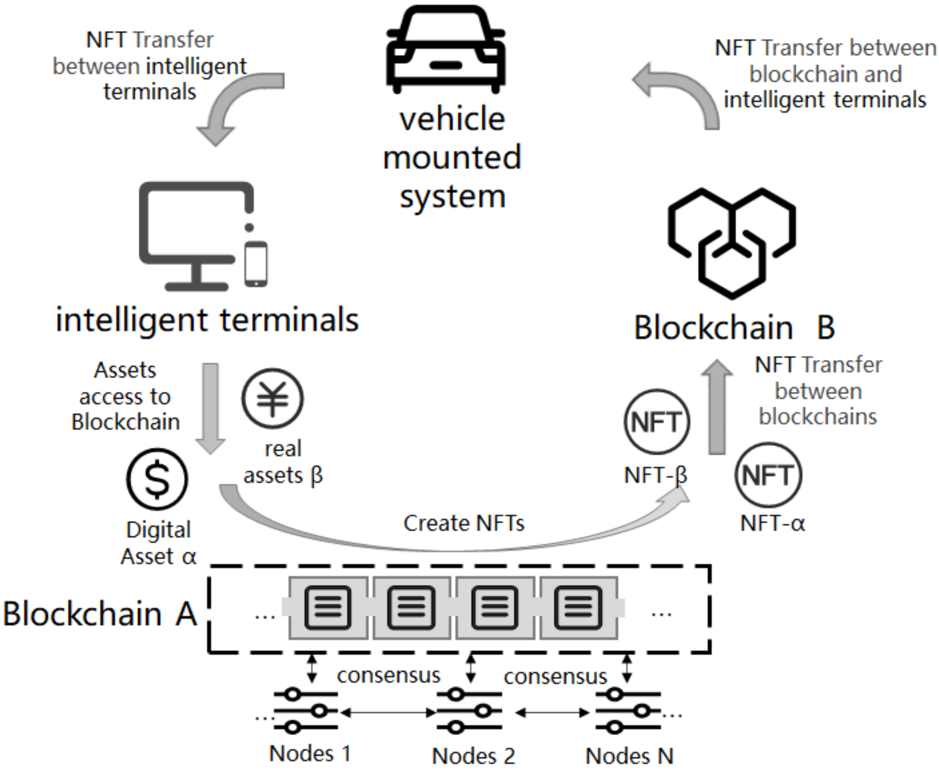


Figure 8. NFT Using Case

In the future automotive ecosystem, fundamentally, every participator (vehicles, consumers, OEMs, etc.) will be decentralized identified against blockchain network powered by DID/Verifiable Claims solution. A car will have its own hardware-wallet to manage its identity, certificate of birth issued by OEM, certificate of insurance issued by an insurance company, etc., and publicly being verified. A consumer or driver will also have his/her own software-wallet to manage identity and claims such as a driver license issued by an agent. The similar for other participators. All these forms a trusted transaction layer to support business models, including digital rights management, where digital rights be able to represent physical items (like computer/cellphone), digital rights be able to represent benefits (like credits), or digital rights be able to represent virtual items (like virtual arts/skin in games). The digital rights can also be coded as NFTs, to leverage its transferability between different platforms. Behind all of these we mentioned are blockchain technology, the value and content of NFTs are protected by different consensus nodes.

Users can save everything in real world as NFTs through car systems, and these NFTs can be transferred and used by any cases in real world.

Vehicles with NFT capabilities need to have a root of trust, anti-physical attack, and secure channel mechanisms. The root of trust allows the vehicle to endorse the generated NFT to prove its legitimacy. The anti-physical attack mechanism enables the vehicle to effectively resist external attacks and protect sensitive data used to generate NFTs. Secure channel ensures secure communication between vehicle and external associated devices.

5.4 Carbon Neutralization

Blockchain technology can be used for carbon data traceability, offering the possibility to ensure the trustworthiness of carbon data sources. Blockchain technology is applied to the chips and cellular communication modules of IoT devices, and specific security containers are used to ensure that the chips have unique DNA by realizing Root of Trust within the devices, giving full play to the value of blockchain technology, making carbon footprint data obtain security protection and credible signature from the collection end, ensuring that carbon footprint data are credible from the source, and truly realizing the "one thing chain", realize the credible chain of carbon data, build a credible carbon data ecology, realize the property rights of carbon data resources and the circulation of carbon data transactions.

Combining IoT technology and blockchain technology, we provide carbon data trustworthy solutions for ESG, carbon trading and green certificate issuance, ensuring carbon data is real from the time of collection, preventing carbon data from being maliciously tampered, and providing neutral and fair independent verification service for carbon data authenticity. It can achieve three dimensions of carbon footprint data trustworthiness: **trustworthiness at the point of data collection, uniqueness of data source, and trustworthiness of data flow.** The project can provide credible data cornerstones for government regulation and commercial behavior, help digital government efficiently improve governance, promote the transformation of enterprises in the clean energy consumption structure, promote green economic development, and realize the value of green data.

Trusted at the data collection

When the data is collected by the IoT device, that is, the data is hashed and signed using the unique private key of that device to form the data fingerprint of that segment of data. After this segment of data is uploaded to the cloud, it can be verified by the hash and signature of the data fingerprint whether it has been tampered with or not from some recognized legitimate device.

Data source one trusted

A unique key pair and ID is generated on the device, the private key will not be available from outside, and the private key is signed on the data hash on the IoT device to ensure that the data comes from that device.

Data flow trusted

The cellular module on the device is uploaded to the blockchain node through the data fingerprint (hash and signature) generated on the IoT device or chip, and the blockchain node will be recorded in the blockchain ledger to ensure that the data is not tampered with.

Section VI: About the RISC-V Blockchain Special Interest Group

The RISC-V Blockchain Special Interest Group (RISC-V Blockchain SIG) is a group explores ways to combine blockchain technology and RISC-V architecture to make sure not only the online data are tamper-free but also the original data are authentic. The RISC-V Blockchain SIG brings experts across the RISC-V and blockchain industry, chipmakers, device vendors, and blockchain service providers all together, see the need of data security improvement.

This whitepaper aims to define the requirements of security in different blockchain using cases and get better combinations of security and costs of RISC-V chips in blockchain with IoT field.

This content represents the collaborative work (“Work”) of the RISC-V Blockchain Special Interest Group (“RISC-V Blockchain SIG”). The RISC-V Blockchain SIG is solely responsible for the Work and Individual RISC-V Blockchain SIG members may not have contributed or participated or may not endorse it.

Thanks to our contributors:

Wenhui Tu, Huan Yang, Zekang Jin, Jiabin Liu, Yaojia Fan, Yabo Zhang from Wanxiang Blockchain Inc.

Leo Lin, Gary Xu, Xishun Feng, Feng Huan from Shanghai Molian Information Technology Co., Ltd.

Boho Yuan. From Guangdong Leapfive technology limited.

Marc Canel, from Imagination Technologies.

Sylvain Guilley, Shengnan Wang, from Secure-IC China Co., Ltd.

Huaqi Fang from Nuclei System Technology.

Liang Liang, Wenhao Li from Shanghai Pingbo Information Technology Co., Ltd.

Appendix A: References

[1]R. Sinha, S. Gaddam, and R. Kumaresan, “LucidiTEE: A TEE-Blockchain System for Policy-Compliant Multiparty Computation with Fairness,” p. 18.

[2]Sylvain Guilley; Michel Rolland and Damien Quenson. (2021). Implementing Secure Applications Thanks to an Integrated Secure Element. In Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP, ISBN 978-989-758-491-6; ISSN 2184-4356, pages 566-571. DOI: 10.5220/0010298205660571

[3]Nucei;Security Extension based on RISC-V Architecture

[4] https://www.rfc-editor.org/rfc/inline-errata/rfc6979.html

[5]https://www.rfc-editor.org/rfc/inline-errata/rfc6979.html

[6] http://www.gmbz.org.cn/main/postDetail.html?id=20180724110812

[7] https://www.rfc-editor.org/info/rfc8032

[8] https://cryptojedi.org/papers/dclxvi-20100714.pdf

[9] https://www.iacr.org/archive/asiacrypt2001/22480516.pdf

[10]http://www.gmbz.org.cn/upload/2018-04-04/1522788048733065051.pdf

[11]https://doi.org/10.6028/NIST.FIPS.180-4

[12] https://doi.org/10.6028/NIST.FIPS.202

[13] http://www.gmbz.org.cn/upload/2018-07-24/1532401392982079739.pdf

[14] https://www.ietf.org/rfc/rfc7693.txt.pdf

[15] https://en.bitcoin.it/wiki/RIPEMD-160

[16] https://doi.org/10.6028/NIST.FIPS.197

[17] https://bitcoin.org/

[18] https://ethereum.org/

[19] https://fabricmc.net/

[20] https://www.zcashcommunity.com/

[21] https://chainmaker.org.cn/

[22] https://venachain-docs.readthedocs.io/

Appendix B: Abbreviations

ID： Identity

DID： Decentralized Identity

BNS ： Blockchain node server

ROT: Root of Trust

TEE: Trusted execution environment

iSE: integrated Secure Element

NFT: Non-Fungible Token

MPC: Multi-Party Computation

BSD: Blockchain Sensing Devices

BWD: Blockchain wallet devices

BGW: Blockchain Gateway

NVM: Non-Volatile Memory

RNG: Random Number Generation

SDMAC: Secure Direct Memory Access Controller

SFUOTA: Secure Firmware Update Over-The-Air

PMP: Physical Memory Protection

RWX: Read, Write, Execute permission

GDPR: General Data Protection Regulation

PIPL: Personal Information Protection Law of the People's Republic of China

PUF: Physically Unclonable Function

TLS: Transport Layer Security

HSM: Hardware Security Module

PKI: Public Key Infrastructure

MAC: Message Authentication Code

RAM: Random Access Memory

ROM: Read only Memory

OEM: Original Equipment Manufacturer