RISC-V®

RISC-V Blockchain SIG meeting

2022- Aug 18

Only RISC-V Members May Attend

- It is easy to become a member. Check out riscv.org
- If you need work done between non-members or or other orgs and RISC-V, please use a joint working group.
  - used to allow SIGs but their purpose has changed.

Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.

Collaborative & Welcoming Community

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/risc-v-international-community-code-of-conduct/

Conventions

- Unless it is a scheduled agenda topic, we don’t solve problems or detailed topics in most meetings unless specified in the agenda because we don’t often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unillaterly. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, …
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Trusted RISC-V Architecture in Blockchain Infrastructure White Paper Meeting Attendees

Patty Tu	WXBC, Chair
Gary Xu	aitos, Vice Chair
Huan Feng	aitos
Yabo Rachel Zhang	WXBC

Trusted RISC-V Architecture in Blockchain Infrastructure White Paper

Introduction to Blockchain

- Overview
- Infrastructure
- Challenges
- Value

The Cryptographic Algorithms

- Cryptographic Algorithms of Blockchain
- Value of hardware
- Supporting algorithms

Security Analysis

- Devices
- Key Assets to Protect
- Threat Models
- Security Requirement

Architecture

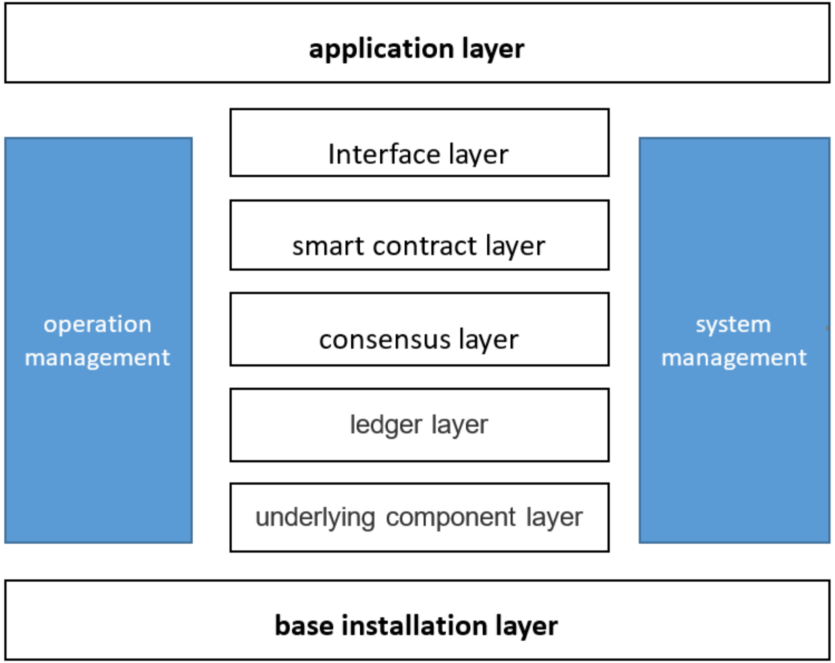
- Overview
- Root of Trust
- TEE
- Secure Elements

Use Cases Implementation

- Overview
- Bio Tech
- Gateway
- NFT
- Carbon Neutralizat

RISC-V®

Blockchain layers and network architecture



application layer

operation management

Interface layer

smart contract layer

consensus layer

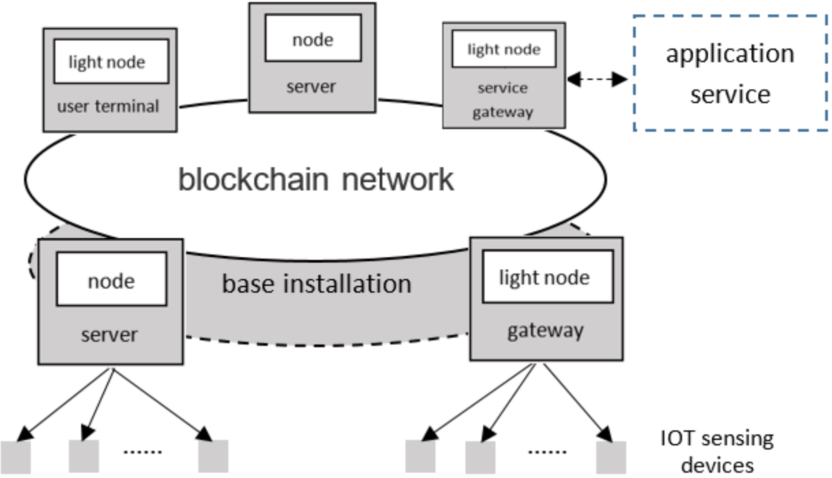
ledger layer

underlying component layer

system management

base installation layer

Blockchain *Technology* Architecture



Base installation Layer

Blockchain Challenges and Objectives

Challenges

Most of IoT device 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.

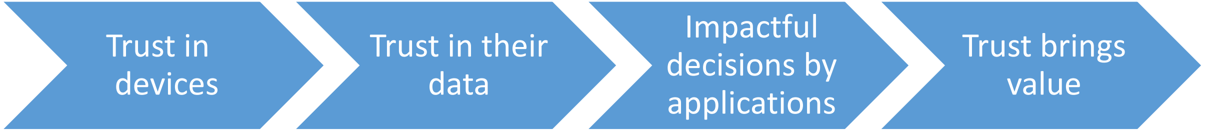
Objectives

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.

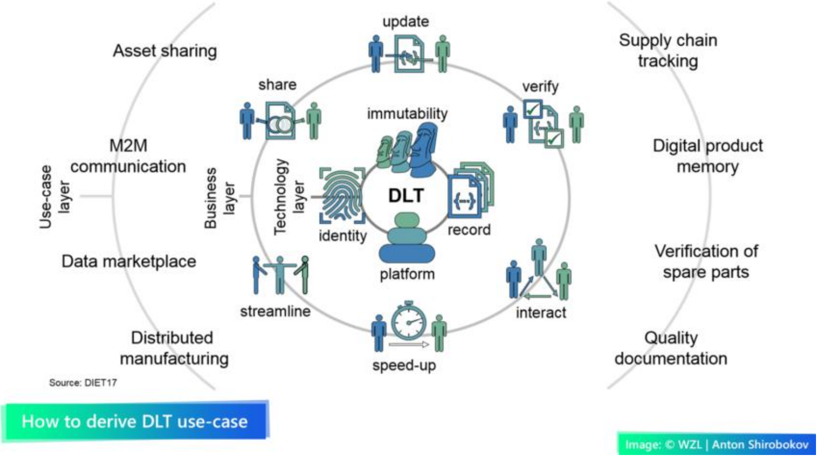
To get better combinations of security and costs of RISC-V chips in blockchain with IoT field.



What Brought Us to Blockchain?
– *the Ultimate Distributed System Logic*

The Case for Blockchain:

- Distributed Ledger: permanent tamper-free data records
- Smart contract: establish automated execution of prior agreement with set conditions; data accessible but not replicable
- Cryptography: data protection across domains
- Consensus: easily establish network of the willing without heavy IT and legal costs.



Source: DIET17

Image: © WZL | Anton Shirobokov

Particularly relevant to the industrial space

- Curated data sharing: addresses one of industrial internet’s biggest challenges – why surrender your data.
- Seamless and real-time brokering of value exchange: from supply chain to value chain, cross-domain data utilization business model.
- Beyond data: could be used to allocate compute resources, in addition to running and training A.I. on mobile devices.

The Cryptographic Algorithms of Blockchain

Cryptographic Algorithms

Hash Algorithm

Digital Signature Algorithm

Encryption Algorithm

The value of hardware chips supporting cryptographic algorithm

Security

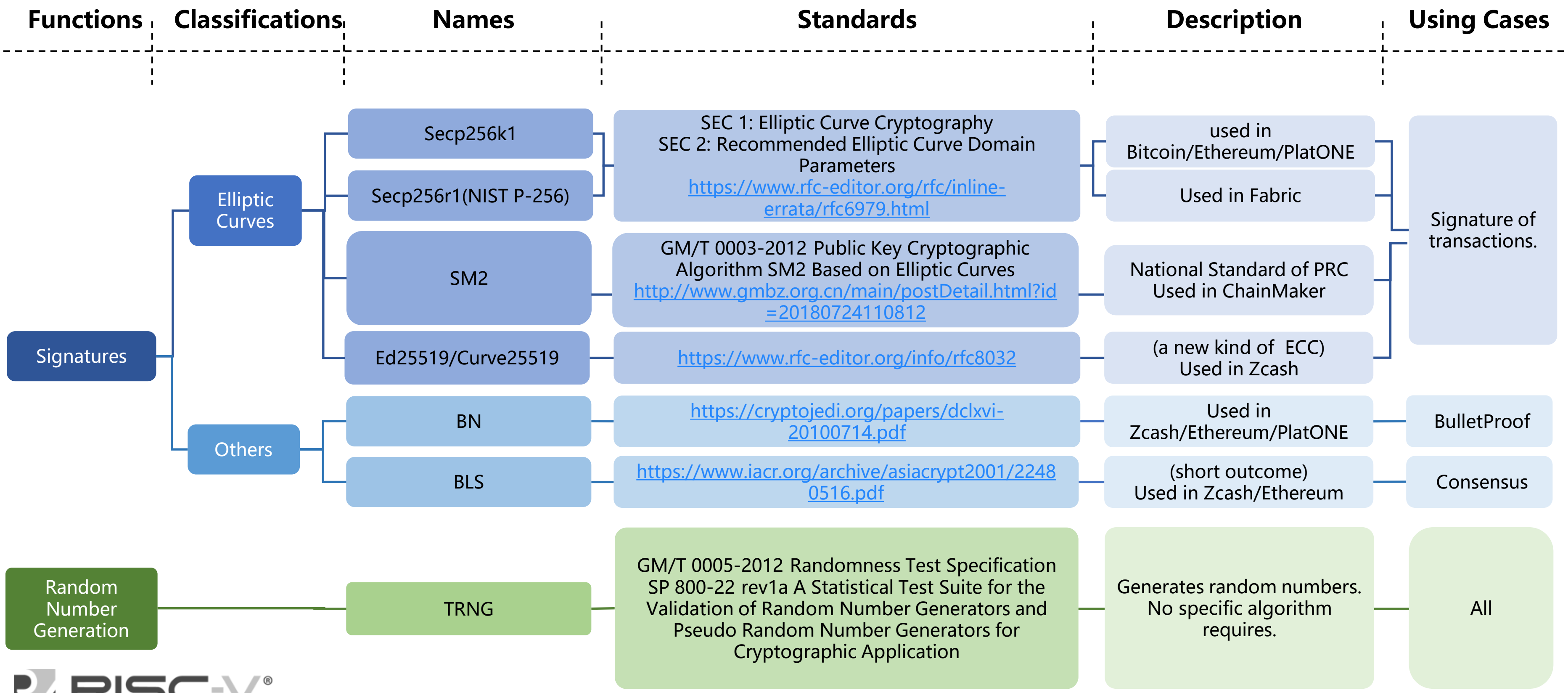
- Hardware chips supporting cryptographic algorithm can elevate the level of security. All the data will be encrypted and decrypted inside of hardware chips so that no data will be disclosed. Hardware chips produce true random numbers from inside, greatly reduced the risks of producing pseudo random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

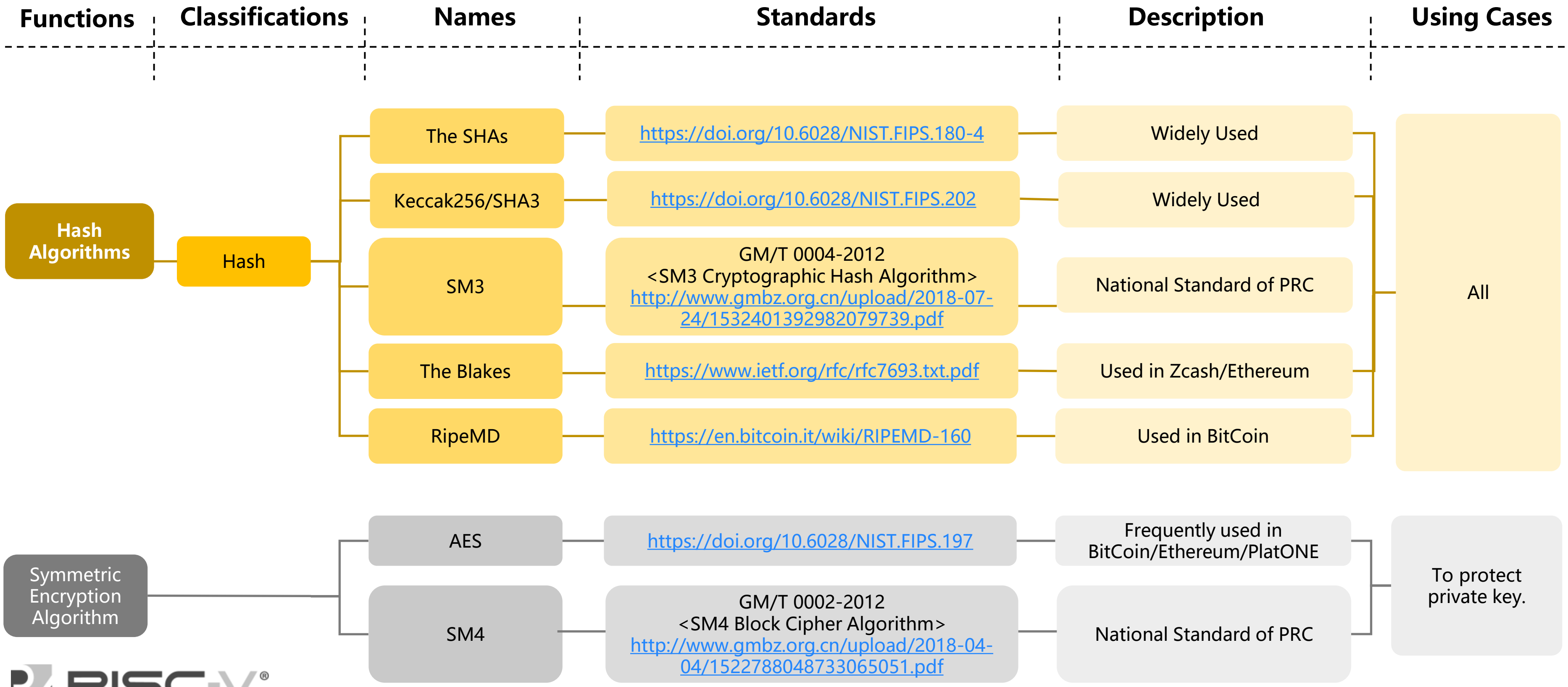
Session II The Cryptographic Algorithms

The Cryptographic Algorithms of Blockchain(1/2)



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/PlatONE	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/PlatONE	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

The Cryptographic Algorithms of Blockchain(2/2)



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/PlatONE	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	

The Cryptographic Algorithms of Blockchain priority

Functions	Categories	Names	Standards	Priority Recommendations
Signature (At least one of them has to be supported.)	Elliptic Curves (Signature verifications for transactions.)	ECDSA(Secp256k1/ Secp256r1)	SEC 1: Elliptic Curve Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters https://www.rfc-editor.org/rfc/inline-errata/rfc6979.html	10
		Ed25519/Curve25519	https://www.rfc-editor.org/info/rfc8032	15
		SM2	GM/T 0003-2012 http://www.gmbz.org.cn/main/postDetail.html?id=20180724110812 <Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves>	20
	Others (mainly for consensus）	BLS/BN	https://www.iacr.org/archive/asiacrypt2001/22480516.pdf https://cryptojedi.org/papers/dclxvi-20100714.pdf	50
Hash Functions （At least one of them has to be supported.）	Hash	Keccak256/SHA3	https://doi.org/10.6028/NIST.FIPS.202	12
		SHAs	https://doi.org/10.6028/NIST.FIPS.180-4	13
		RipeMD	https://en.bitcoin.it/wiki/RIPEMD-160	17
		SM3	GM/T 0004-2012 http://www.gmbz.org.cn/upload/2018-07-24/1532401392982079739.pdf <SM3 Cryptographic Hash Algorithm>	20
		Blakes	https://www.ietf.org/rfc/rfc7693.txt.pdf	25
Random Number Generation (Has to be supported.)	Random Number	TRNG	《GM/T 0005-2012 》 SP 800-22 rev1a :《A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Application》SP 800-22 Rev. 1a,	10
Symmetric Encryption Algorithm (Has to be supported.)	Block Cipher Algorithm	AES	https://doi.org/10.6028/NIST.FIPS.197	10
		SM4	GM/T 0002-2012 http://www.gmbz.org.cn/upload/2018-04-04/1522788048733065051.pdf <SM4 Block Cipher Algorithm>	21

Session III Security Analysis

Blockchian Devices and key assets

Blockchain Devices

- Blockchain sensing device
- Blockchain wallet devices
- Blockchain gateway
- Blockchain node server

Key Assets

- System Software
- Device configuration
- Client secrets
- Wallet secrets
- Sensor data
- Communication
- Blockchain Ledger

Session III Security Analysis

Threat 1/5

Threat model	Description
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.

Session III Security Analysis

Threat 2/5

Attack method	Description
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..

Session III Security Analysis

Threat 3/5

Attack method	Description
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.

Session III Security Analysis

Threat 4/5

Attack method	Description
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.

Session III Security Analysis

Threat 5/5

Attack method	Description
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: 1. Unproven Cryptography 2. Non-Extensible Cryptography 3. Security Misconfiguration 4. Insufficient Logging and Alerts 5. Weak Boundary Defense

Session III Security Analysis

Security Requirements

	Security Requirements
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 defence 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 defence 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 defence Software Attack.

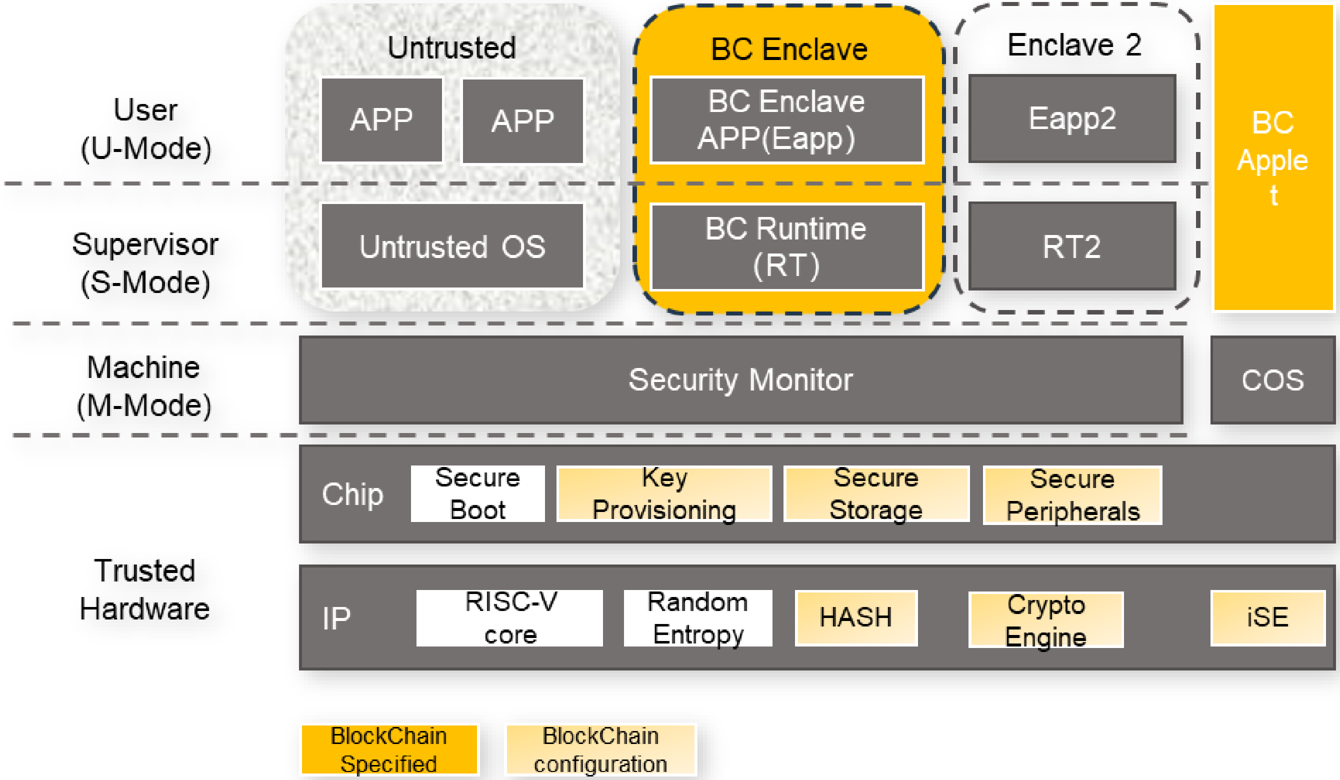
Session III Security Analysis

Security Requirements

	Security Requirements
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 defence Software Attack.

Section IV Architecture

Trusted Architecture(reference)



Section IV Architecture

Root of Trust

Platform integrity, both from physical and logical standpoints.

- This requires a verification of the presence of the IPs, and of their proper functioning (e.g., thanks to self-tests);
- A verification of the integrity and authenticity of the firmware is required.
- This is referred to as a two-level “secure-boot” stage.

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

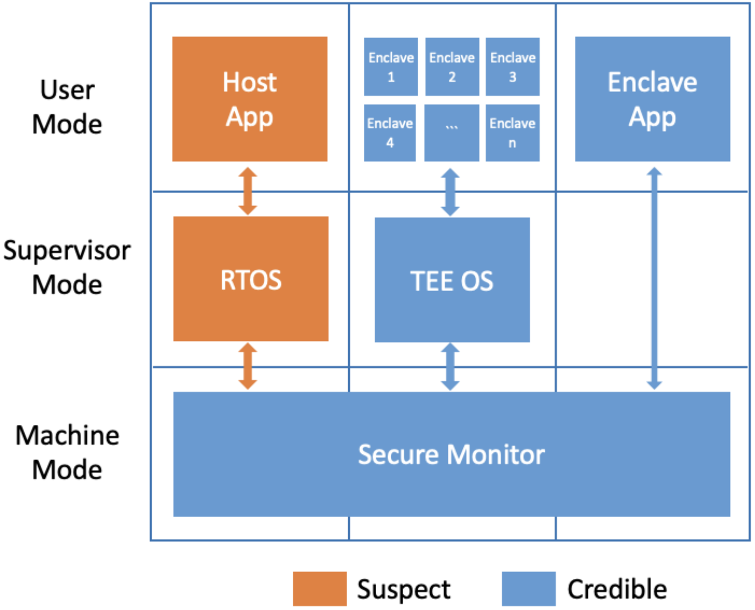
- OBKG / Physically Unclonable Function (PUF)
- Injection is straightforward

Trusted Execution Environment

TEE on RISC-V consists of following components,

1. Secure monitor which is extended with TEE related features.
2. TEE services which provide basic security capabilities, such as secure storage service，attestation service and cryptography service.
3. Secure enclaves, which run security-sensitive logic.
4. Untrusted components, which run untrusted operating system and untrusted apps.

- Memory protection
- Isolation of interrupt
- Secure storage
- Security of peripheral devices
- Provision and attestation of the device



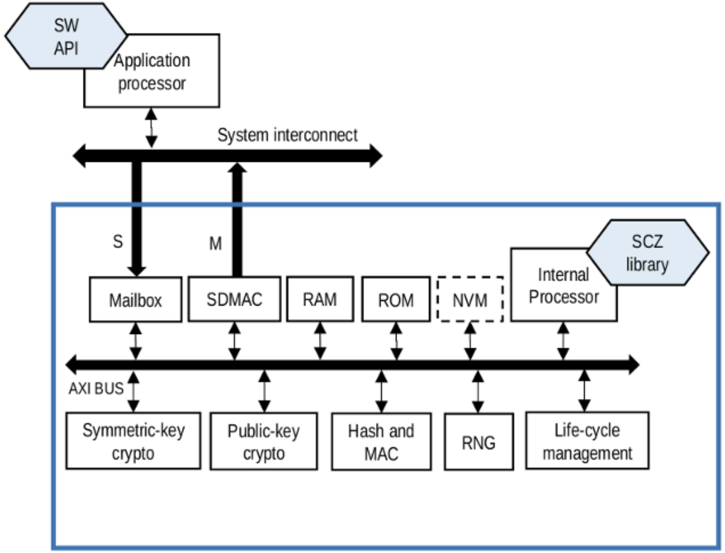
Section IV Architecture

Integrated Secure Elements

The iSE is an enclave, which is isolated from the host system

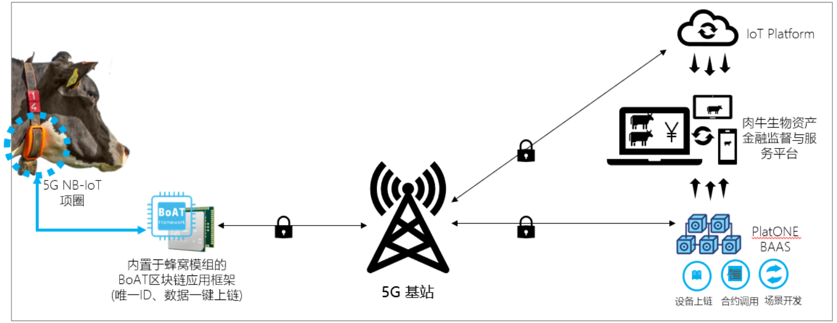
Internally, the iSE has some Non-Volatile Memory (NVM) storage for the keystore, the capability to generate keys with a Random Number Generation (RNG), and basic cryptographic primitives. In addition, it communicates with the host (data to encrypt/decrypt/sign/etc.) through a Secure Direct Memory Access 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.

- Platform integrity verification
- Key management and cryptographic services.
- (optionally) User management and mapping between roles and permissions.



Detailed Use Cases - Bio Tech

Bio Tech


IoT Platform
肉牛生物资产金融监督与服务平台
5G NB-IoT 项圈
BoAT Framework
内置于蜂窝模组的 BoAT区块链应用框架 (唯一ID、数据一键上链)
5G 基站
PlatONE BAAS
设备上链
合约调用
场景开发

Security Evaluation

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.

Section V Use Cases Implementation

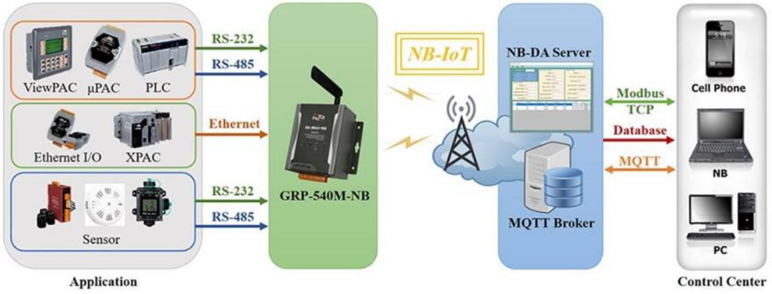
Detailed Use Cases - Gateway

Gateway

AI-based video analysis

Requirement of regulatory compliance (GDPR, PIPL)

Trusted Execution Environment

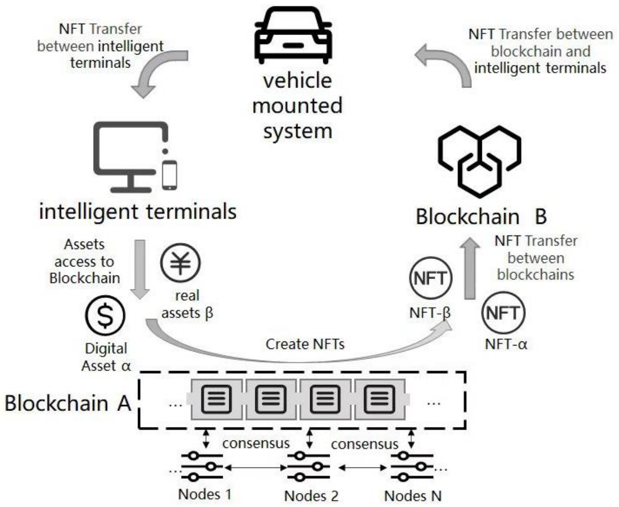


Security Evaluation

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.

Detailed Use Cases – Non-Fungible Token

Non-Fungible Token



Security Evaluation

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

Section V Use Cases Implementation

Detailed Use Cases - Carbon Neutralization

Carbon Neutralization

carbon emission monitoring

carbon emission reduction monitoring

Carbon emission trend analysis

Carbon neutralization rate

Carbon Tax measurement

Security Evaluation

Credible data collection site: Integrated on the chip of the IoT device. When the IoT device collects data, it will perform Hash calculation on the data and use the unique private key of the device to sign to generate the Data fingerprint of the piece of data. After the data is uploaded to the cloud, it can be verified by the hash and signature of the data fingerprint to check whether the data has been tampered with or whether it comes from an illegal device that is not recognized.

Trusted data source: This scheme generates a unique key pair and ID on the device. The private key cannot be obtained from the outside, and the private key signs the data hash on the IoT device to ensure that the data comes from the real and unique IoT device.

Time line for Next Step

- 。。。。

Thank You

RISC-V®