RISC-V Blockchain SIG meeting

2021-Dec - 07

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.

RISC-V®

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/

RISC-V®

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

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

Trusted RISC-V Architecture in Blockchain Infrastructure White Paper

Introduction to Blockchain

- Overview
- Infrastructure
- Challenges
- Value

Security Analysis

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

Architecture

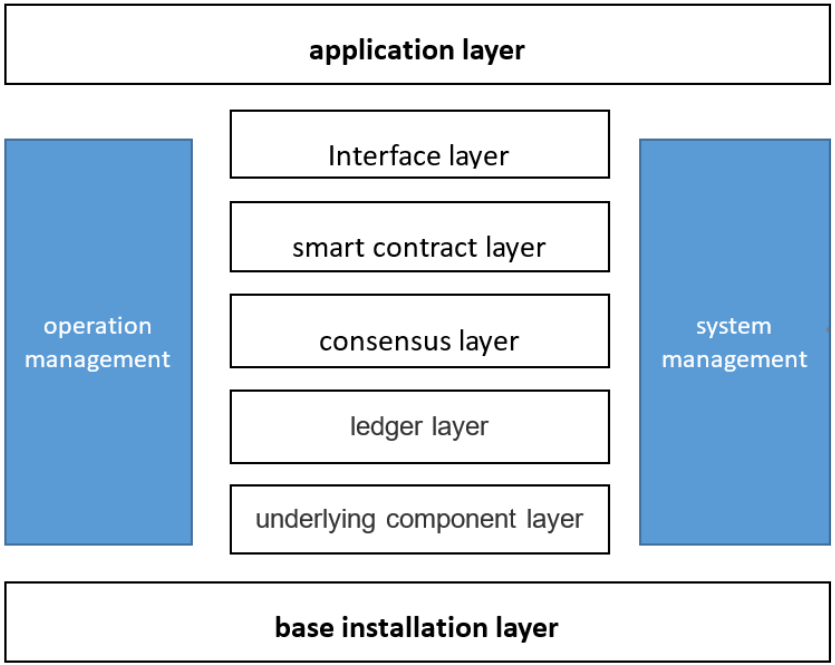
- Overview
- Root of Trust
- TEE
- Secure Elements

Use Cases Implementation

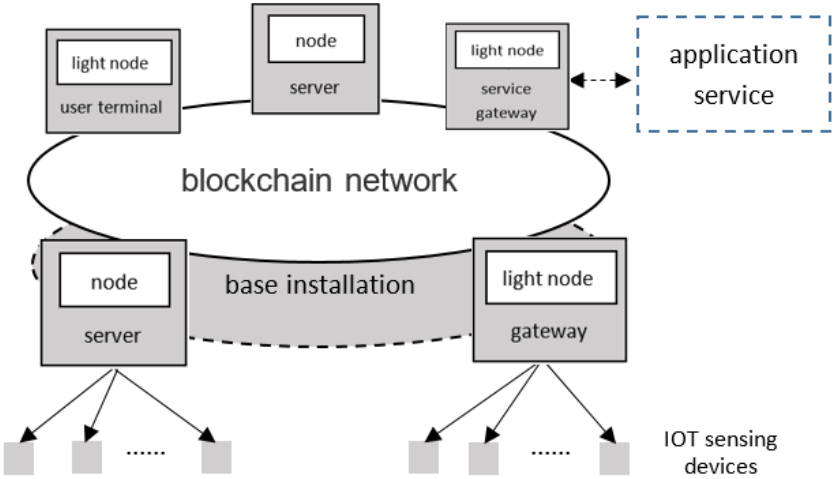
- Overview
- Bio Tech
- Gateway
- NFT

RISC-V®

Blockchain layers and network architecture



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.

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

Threat 1/5

Threat	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.

Threat 2/5

Threat	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 2 Security Analysis

Threat 3/5

Threat	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.

Threat 4/5

Threat	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.

Threat 5/5

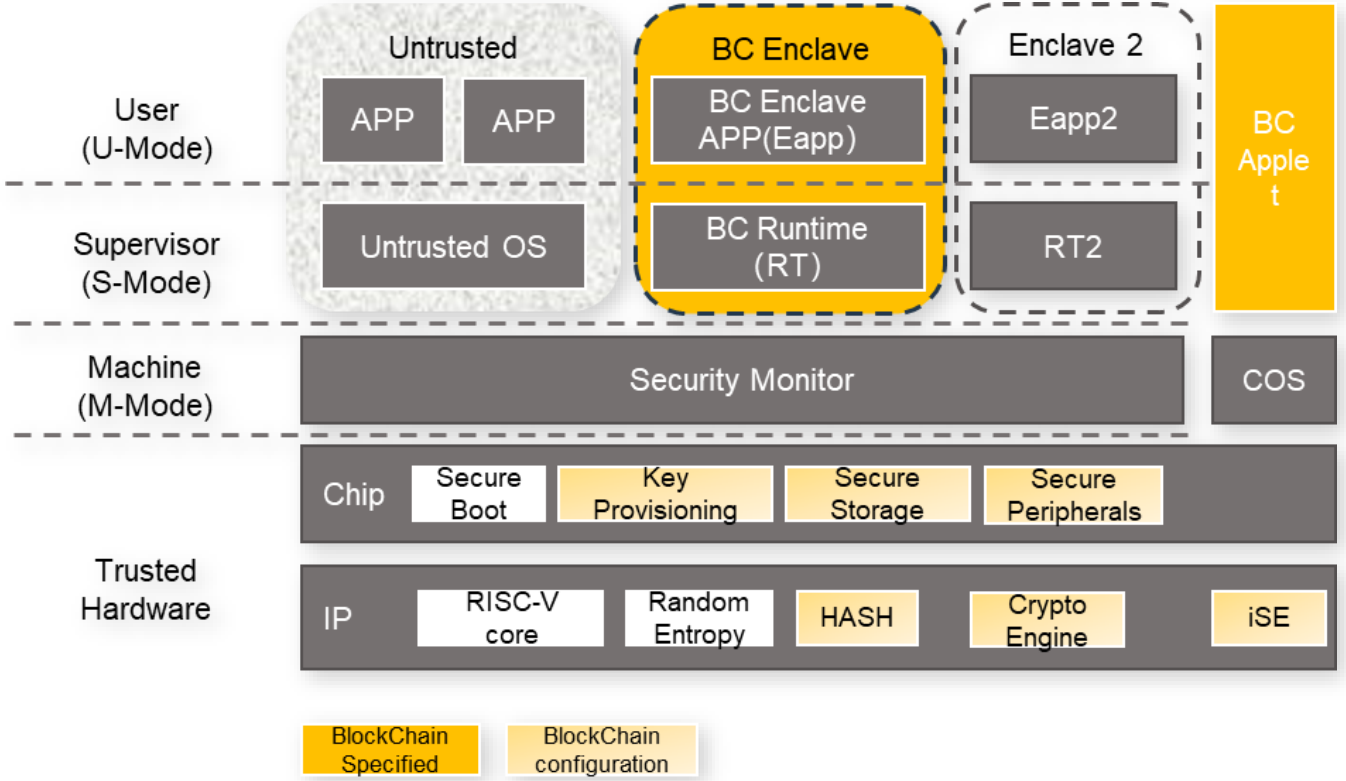
Threat	Description
Untrustworthy Node-Chain Seam	The cryptographic difference between what was intended by the participant, what happens in the node, and what happens on the chain must all be consistent. Architects should enforce a design such that the node is unable to modify a transaction (signing 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

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.
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.
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.

Section III Architecture

Trusted Architecture(reference)



Section III Architecture

Root of Trust

Platform integrity, both from physical and logical standpoints.

- First of all, 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 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

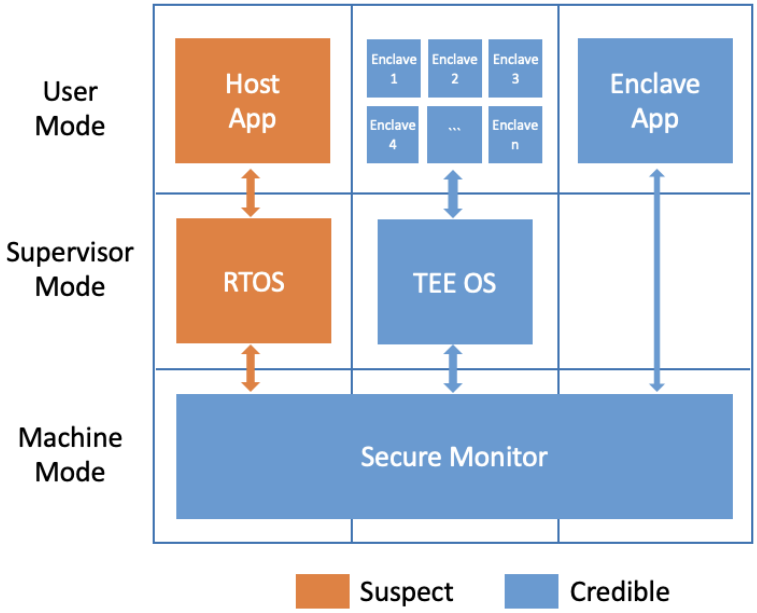
- OBKG / Physically Unclonable Function (PUF)
- Injection is straightforward

Section III Architecture

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 III Architecture

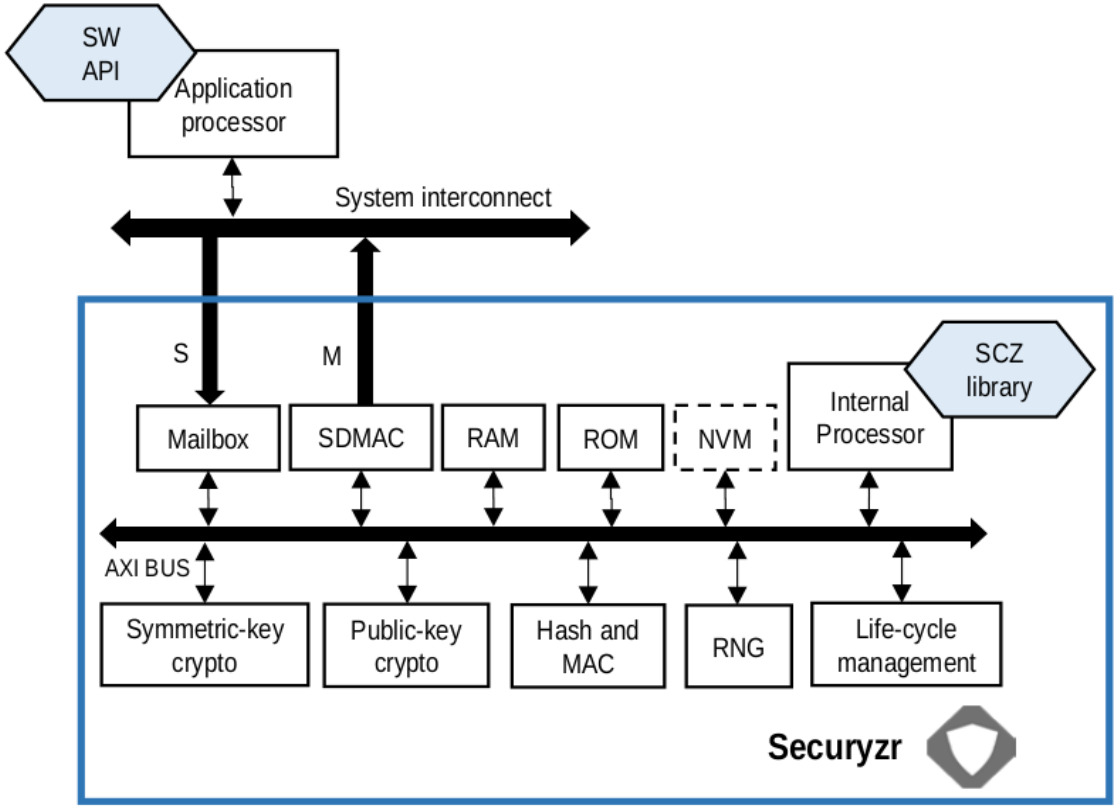
Integrated Secure Elements

Hardware

- The iSE is an enclave, isolated from the host system.
- The iSE has Non Volatile Memory (NVM) storage for the keystore, OBKG, Random Number Generation (RNG), and basic cryptographic primitives

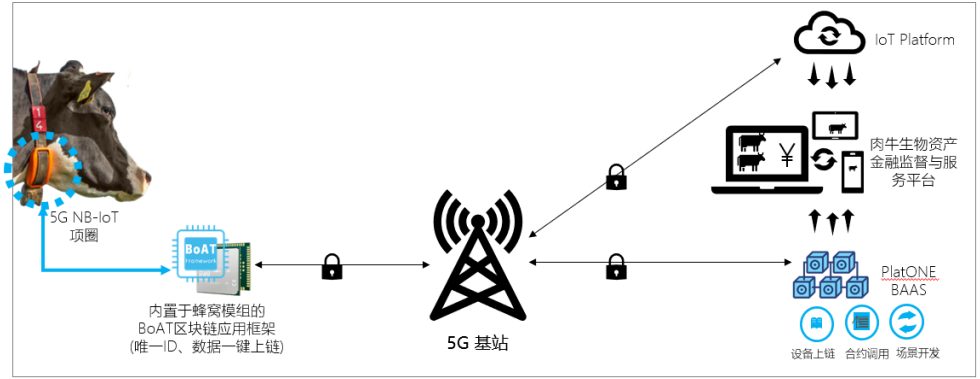
Software

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



Detailed Use Cases

Bio Tech



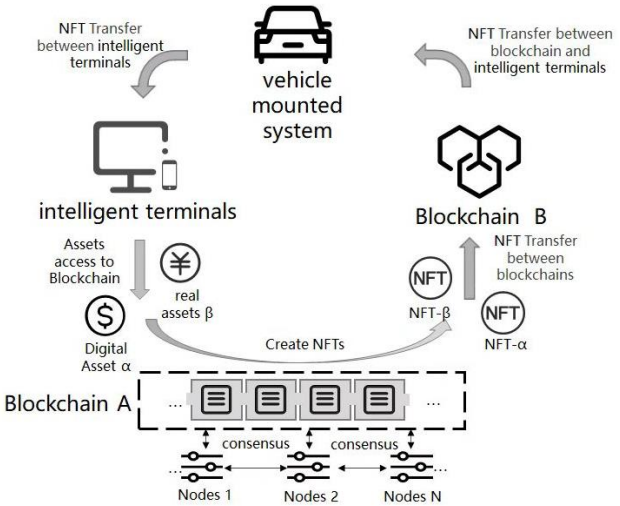
Gateway

AI-based video analysis

Requirement of regulatory compliance (GDPR, PIPL)

Trusted Execution Environment

Non-Fungible Token



Time line for Next Step

Document update - by 22nd Dec 2021

- Security Requirements
  - More input for Security Requirements
  - Mapping Threat vs. Security Requirements
- TEE & Integration SE
  - TEE & SE in Blockchain full picture
  - TEE & SE functions support for Blockchain
- Use case implementation

Thank You