RISC-V Blockchain SIG meeting

2021-Nov-2nd

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.

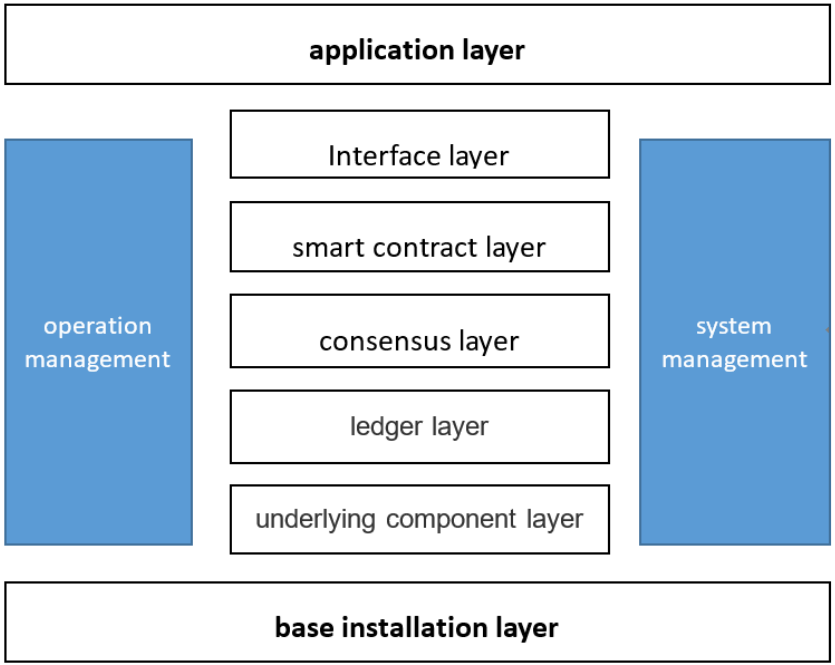
https://riscv.org/risc-v-international-community-code-of-conduct/

RISC-V®

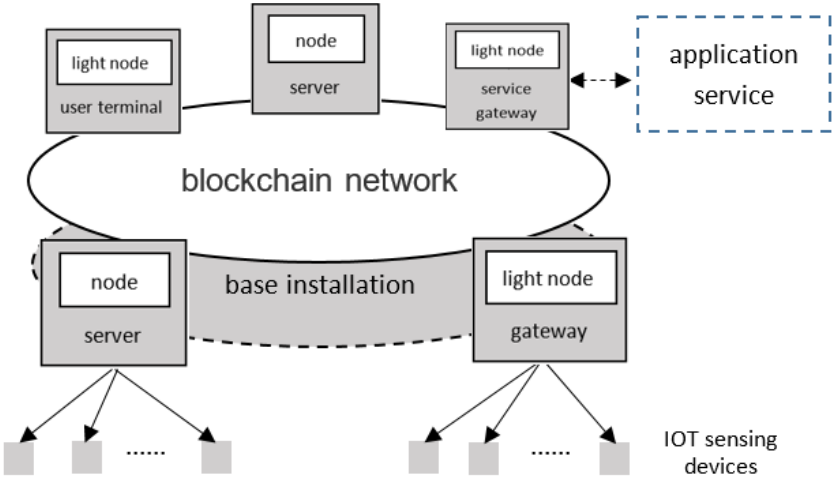
Conventions

- 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

Blockchain layers and network architecture



Blockchain *Technology* Architecture



Base installation Layer

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 gateway
- Blockchain full nodes
- Blockchain light node

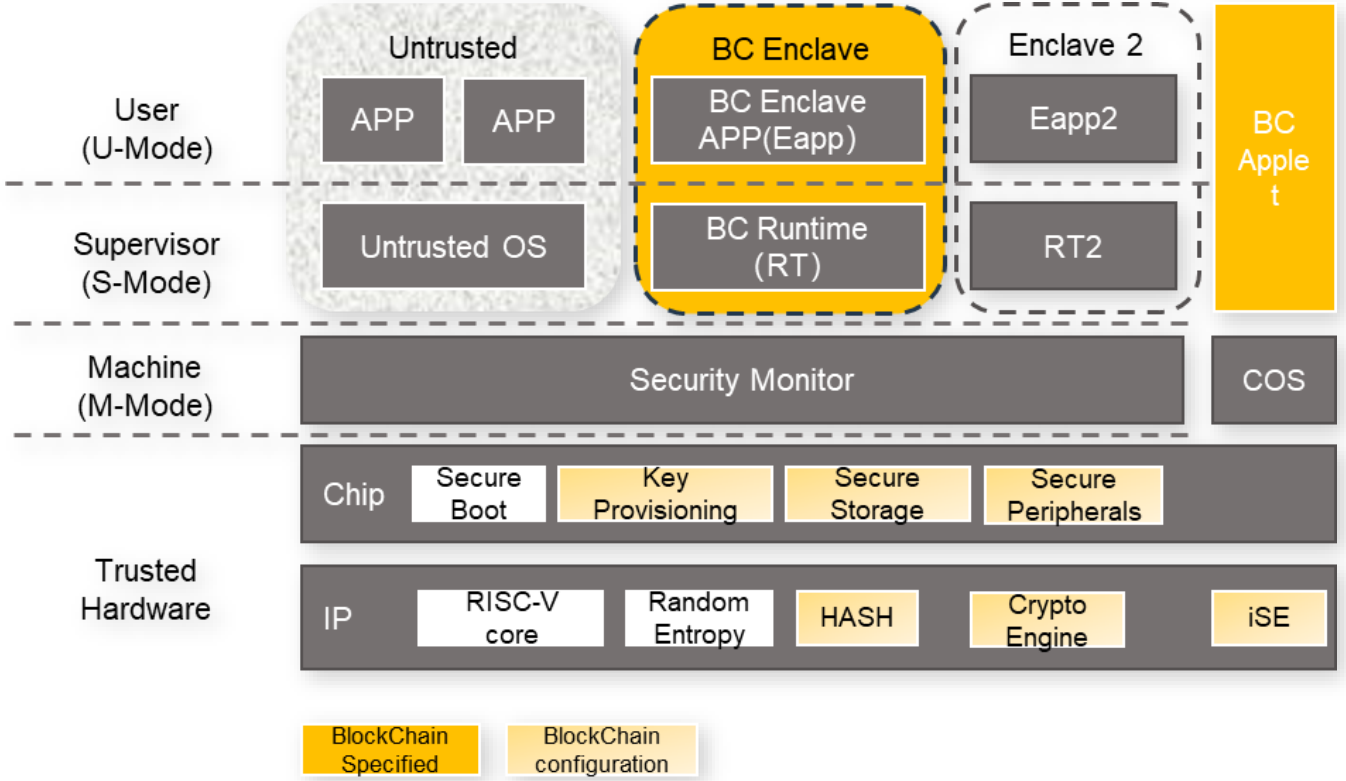
Key Assets

- Blockchian applications
- Blockchain accout keys
- Sensor data
- System Image
- Device configuration
- Logs
- Communication

Threat and Security Requirements

Threat	Security Requirements
Physical Attack	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.
Man-in-the-middle Attack	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.
Software Attack	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.

Trusted Architecture(reference)



TimeLine of next step

- One more week to gather data
- We'll have a draft document in two weeks.
- Review plan will be set later.
- White Paper document approval process need to be invented.

Thank You