RISC-V Blockchain SIG meeting

2021-Aug-10

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

Agenda for Today

1. Attendees' self-introductions.

2. Introduction of the blockchain SIG and the draft charter.

3. Brainstorming on strategy, current gaps between RISC-V and blockchain application etc.

RISC-V®

Attendees

Patty Tu, WXBC, Chair
Gary Xu, aitos, Vice Chair
Karl Weaver, aitos
Philipp Tomsich, software SIG chair
Marc Canel, Imagination
Jianming, Changhong Microsoft IoT center
John Pan, aitos
Kim McMahon (RISC-V specialist. Call for papers, Some are open.)
Mia Tang, aitos
Rachel, WXBC
Thomas Jin, WXBC
Tony Liu, aitos
Tobias Strauch, Germany, Munich
Vasan vs, IIT Madras, India
Wenlong Liu, aitos
Marvin Chen, WXBC

CHARTER

Why are We Here	What Do We Do	What Can We Provide
A Strategy integrates • Oversights for blockchain technology • Solutions in RISC-V architecture • Software ecosystem	✓ No gaps between RISC-V and blockchain ——— In ISA/software ✓ The performance and security ——— Meets/exceeds the industry expectation	SIG members : • Support the successful PoC development. • Engage and interact with other RISC-V committees if needed.

RISC-V®

Original Blockchain SIG Draft Charter(to be Updated)

- Blockchain SIG is proposed to develop a strategy and provide oversights for blockchain technology and solutions in RISC-V architecture and software ecosystem.

- The goals are to ensure there are no gaps in the ISA or software and it meets or exceeds industry expectation in performance and security. (e.g., privacy-preservation, cryptographic algorithms, trusted execution, data governance, data integrity and data provenance, etc.)

- In addition, the blockchain SIG will work with the implementation on horizontal committees to make sure someone in the community develops a RISC-V based PoC (Proof of Concept) to ensure the whole stack from hardware to software meets the goals.

- As with all groups, the SIG will engage and interact with other appropriate committees and groups.

RISC-V®

Our SIG Delivery (to be Updated)

2021 Aug. 10
First meeting

2021 Oct. 30
Draft Strategy

2021 Dec. 30
Reference system architecture

What we should finish
Members
Tasks splitting
Preparing works

What we should finish
Gap analysis
IC/Device/embedded software

What we should finish
Analysis of scenarios and security requirements
Implementation: POC
Customizable trusted architecture
TEE/Root of Trust/Combination with SE etc.

RISC-V®

Brainstorming

Blockchain experts:
  To provide blockchian scenarios and requirements.
   Security requirements and algorithms accelerator requirements
   ECDSA, Chinese SM2.

RISC-V experts:
  To analyze the requirements,
   with help from Crypto team, extensions, TEE team

Actions in next 2 weeks

1. To prepare blockchain application scenarios.

2. To prepare technical requirements of blockchain.

3. To share the above info and to have discussion with security, TEE team offline or in next

   SIG meeting in two weeks.

RISC-V®

Thank You

RISC-V®