RISC-V®

RISC-V Blockchain SIG meeting

2022-Jan- 24

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

● Mark Himelstein	RISC-V CTO
● Marc Canel	Imagination
● Stephano Cetola	RISC-V
● Patty Tu	WXBC, Chair
● Gary Xu	aitos, Vice Chair
● Huan Feng	aitos
● Yabo Rachel Zhang	WXBC
● Tom Liu	aitos
● Allen Shen	StarFive

Trusted RISC-V Architecture in Blockchain Infrastructure White Paper

Introduction to Blockchain

- Overview
- Infrastructure
- Challenges
- Value

The Cryptographic

- 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

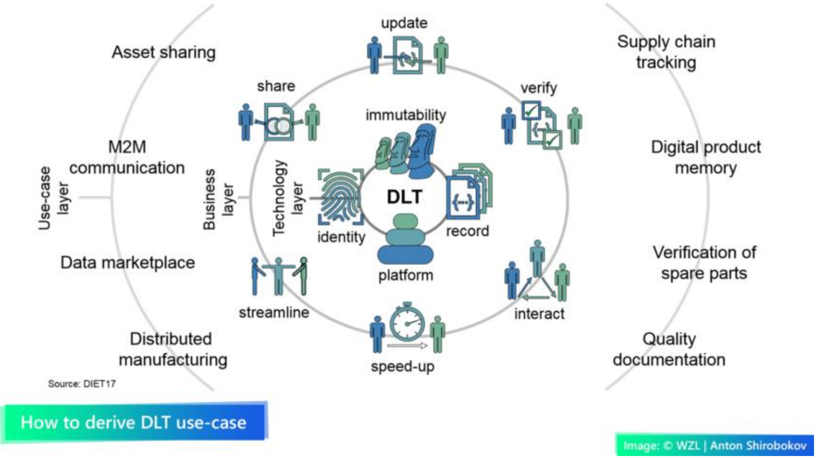
Use Cases Implementation

- Overview
- Bio Tech
- Gateway
- NFT

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.



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

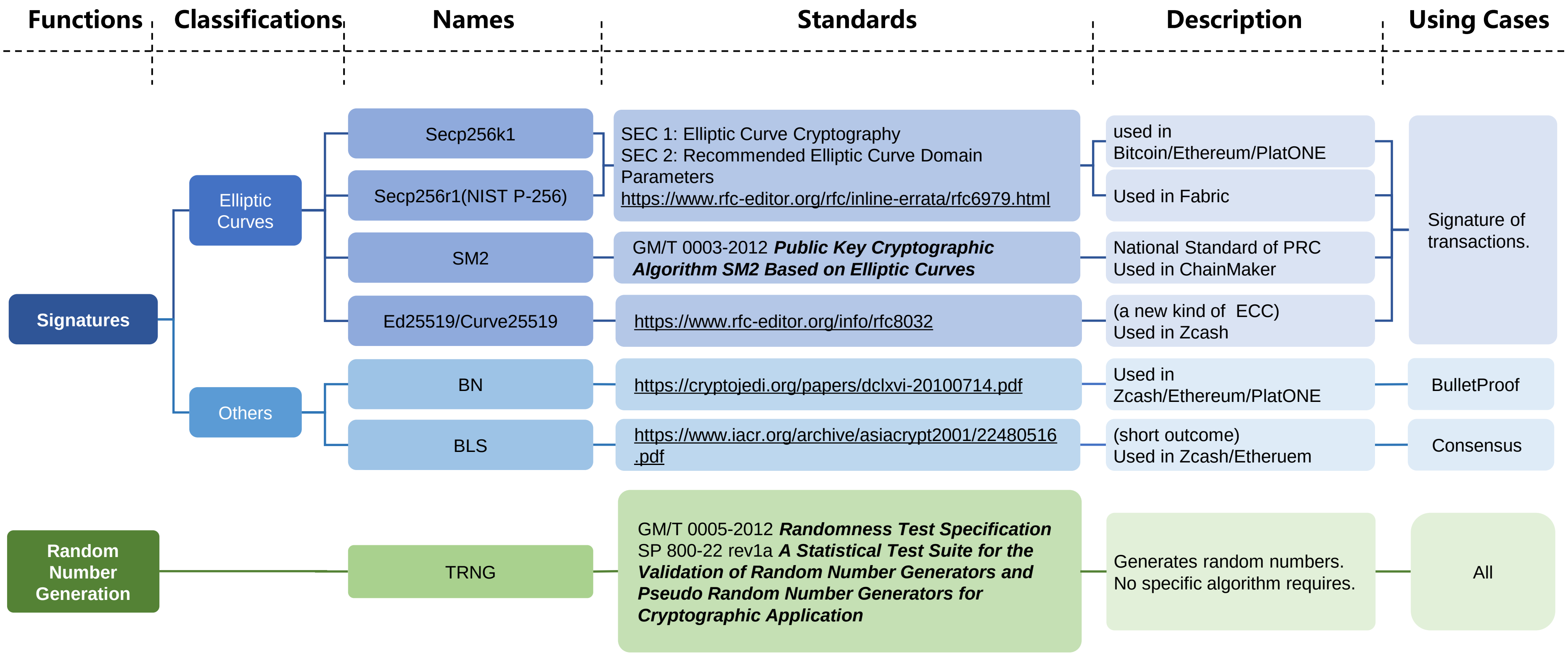
Security

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.

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***	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/Etherueum	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

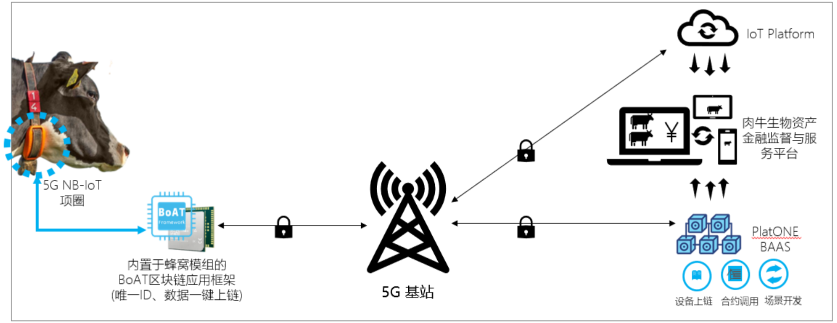
The Cryptographic Algorithms of Blockchain(2/2)

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***	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***	National Standard of PRC	

Section V Use Cases Implementation

Detailed Use Cases - Bio Tech

Bio Tech



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.

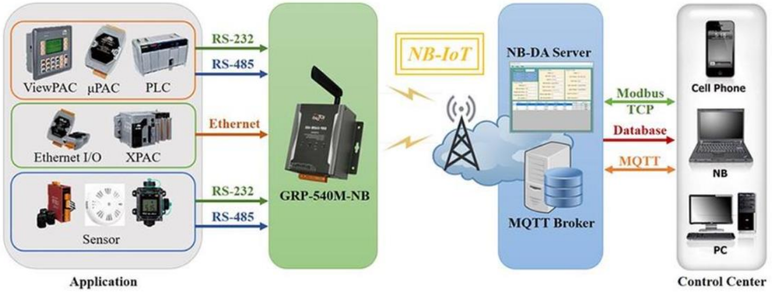
Detailed Use Cases - Gateway

Gateway

AI-based video analysis

Requirement of regulatory compliance (GDPR, PIPL)

Trusted Execution Environment

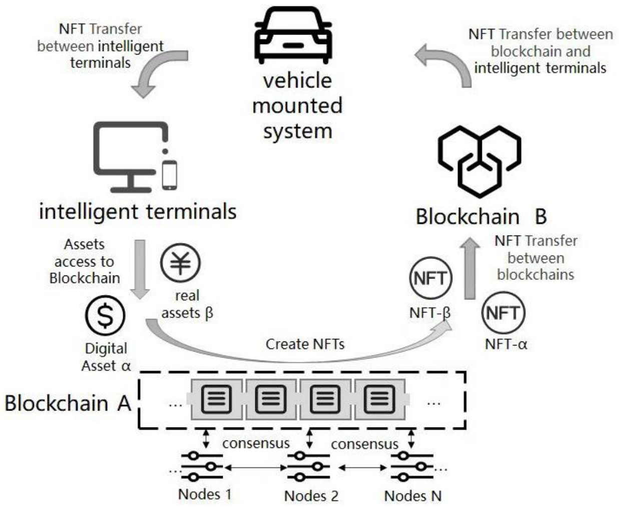


Security Evaluation

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

Time line for Next Step

- **Documentation review by tech chairs and security experts of RISC-V members**
- **Add carbon neutralization use case before next meeting**
- **Plan to finish before summer time**

Thank You

RISC-V®