Zero-Knowledge Proof Schemes for Lightweight IoT Devices in Permissioned Blockchain Networks

Nguyen Viet Hoa

Computer Communications Laboratory (CCL)
University of Aizu (UoA)

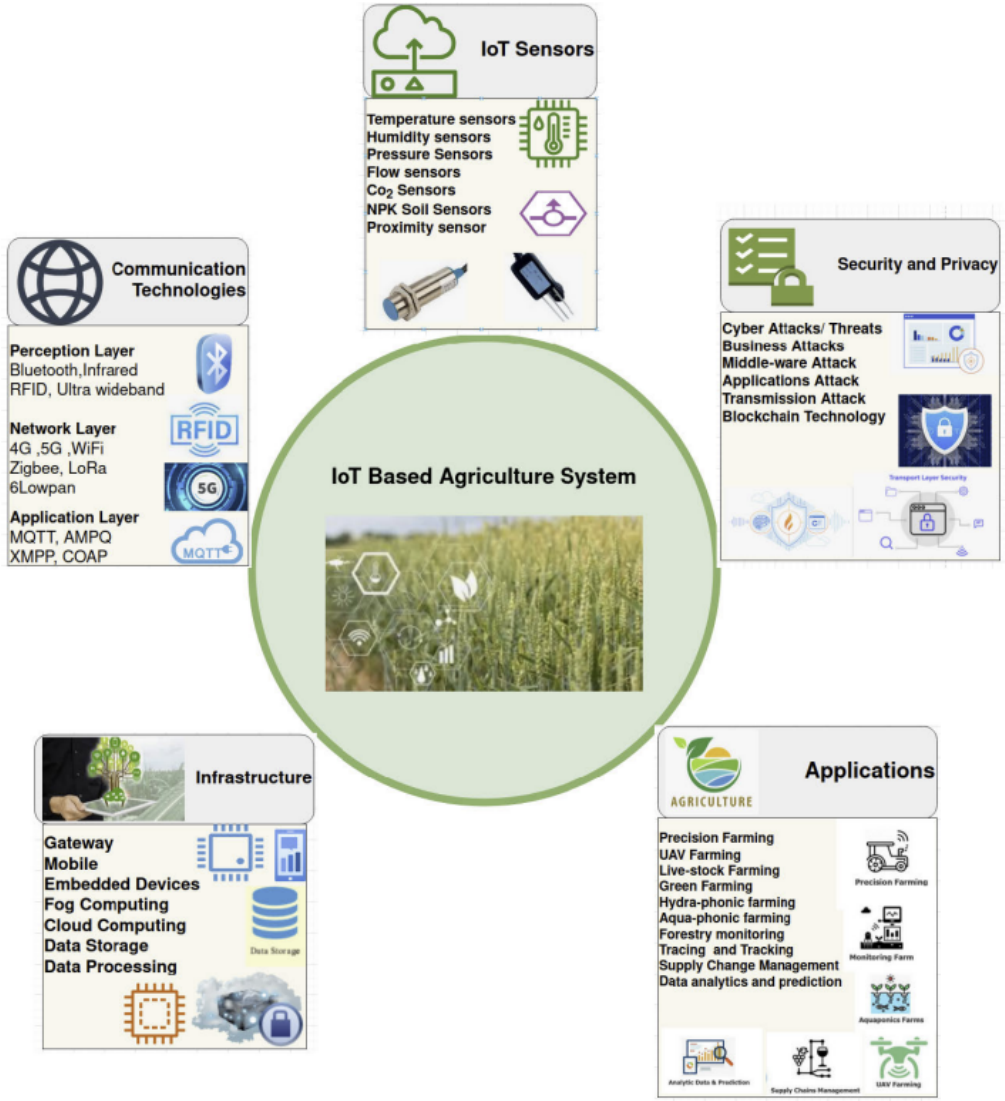
February 26, 2025

Agenda

1. Introduction
2. ZKPs as a Authentication Solution
3. Case Studies
4. Blockchain System Comparison
5. Technical Deep Dive
6. Performance in IoT Environments
7. Identifying Research Gaps
8. Conclusion

IoT Security Challenges

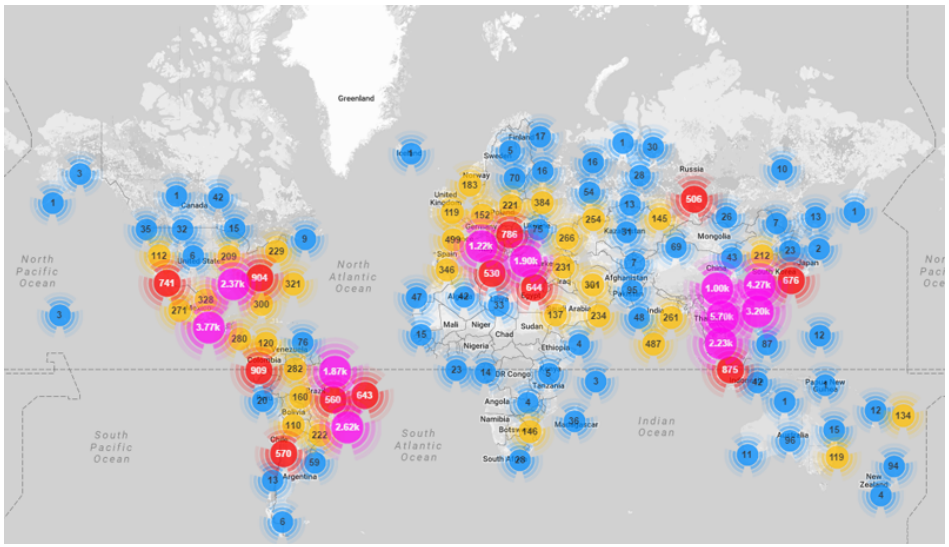
- The Internet of Things (IoT) is massive, forecast of over **75 billion** connected devices by 2025 (nccoe.nist.gov).
- Traditional methods often prove inadequate, especially as many devices are deployed in uncontrolled environments and can be **physically or remotely attacked**.
- A main issue is **poor/absent authentication** in IoT systems.



Taxonomy IoT based agriculture system.

Case Study: Mirai Botnet (2016)

- The Mirai botnet attack was a massive DDoS attack that affected millions of devices connected to IoT; simply by exploiting default passwords and trivial credentials (usenix.org).
- Exposed how easily malicious actors can hijack poorly secured "smart" cameras, routers, and sensors, using them in coordinated cyber-attacks.
- Underscored that conventional authentication (factory-set passwords/static keys) is not robust enough for IoT's scale.

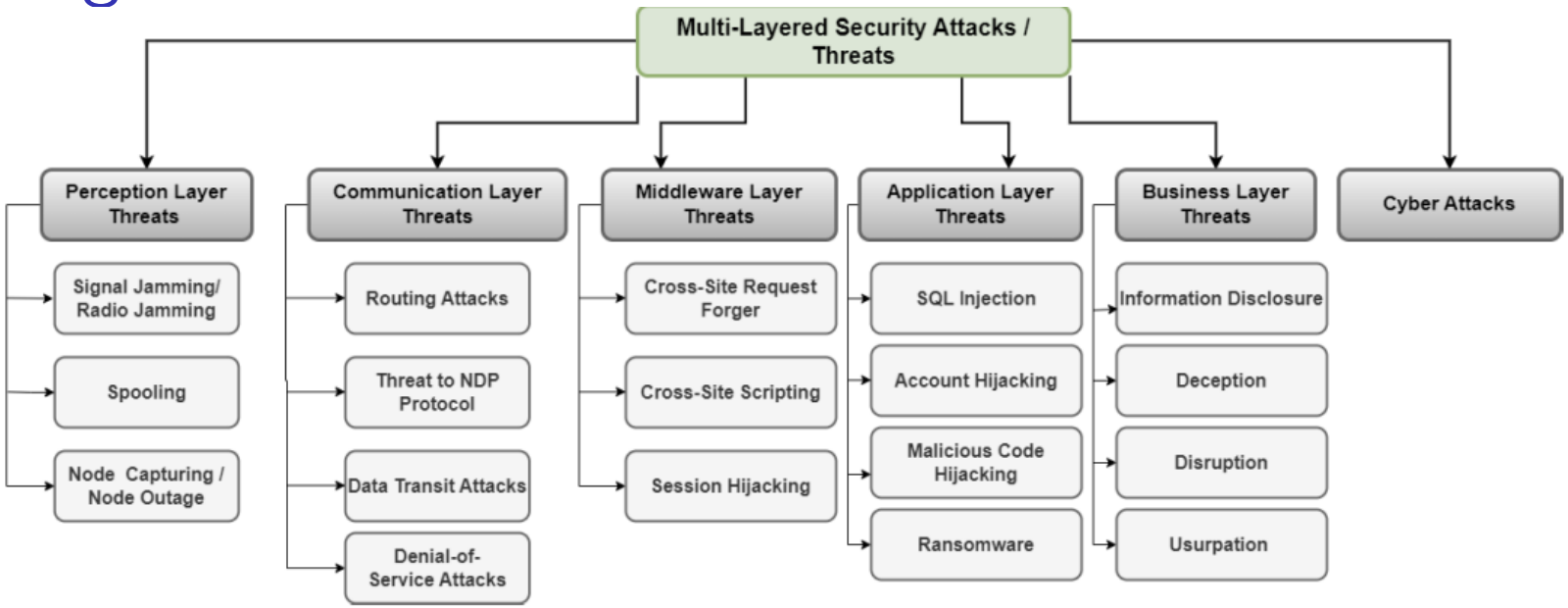


Attack Vector

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Device Hijacking

Challenges in Conventional IoT Authentication



Taxonomy of multi-layered security and privacy concerns in IoT

- Many IoT devices lack user interfaces for updating credentials.
- Centralized auth servers become points of failure in distributed ecosystems.
- Heavyweight cryptographic handshakes (e.g., full TLS with certificate verification) are impractical for resource-constrained devices.
- Manufacturers often resort to simpler, yet less secure, schemes to reduce computational load.
- **Conclusion:** IoT growth has outpaced current security measures
- **Solution:** A new authentication paradigms for IoT is needed

Zero-Knowledge Proofs (ZKPs)

Core Idea:

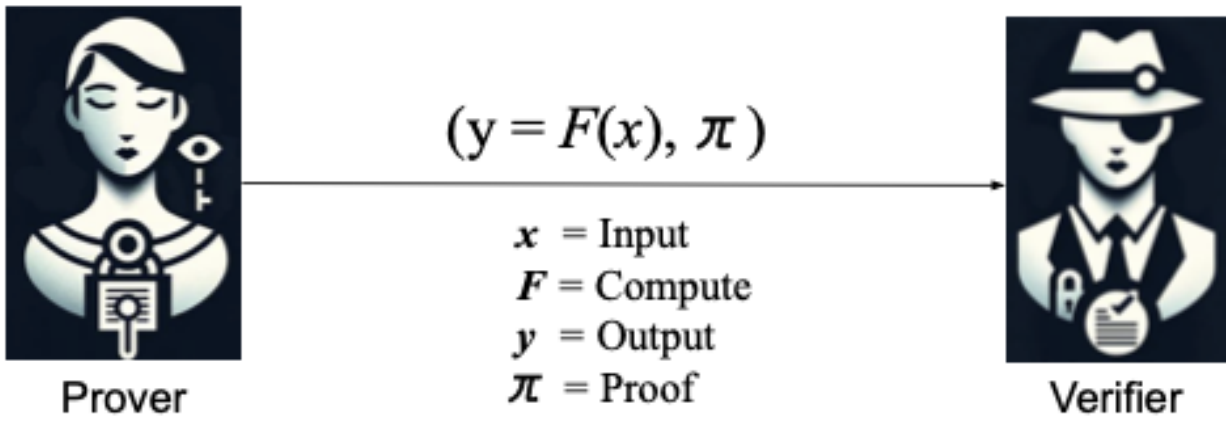
- Prover convinces verifier of a truth statement's *without* revealing secrets
- A device can prove private-key possession *without* disclosing it

Advantages:

- Immunity to replay attacks (since cannot reusable secrets)
- Privacy-preserving (no raw data or ID dispose)
- Non-interactive proofs reduce overhead

Result:

- Trust established *mathematically*
- Facilitates large-scale devices deployments



Key components of zero-knowledge proofs

ZKP Fundamentals: Interactive vs. Non-Interactive

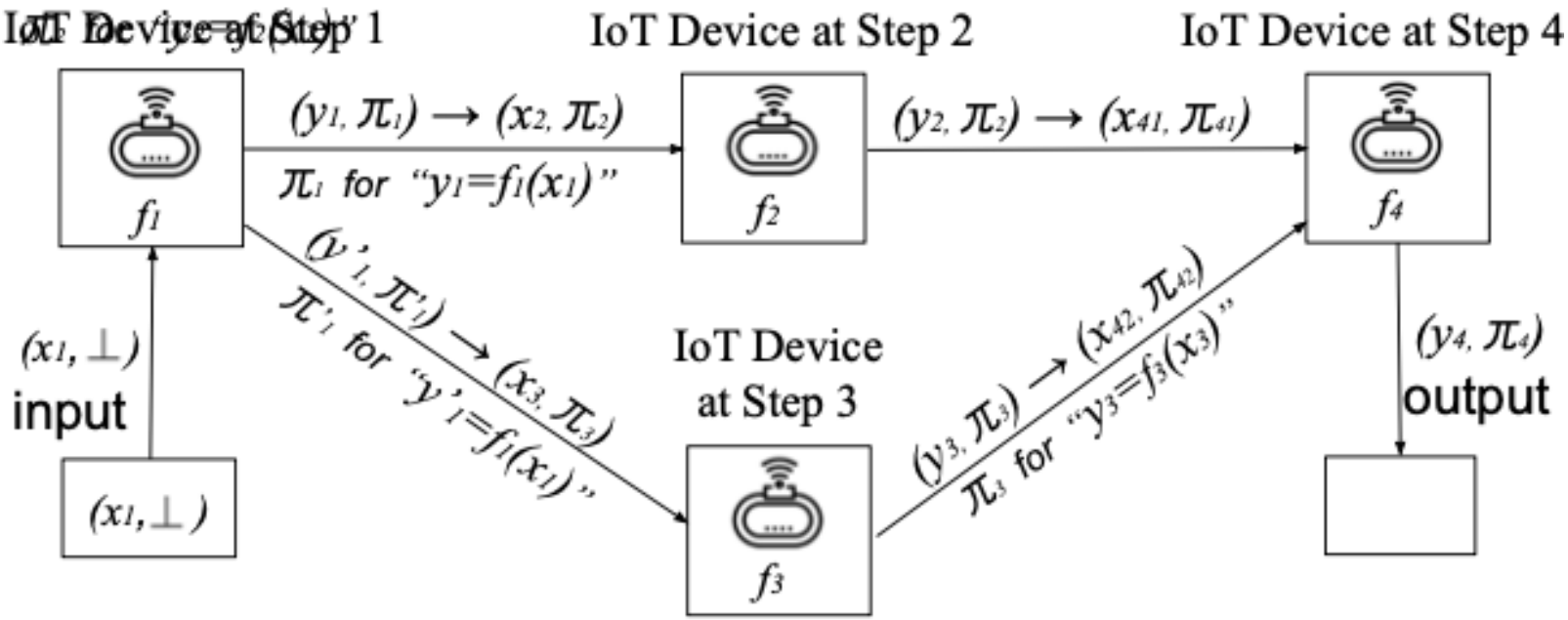
Interactive to Non-Interactive

- Early ZKPs were **interactive**: Prover & Verifier exchanged multiple messages.
- The **Fiat–Shamir** heuristic converts multi-round proofs into a single-message scheme.
- This is crucial for IoT with constrained bandwidth or sporadic connectivity (reduces round trips).

In IoT, non-interactive ZKPs (NIZKs) help reduce communication overhead, making them more practical for large-scale device authentication.

Type	**Rounds**	**Comm Overhead**	**IoT Fit**
Interactive	Multi	Higher	Limited
Non-Interactive	Single	Lower	Preferred

ZKPs as a IoT Authentication Solution



A sample IoT devices setup with ZKP

Why choosing ZKPs as a new solution to IoT authentication?

- IoT device can proves "X" *without* revealing secrets.
- Keeps sensitive data hidden.
- Minimizes communication overhead.
- Math-based proof replaces shared secrets, reducing the attack surface.

Real-World Applications

Military & Defense IoT:

- Sensors prove authenticity without revealing location

Critical Infrastructure:

- Smart meters: privacy-preserving billing proofs on blockchain

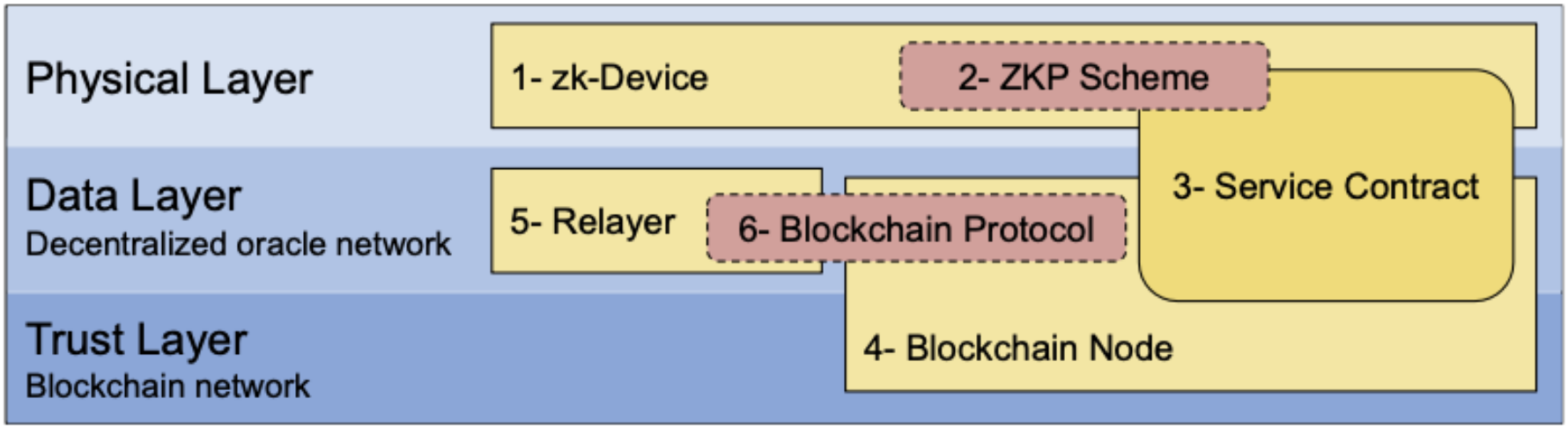
Supply Chains:

- Prove product origin/compliance w/o disclosing sensitive info

Blockchain in zk-IoT

	Permissionless	**Permissioned**
Membership	Open to public	Restricted
Throughput	Low (e.g., 7–30 TPS)	Higher (100+ TPS)
Fees	Usually required (gas)	Often zero or internal
ZKPs	More privacy & small proofs	Selective disclosure

Main Differences between Permissionless Blockchain vs. Permissioned



The main components of the zk-IoT framework

zk-IoT Communication on Blockchain Layers

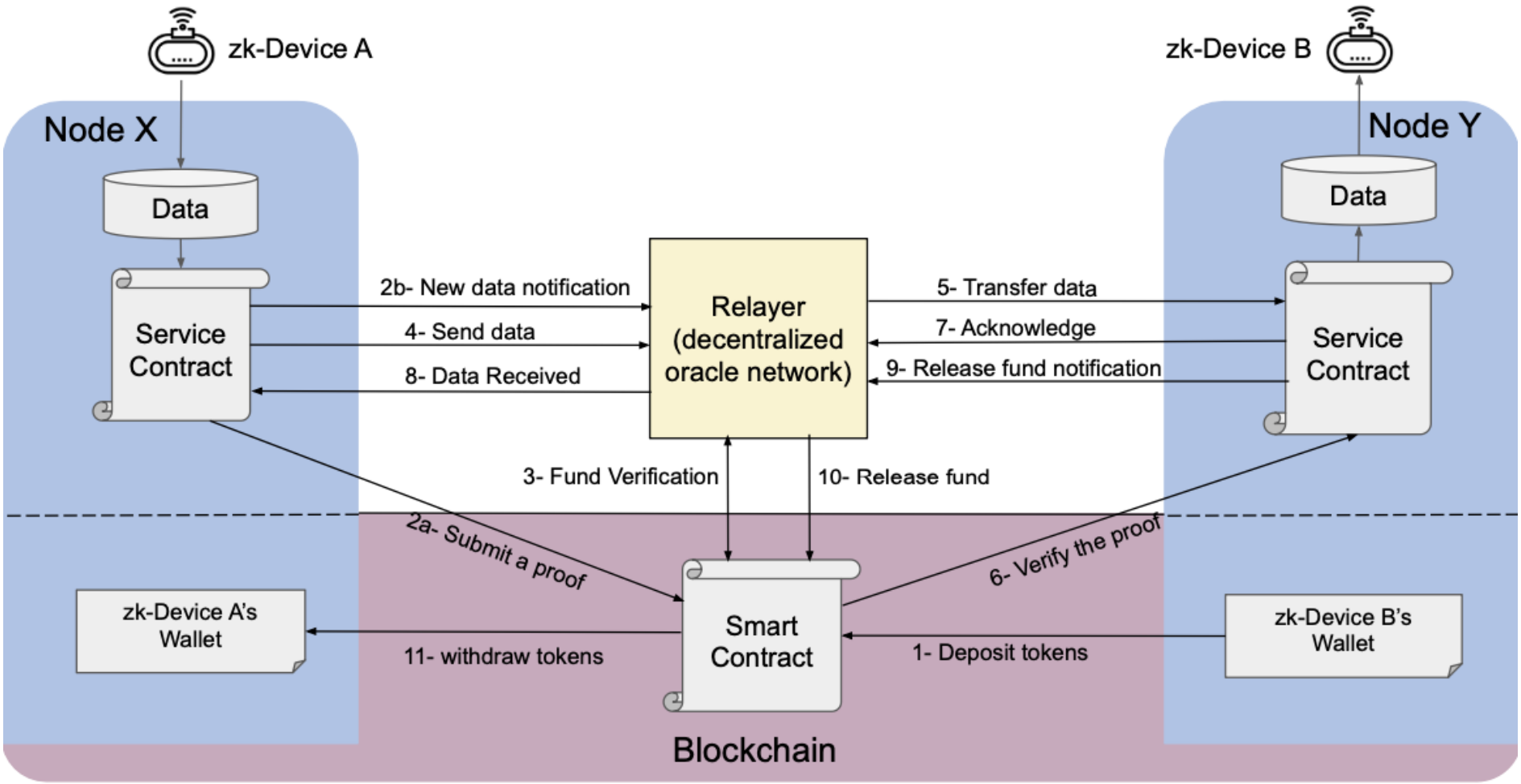


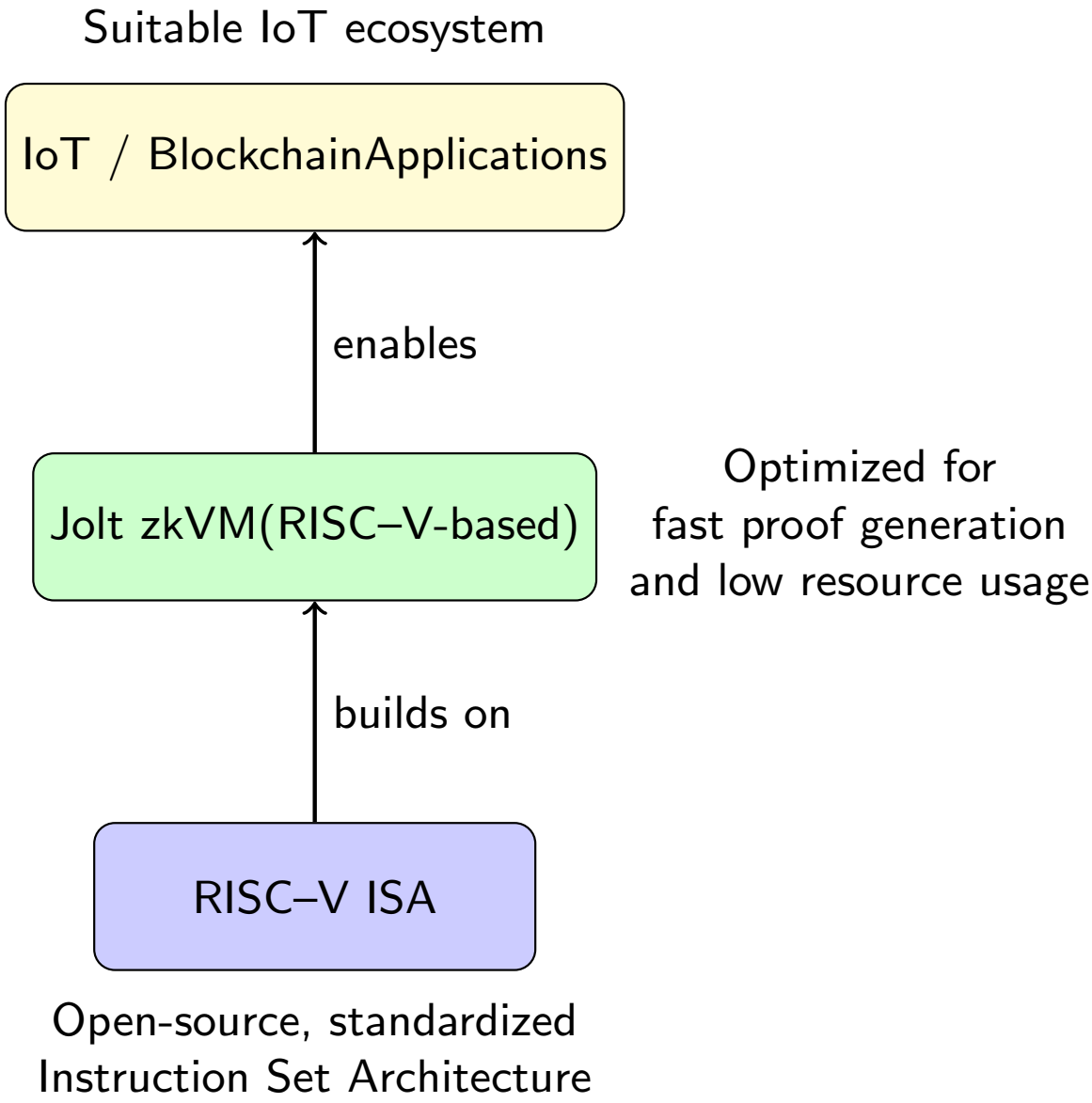
Illustration of zk-IoT communication across blockchain layers

ZKP Families & Comparative Metrics

Approach	Proof Size	Prover Cost	Verifier Cost	Setup
zk-SNARKs	$<$1 KB	High (heavy on RAM)	Very fast	Trusted
zk-STARKs	Tens of KB	High (parallelizable; memory intensive)	Slower	None; post-quantum
Bulletproofs	$\sim$2 KB	Moderate (sec on MCUs)	Moderate	None
Jolt zkVM	$<$1–few KB	Very fast (2–5$\times$ faster than other zkVM)	Extremely fast	Trusted

- SNARKs: Ideal for low-bandwidth; often requires outsourced proving
- STARKs: no trusted setup, but bigger proofs, suited for complex computations.
- Bulletproofs: good for smaller statements (e.g., range proofs).
- **Jolt zkVM: Jolt zkVM builds on SNARK principles; its setup is streamlined for R1SC-V applications. Therefore, fast, scalable and suitable for IoT system**

Jolt zkVM and R1SC-V Relationship



Challenges in Applying ZKPs to IoT

Computational Efficiency:

- Existing ZKP schemes are computationally heavy for IoT devices.
- Involve intensive math (modular arithmetic, FFTs, large transcript hashing).

Scalability:

- IoT networks can involve thousands of devices sending frequent proofs.
- Verification and network overhead can become bottlenecks.
- Distributed proof generation, batched/aggregated proofs, and recursive ZKPs is not widely investigate and everyday-applied

Blockchain Integration Challenges:

- Verification is limited (e.g., high gas costs on Ethereum).
- Storing numerous proofs may bloat the blockchain.
- Trusted setups (for zk-SNARKs) and a lack of standardized interfaces create integration gaps.

Proposed Solution & Main Contributions

Proposed Solution:

- Develop a new lightweight ZKP algorithm built on Jolt zkVM (leveraging RISC-V).

Main Contributions:

- A ZKP algorithm that specifically for IoT devices for small IoT devices.
- (Hopefully) Achievable fast proof generation and verification rate.
- Enhanced scalability for high-frequency IoT authentication.

Thank you for listenting
Q & A