Consensus-as-a-service

By Michael Chen – CMO @ Fantom

Short Introduction

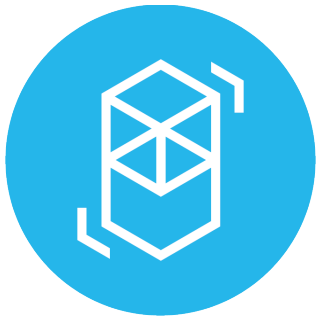
Zklux#1

Our research partners

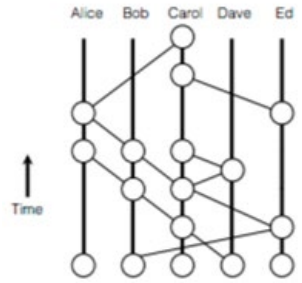
Our collaboration with Sikoba Research

- New Programming Language Toolchain
- Isekai, a verifiable computation project
- Token Economics

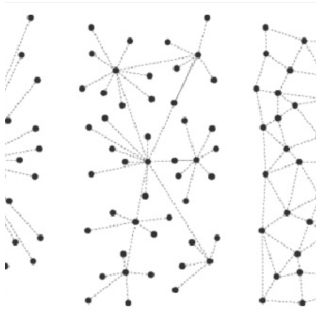
Fast Track Course on Fantom



Founded in 2018

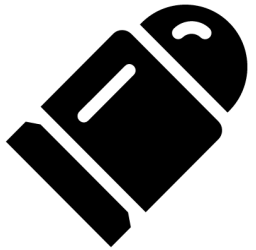


aBFT Consensus



Consensus-as-a-service

Interoperability



Bulletproofs

Bulletproofs

By Dmitry Khovratovich at Sikoba Research

Compared to ZK-snarks

It does not require a trusted setup as compared to ZK-SNARKs

Compatibility

It does not use pairings and works with any elliptic curve with a reasonably large subgroup size; the fastest elliptic curves such as Ristretto are supported.

Cost Scales Linearly

The verifier cost scales linearly with the computation size.

Bitcoin, Blockchain Bloat, and Monero.

Bulletproofs already being used in Monero.

Targets weakness for RingCT

RingCT scheme produces large range proof sizes.

Testing ground for Bitcoin

Being explored on the roadmap for Bitcoin

Before we move on.

We publish the work of our partners on our Medium and our Website

Go to https://fantom.foundation/developers