Construction

Let S

be a statement for which an easily verifiable cryptographic proof P

(e.g. SNARK/STARK) can be produced, but where P

takes a long time to generate (say, up to 1 hour). An “eventually-cryptographic” proof P'

is created by posting collateral vouching for the validity of S

and promising to deliver the cryptographic proof P

within 1 hour. If P

is not produced within 1 hour the collateral is burned.

A “weak prover” without the computational resources to produce P

fast enough can delegate production of P

to a “power prover”. In exchange for payment from the weak prover, the power prover also covers the collateral in case of failure to deliver P

.

Example: succint block witnesses

In the context of stateless clients, accessing state and history involves providing relatively heavy witnesses (Merkle paths). Individual witnesses in a block are batched to form a monolithic “block witness” which dominates the block size.

An eventually-cryptographic proof for witness validity can replace the large cryptographic proof (the block witness) with a constant-size constant-time proof. This would address the bandwidth overhead of stateless clients.

Discussion

Decentralised software has access to a suite of tools—ranging from mathematics to economics—to evaluate truthiness of statements:

- Mathematics

: For statements true by construction (think 256-bit arithmetic)

- Cryptography

: For statements showed true for all practical purposes because of physical limitations of computers (think ECDSA, SHA3, SNARKs/STARKs)

- Crypto-economics

: For statements convincingly true because of verifiable financial incentives (think TrueBit)

- Economics

: For statements signaled true through market dynamics (think prediction markets)

Eventual-cryptography fits in the above spectrum between crypto-economics and cryptography. Proofs start with crypto-economic strength (though without verifiers or fraud proofs) and finalise with cryptographic strength.

While the long-term promise of SNARKs/STARKs is to elevate many crypto-economic proofs to cryptographic strength, eventually-cryptographic proofs can fill the medium-term practicality gap of SNARKs/STARKs, in particular with regards to the time and computational resources to generate the proofs.