INPUT | OUTPUT

Cardano

An Overview

Our vision

Our vision is to enable a more democratic, equitable society, so *all* people have economic inclusion.

1.7 billion people in the world are unbanked and many are being denied financial services because their identities can't be verified – IO's vision is to solve this.

Our Approach

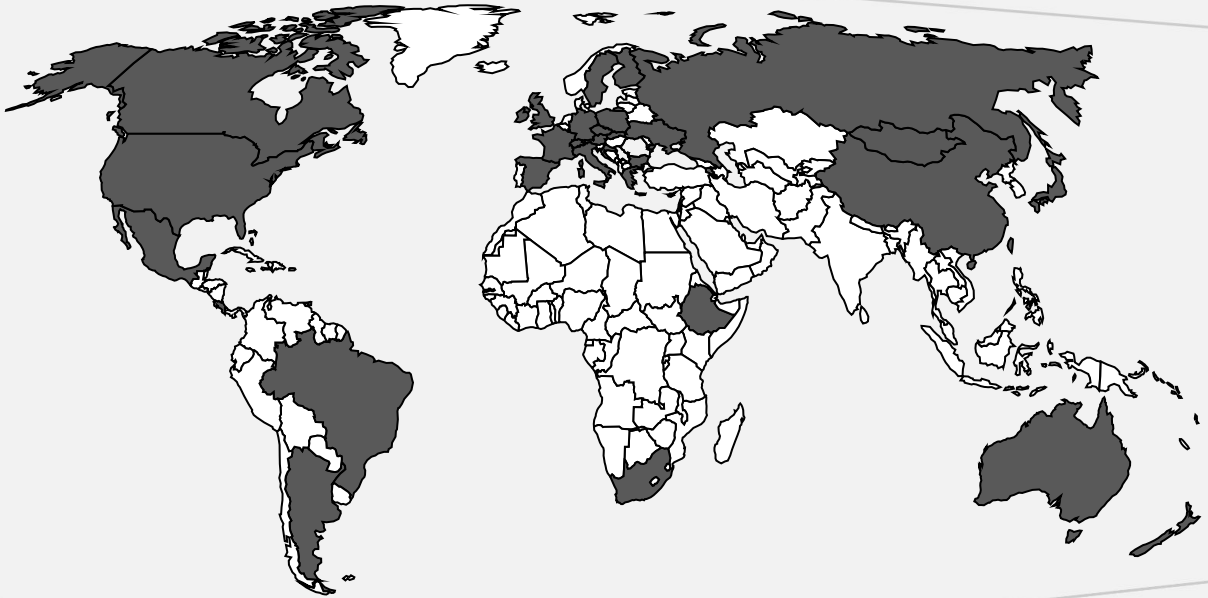
IO's approach and offerings are underpinned by fundamental science and research.

50 IO scientists at four universities have produced over 60 academic papers. Some of the most notable achievements include:

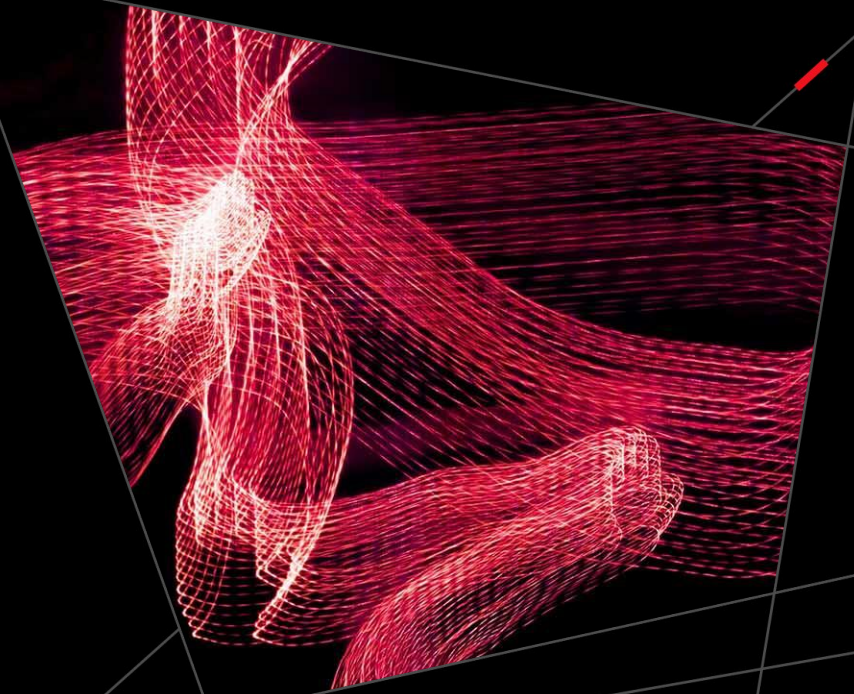
- **The first company to solve the Proof-of-Stake problem** and consequently...
- ...the development of a blockchain protocol which is **4 million times more energy-efficient than Bitcoin** (for comparison, Bitcoin's energy consumption equals Belgium while our developed platform, Cardano equals one household).
- A global scale financial system that is **100x more decentralized** than Bitcoin.
- **The first provably secure blockchain protocol**, paving the way for a highly secure financial network.
- The first research to apply the **rigor of functional programming languages** to the design of smart contracts.

Our footprint

- IO has over **200 employees** across **41 countries**.
- It is a decentralized company with no geographical restrictions.



A New Era – What is 3rd Generation Blockchain?



Blockchain generations

IO has developed Cardano, a third generation blockchain platform that overcomes the limitations of previous generations.

First generation – Bitcoin

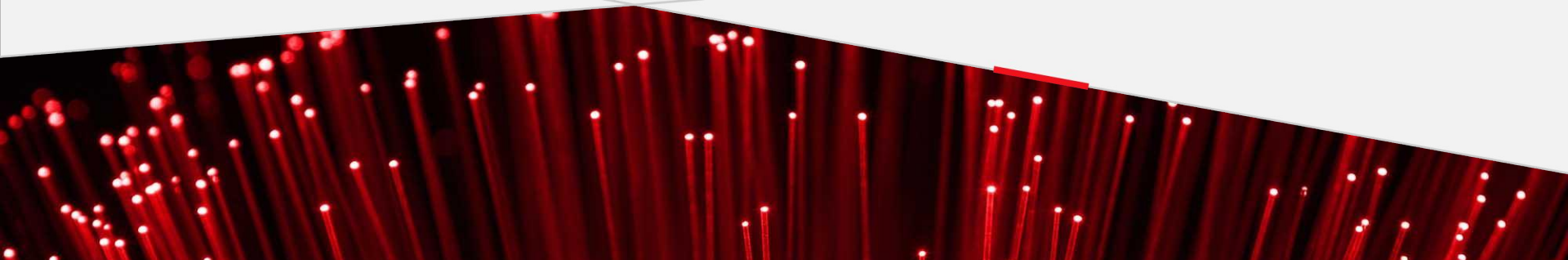
The age of digital currencies

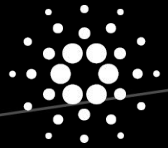
- **Enabled direct peer-to-peer transactions** – and was therefore revolutionary.
- **But it was limited** - it can only enable peer-to-peer financial exchange.

Second generation – Ethereum

The age of smart contracts

- **Enabled terms and conditions** – (or “smart contracts”) to be attached to peer-to-peer exchange.
- **But it was limited** – isn’t globally scalable and isn’t interoperable.





INPUT | OUTPUT

Third generation – Cardano

The age of real-life applications

Cardano has more advanced features than previous blockchain generations.

These advanced features have been made possible due to IO's approach, making it:

- **Scalable** - The ability to underpin all global commerce.
- **Interoperable** - Compatible with legacy financial systems as well as current, and future blockchain systems.
- **Sustainable** - Maintains itself and enables participants to govern it to ensure this sustainability.

INPUT | OUTPUT

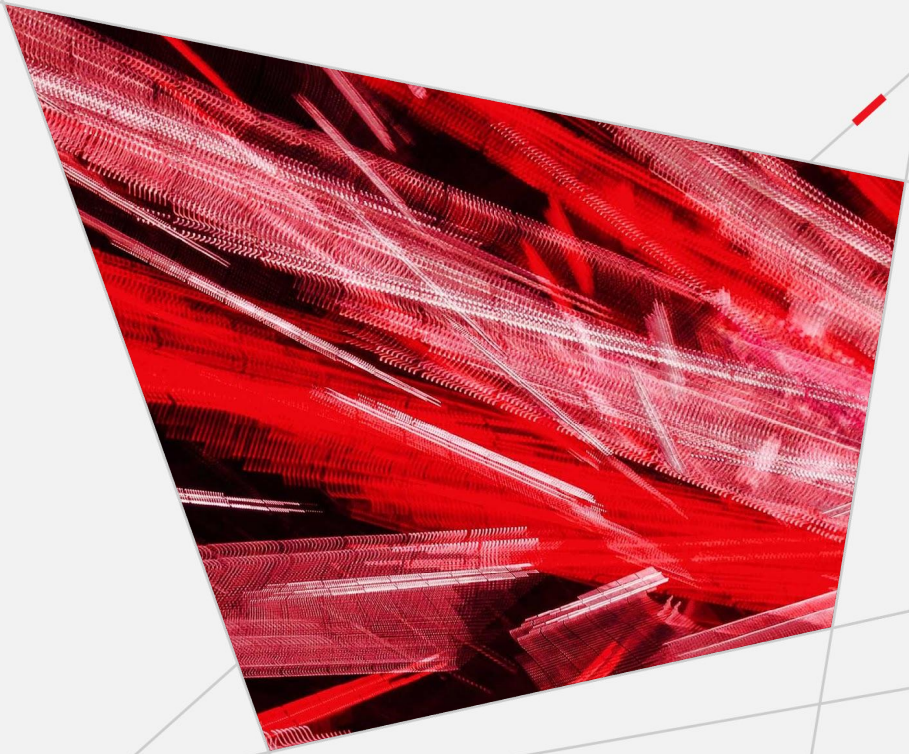
What else makes Cardano special?

- 100x more decentralized than Bitcoin.
- Underpinned by scientific rigor.
- World's first provably secure blockchain.
- Geographically diverse blockchain.
- Top 10 cryptocurrency.
- Interoperable with other blockchain and legacy systems.
- World's most environmentally sustainable blockchain solution .
- Home to ADA, leading Proof-of-Stake (POS) coin by market cap.
- World's first Proof-of-Stake blockchain.

CARDANO

Formal methods

Cardano engineers deploy *Formal Methods* to guarantee faithful translation of science into performant code.



From Mathematical Paper...

Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain

Bernardo David*, Peter Gaži**, Aggelos Kiayias***, and Alexander Russell†

October 6, 2017

Abstract. We present "Ouroboros Praos", a proof-of-sta
the first time, provides security against *fully-adaptive cor
setting*: Specifically, the adversary can corrupt any partic
population of stakeholders at any moment as long the st
an honest majority of stake; furthermore, the protocol tol
message delivery delay unknown to protocol participants.
To achieve these guarantees we formalize and realize in th
suitable form of forward secure digital signatures and a new
that maintains unpredictability under malicious key genera
a general combinatorial framework for the analysis of se
may be of independent interest. We prove our protocol sec
assumptions in the random oracle model.

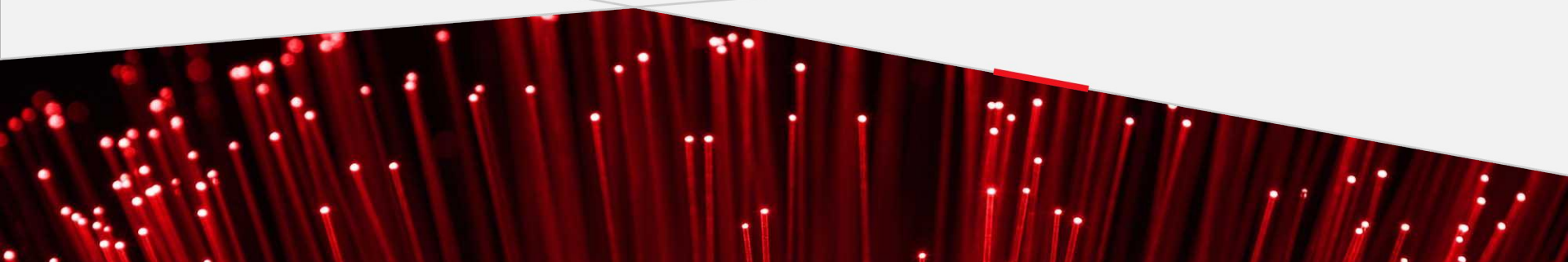
Protocol π_{SPoS}

The protocol π_{SPoS} is run by stakeholders $U_1, \ldots, U_n$ interacting among themselves and with ideal functionalities $\mathcal{F}_{\mathsf{INIT}}, \mathcal{F}_{\mathsf{VRF}}, \mathcal{F}_{\mathsf{KES}}, \mathcal{F}_{\mathsf{DSIG}}, \mathsf{H}$ over a sequence of slots $S = \{sl_1, \ldots, sl_R\}$. Define $T_i \triangleq 2^{\ell_{\mathsf{VRF}}} \phi_f(\alpha_i)$ as the threshold for a stakeholder U_i, where α_i is the relative stake of U_i, ℓ_{VRF} denotes the output length of $\mathcal{F}_{\mathsf{VRF}}$, f is the active slots coefficient and ϕ_f is the mapping from Definition 1. Then π_{SPoS} proceeds as follows:

1. **Initialization.** The stakeholder U_i sends $(\mathsf{KeyGen}, sid, U_i)$ to $\mathcal{F}_{\mathsf{VRF}}$, $\mathcal{F}_{\mathsf{KES}}$ and $\mathcal{F}_{\mathsf{DSIG}}$; receiving $(\mathsf{VerificationKey}, sid, v_i^{vrf})$, $(\mathsf{VerificationKey}, sid, v_i^{kes})$ and $(\mathsf{VerificationKey}, sid, v_i^{dsig})$, respectively. Then, in case it is the first round, it sends $(\mathsf{ver\_keys}, sid, U_i, v_i^{vrf}, v_i^{kes}, v_i^{dsig})$ to $\mathcal{F}_{\mathsf{INIT}}$ (to claim stake from the genesis block). In any case, it terminates the round by returning $(U_i, v_i^{vrf}, v_i^{kes}, v_i^{dsig})$ to $\mathcal{Z}$. In the next round, U_i sends $(\mathsf{genblock\_req}, sid, U_i)$ to $\mathcal{F}_{\mathsf{INIT}}$, receiving $(\mathsf{genblock}, sid, \mathcal{S}_0, \eta)$ as the answer. U_i sets the local blockchain $\mathcal{C} = B_0 = (\mathcal{S}_0, \eta)$ and its initial internal state $st = H(B_0)$.
2. **Chain Extension.** After initialization, for every slot $sl_j \in S$, every online stakeholder U_i performs the following steps:
   (a) U_i receives from the environment the transaction data $d \in \{0,1\}^*$ to be inserted into the blockchain.
   (b) U_i collects all valid chains received via diffusion into a set $\mathbb{C}$, pruning blocks belonging to future slots and verifying that for every chain $\mathcal{C}' \in \mathbb{C}$ and every block $B' = (st', d', sl', B_\pi', \sigma_{j'}) \in \mathcal{C}'$ it holds that the stakeholder who created it is in the slot leader set of slot sl' (by parsing B_π' as (U_s, y', π') for some s, verifying that $\mathcal{F}_{\mathsf{VRF}}$ responds to $(\mathsf{Verify}, sid, \eta \| sl', y', \pi', v_s^{vrf})$ by $(\mathsf{Verified}, sid, \eta \| sl', y', \pi', 1)$, and that $y' < T_s$), and that $\mathcal{F}_{\mathsf{KES}}$ responds to $(\mathsf{Verify}, sid, (st', d', sl', B_\pi'), sl', \sigma_{j'}, v_s^{kes})$ by $(\mathsf{Verified}, sid, (st', d', sl', B_\pi'), sl', 1)$. U_i computes $\mathcal{C}' = \mathsf{maxvalid}(\mathcal{C}, \mathbb{C})$, sets $\mathcal{C}'$ as the new local chain and sets state $st = H(\mathrm{head}(\mathcal{C}'))$.
   (c) U_i sends $(\mathsf{EvalProve}, sid, \eta \| sl_j)$ to $\mathcal{F}_{\mathsf{VRF}}$, receiving $(\mathsf{Evaluated}, sid, y, \pi)$. U_i checks whether it is in the slot leader set of slot sl_j by checking that $y < T_i$. If yes, it generates a new block $B = (st, d, sl_j, B_\pi, \sigma)$ where st is its current state, $d \in \{0,1\}^*$ is the transaction data, $B_\pi = (U_i, y, \pi)$ and σ is a signature obtained by sending $(\mathsf{USign}, sid, U_i, (st, d, sl_j, B_\pi), sl_j)$ to $\mathcal{F}_{\mathsf{KES}}$ and receiving $(\mathsf{Signature}, sid, (st, d, sl_j, B_\pi), sl_j, \sigma)$. U_i computes $\mathcal{C}' = \mathcal{C} \lfloor B$, sets $\mathcal{C}'$ as the new local chain and sets state $st = H(\mathrm{head}(\mathcal{C}'))$. Finally, if U_i has generated a block in this step, it diffuses $\mathcal{C}'$.
3. **Signing Transactions.** Upon receiving $(\mathsf{sign\_tx}, sid', tx)$ from the environment, U_i sends $(\mathsf{Sign}, sid, U_i, tx)$ to $\mathcal{F}_{\mathsf{DSIG}}$, receiving $(\mathsf{Signature}, sid, tx, \sigma)$. Then, U_i sends $(\mathsf{signed\_tx}, sid', tx, \sigma)$ back to the environment.

Fig. 4: Protocol π_{SPoS}.

- Written in English.
- Written by Mathematicians.
- Very abstract.

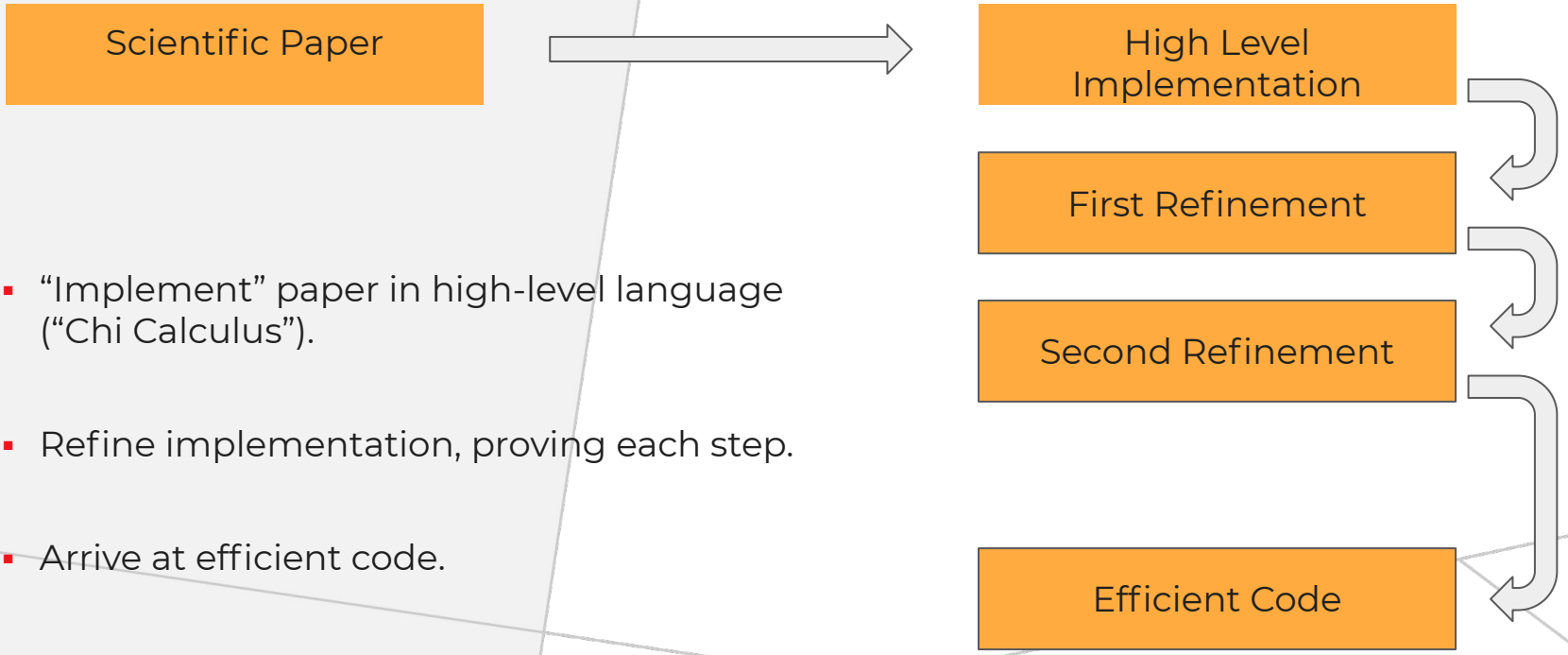


...To Efficient Code

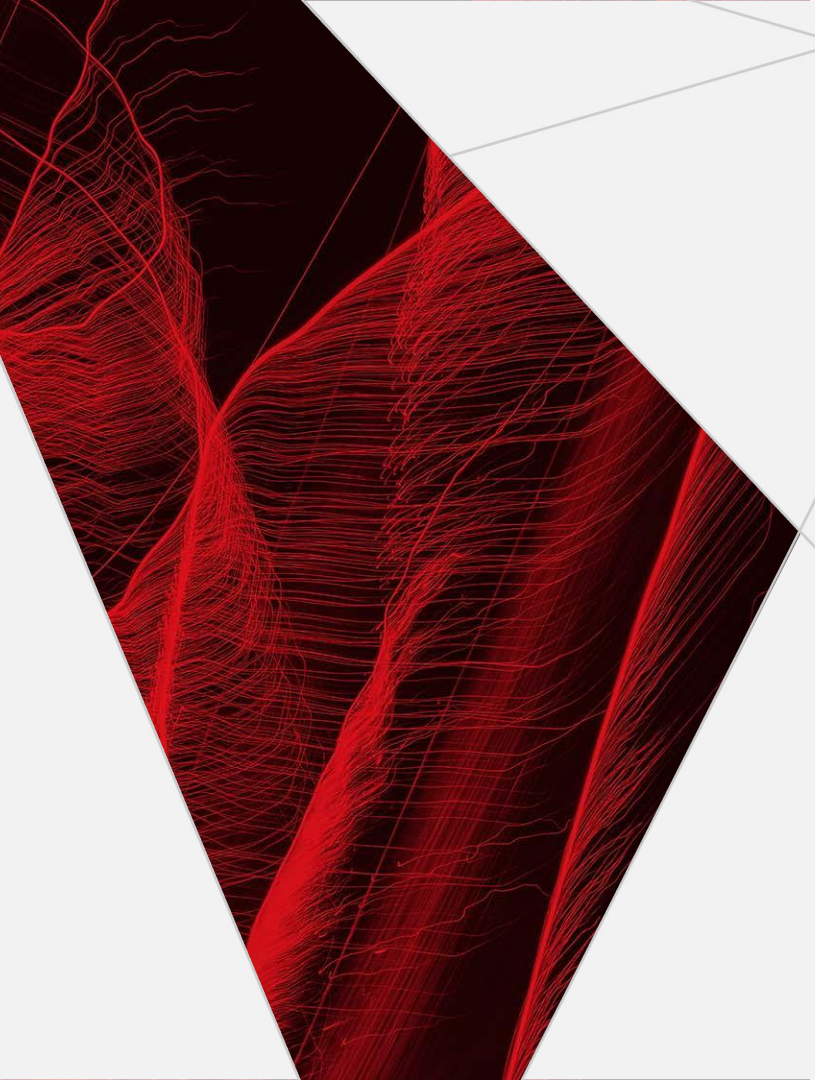
- Written in Haskell.
- Written by Software Engineers.
- Efficient code.

```haskell
-- CHECK: @verifyEncShare
-- | Verify encrypted shares
verifyEncShares
    :: MonadRandom m
    => SecretProof
    -> Scrape.Threshold
    -> [(VssPublicKey, EncShare)]
    -> m Bool
verifyEncShares SecretProof{..} threshold (sortWith fst -> pairs)
    | threshold <= 1     = error "verifyEncShares: threshold must be > 1"
    | threshold >= n - 1 = error "verifyEncShares: threshold must be < n-1"
    | otherwise =
          Scrape.verifyEncryptedShares
              spExtraGen
              threshold
              spCommitments
              spParallelProofs
              (coerce $ map snd pairs)  -- shares
              (coerce $ map fst pairs)  -- participants
  where
    n = fromIntegral (length pairs)
```

The Solution: Formal Methods



- “Implement” paper in high-level language (“Chi Calculus”).
- Refine implementation, proving each step.
- Arrive at efficient code.

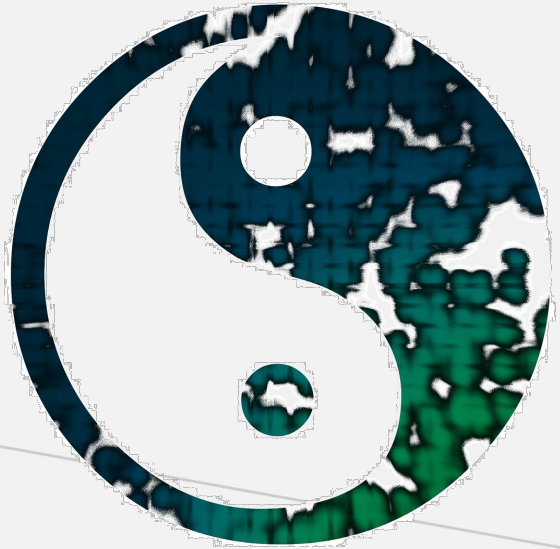


INPUT | OUTPUT

Decentralization

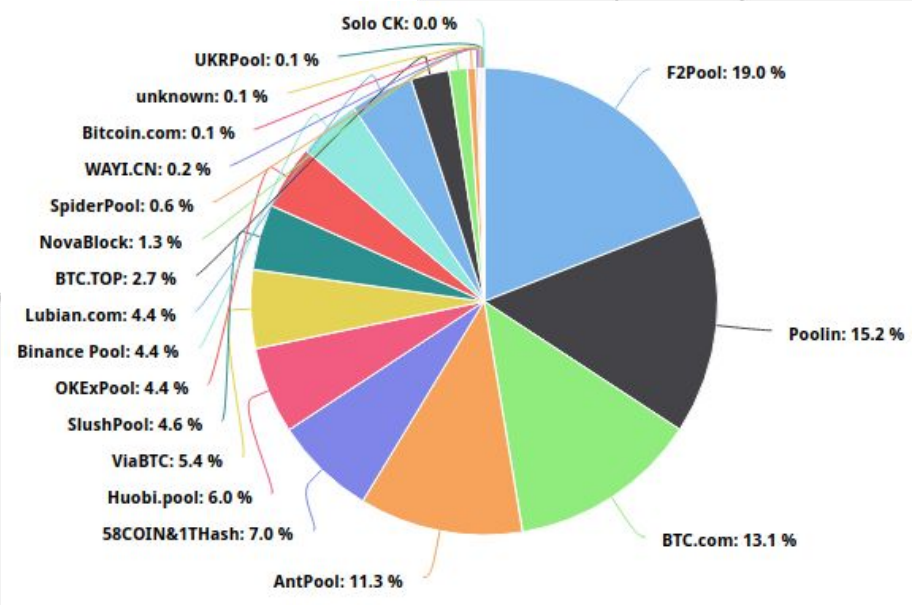
Cardano *Incentives* achieve a level of decentralization that is orders of magnitudes higher than that of Bitcoin.

Staking - The Dual Role of Ada



- Payment
  - Store of value
  - Pay for goods and services
- Staking
  - Participation in the “virtual lottery”
  - Can be delegated to a stake pool.

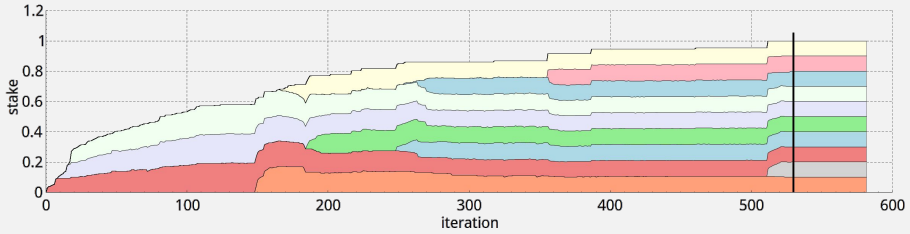
Decentralisation à la Bitcoin



Bitcoin pool distribution BTC.com (22/06/2020)

- And it does not even work that well!
- The five largest mining pools dominate the chain.

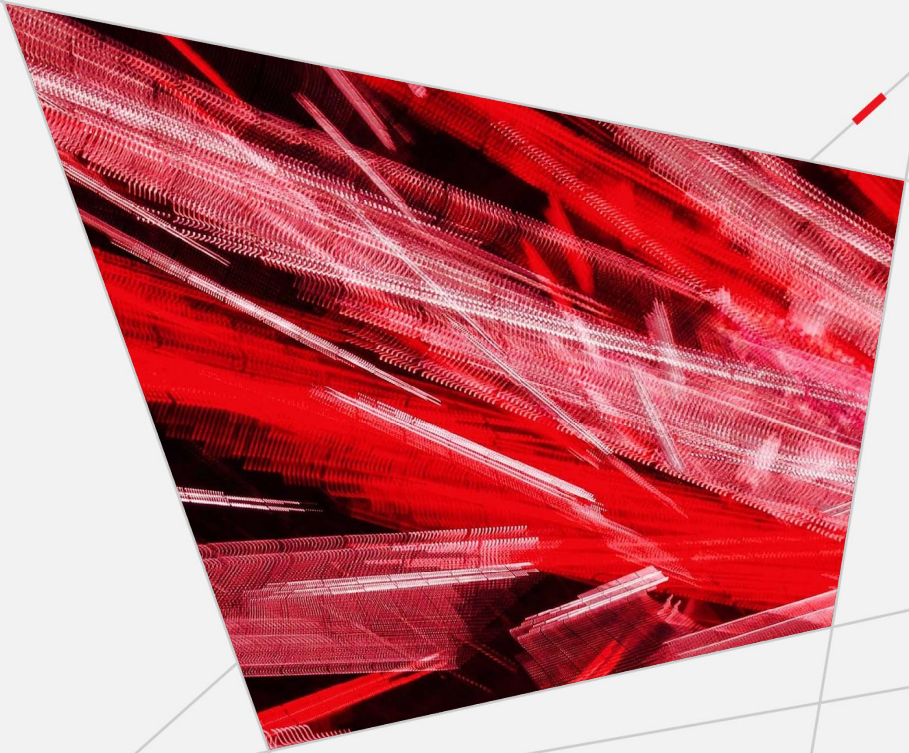
True Decentralisation



- The Cardano Incentives mechanism prevents pools from growing too large.
- Cardano will are targeting 500 pools (soon: 1000), but the sky's the limit.

Cardano development stages

Cardano has several stages of development, each focused on a set of functionalities that together make it more advanced than previous blockchain generations.



Cardano development stages

Foundation

Laying the groundwork for the most advanced blockchain generation.

- This stage – which is now complete – was focused on building a community to support the creation of Cardano.
- It allowed users to buy and sell the ADA cryptocurrency on the Ouroboros protokol.
- Ouroboros is the first Proof-of-Stake protocol, underpinned by academic research, and a mathematically-proven level of security.
  It was developed by IO.

Cardano development stages

Decentralization

Ensuring greater security and robustness.

- In this stage, nodes (blocks of data) are hosted by more and more network participants, leading to it becoming decentralized.
- The more decentralized the networks, the less risk of compromise by malicious behaviour.
- Cardano will be 50-100x more decentralized than other large blockchain networks, and therefore more secure.

Cardano development stages

Smart contracts

Enterprise-ready smart contract creation and management.

- This stage adds the ability to build decentralized applications (DApps), on Cardano's solid foundation of peer-reviewed research and high-assurance development.
- Critically, it enables users from technical and non-technical backgrounds to create and execute functional smart contracts.
- This supports the development of enterprise-level smart contracts for mission-critical applications.

Cardano development stages

Scalability

Establishing unrivalled high-performance, resilience.

- This stage focuses on optimization, and the underlying performance of the Cardano network, improving scalability and interoperability.
- This includes the introduction of sidechains (new blockchains interoperable with the main Cardano chain) increasing the capacity of the network, and enabling experimental features without impacting security.
- This means secure and reliable scalability, and consequently, maintainability.

Cardano development stages

Governance

Establishing self-sustainability to secure the future.

- This stage focuses on ensuring Cardano can be maintained and improved over time.
- It sees the addition of a treasury system, whereby a fraction of all transaction fees are pooled to provide funds for development activities undertaken following the voting process.
- IO has at this stage makes Cardano truly decentralized and future-proof, and transfers management to the community.


INPUT | OUTPUT
Thank you