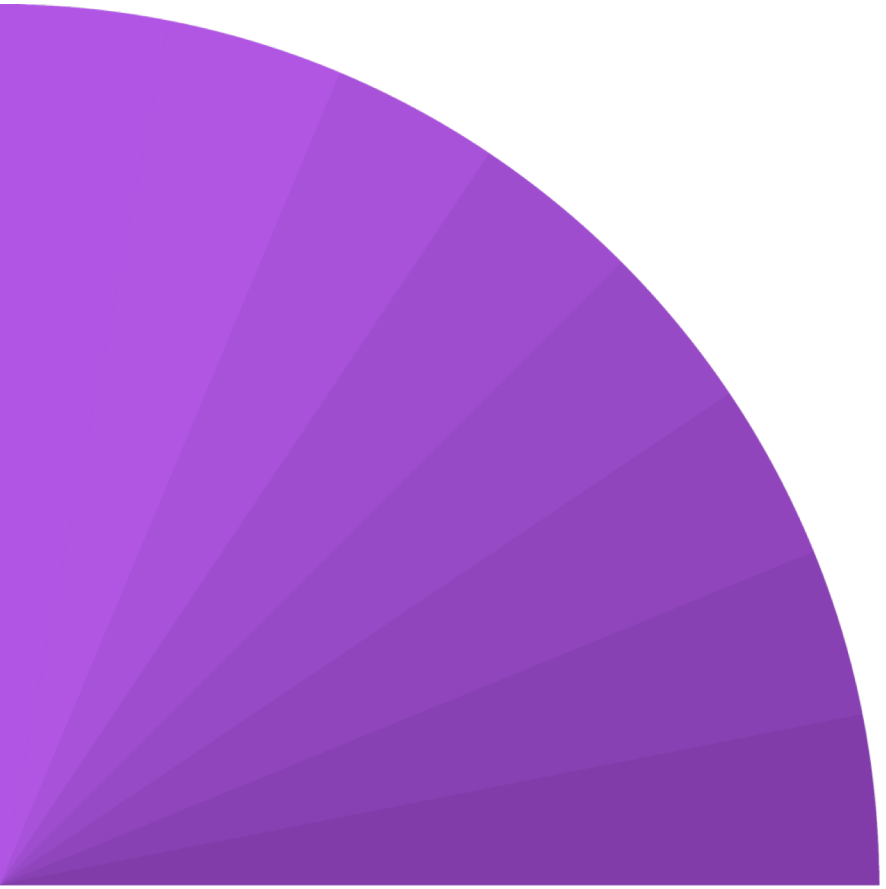
Digital Asset Custody Using MPC

Technology Advisory Committee
February 2020

Discussion Points



The Challenge

- Security v. Liquidity
- An impractical solution

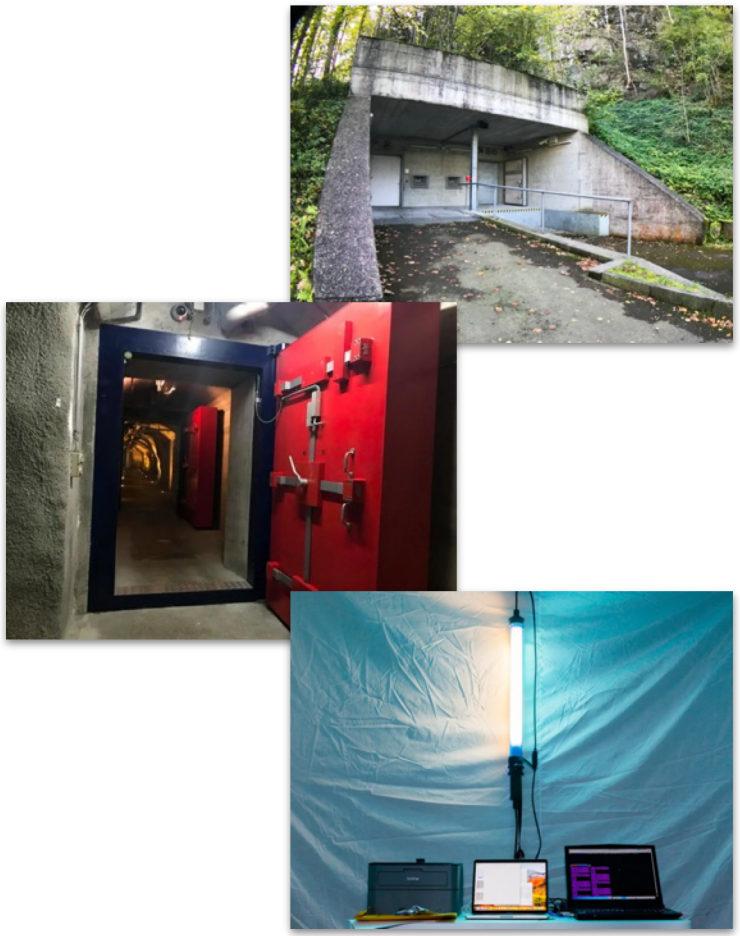
The Building Blocks

- Multi-Party Computation
- Zero Knowledge Proof
- Diffie-Hellman

What this Means for Custody

- Distributed, mathematical resolution
- Trade-off between security and liquidity evaporates

The Challenge - Security v. Liquidity



While blockchains enable **a connected decentralized economy**, private keys dictate **a disconnected centralized infrastructure.**

Existing Solutions

Liquidity		**Security**
Software	Hardware	
Hot	Cold	
Single-Sig	Multi-sig	
Single Key	Sharding	

Breaking the paradigm requires expertise in **security** and **cryptography**.

The Challenge – An impractical solution

- The blockchain itself is based on **math**
  - An elegant solution to the challenge of storing and sharing information in a decentralized model.
  - Protecting it with a combination of human labor or hardware reduces the benefits of that ecosystem.
- The safest and most practical way to protect a mathematical protocol is with **math** itself

EdDSA Curve Calculations

Generate a pub address with a private key

$$pub = g^{\alpha} \bmod p$$

Signing an EDDSA transaction for a specific pub address with a private key

$$where\ h = hash(M \mid pub \mid g^{k}) \bmod q$$

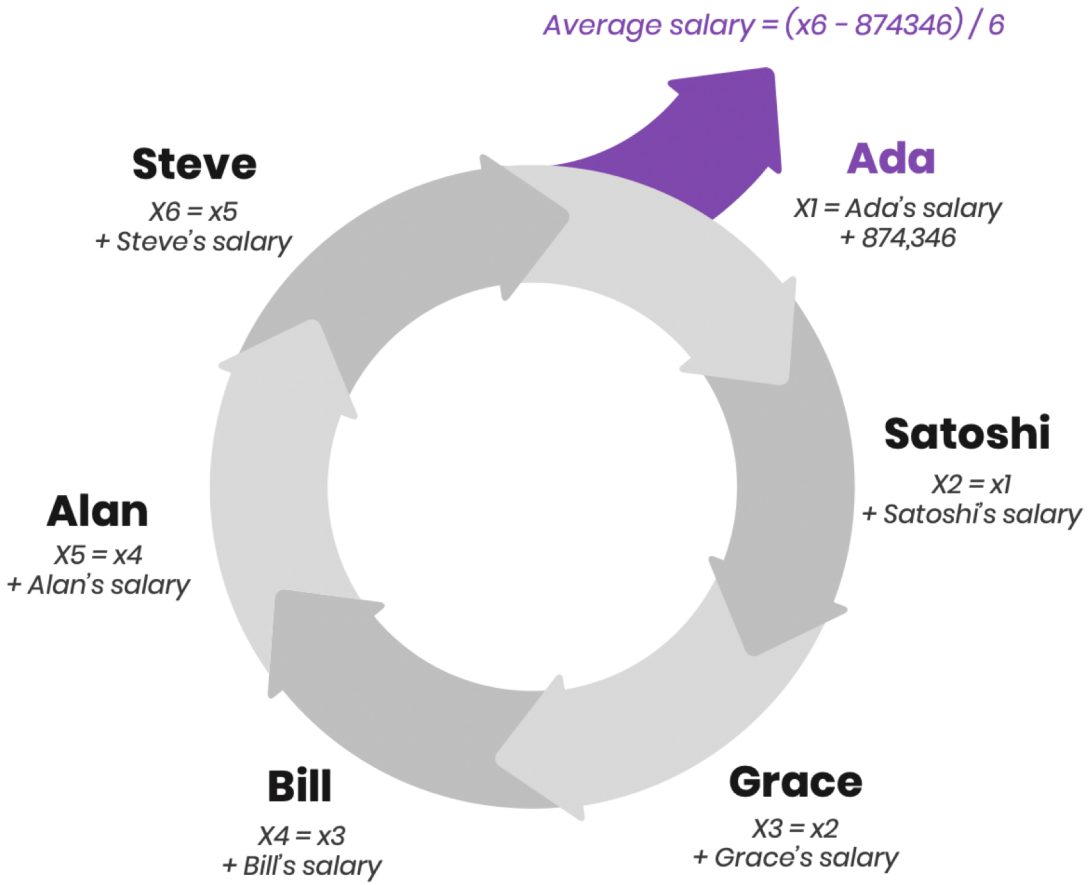
$$sig = k - h * \alpha \bmod q$$

The community then verifies you must have had the correct key

$$hash(M \mid g^{sig} * pub^{h}) \bmod q = h$$

The Building Blocks – MPC

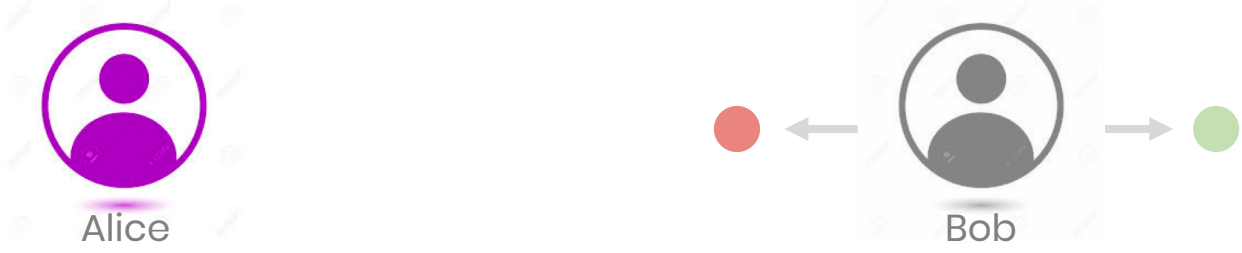
The ability of multiple parties to **jointly perform** mathematical computations without any party **revealing its secret** to the others.



The Building Blocks – Zero Knowledge Proof

Method by which one party (the prover) can demonstrate to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x.

- Alice wants to prove to Bob – who is colorblind – that a red and green ball are truly different.
- She asks him to hide one behind his back and show her the other.
- He then takes both back – either swaps them or doesn't – and shows her one a second time.
- Alice confirms to Bob whether he swapped them or not.



The Building Blocks – Diffie Hellman

Alice

Bob

Publicly agree on two numbers
p = prime (29)
g = generator (4)

Randomly generate 2 local values.

12 L_1

10 L_2

Calculate a public variant | g^local Mod p

(4 ^ 12) Mod 29 = 20

(4 ^ 10) Mod 29 = 23

Exchange the result

20 →

← 23

Calculate the Public Address | shared*g^local Mod p

(20 * 23) Mod 29 = **25**

(23 * 20) Mod 29 = **25**

Jointly calculated public Key = **25**

Implicit Key (α) = 12 + 10 = 22

Validation = 4 ^ (22) Mod 29 = **25**

curv

What it means – is there another way?

Can multiple parties work together to solve signature equations without **ever creating a key** to begin with – nor **ever exposing** any critical information to one another?

Collaboratively calculating a public address

$$pub = g^{\alpha} \bmod p \longrightarrow pub = ((g^{L_1} \bmod p) * (g^{L_2} \bmod p)) \bmod p$$

Yes

Collaboratively calculating a hash

$$h = hash(M \,|\, pub \,|\, g^{k}) \bmod q \longrightarrow h = hash(M \,|\, pub \,|\, g^{(k_1+k_2)} \bmod q$$

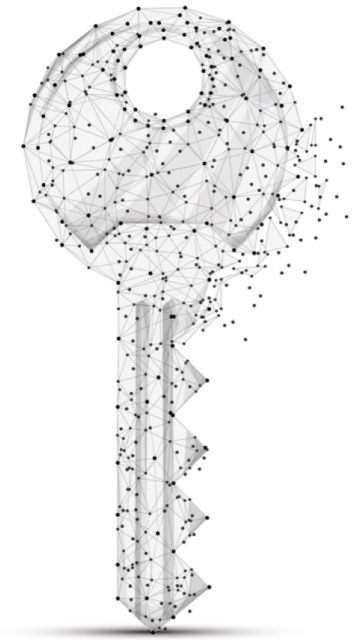
Yes

Collaboratively signing

$$sig = k - h * \alpha \bmod q \longrightarrow sig = (k_1 + k_2) - h * (L_1 + L_2) \bmod q$$

Yes

What this means for custody



The trade-off between security and liquidity evaporates

Secure

- Eliminates any single point of failure
- Local variables can be constantly rotated to avoid compromise

Connected

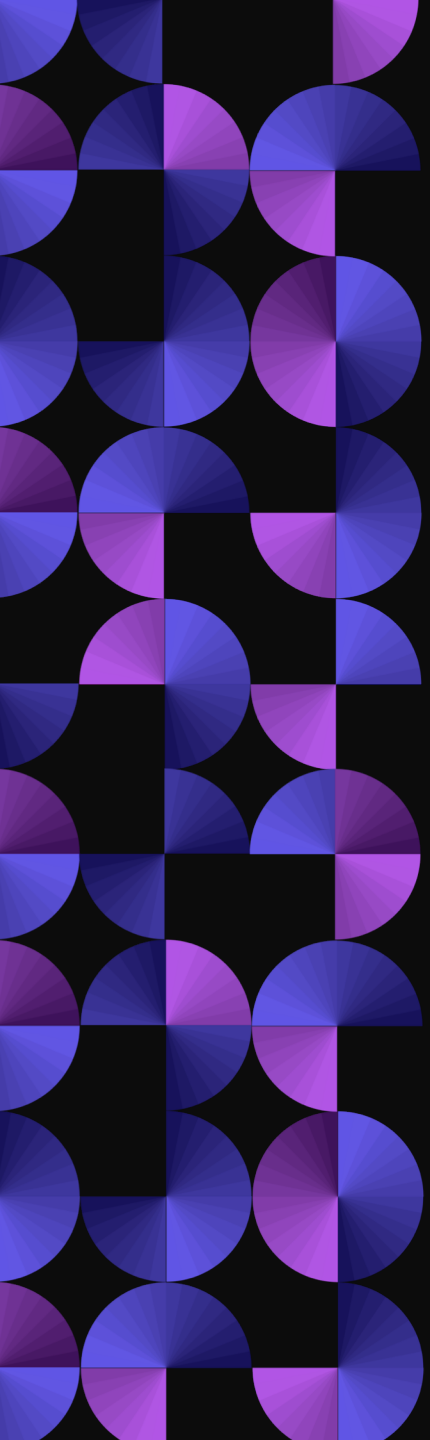
- Empowers instant access to all digital assets

Flexible

- Rules can define when and how local variables are used

Blockchain agnostic

- Security no longer the responsibility of the DLT



curv

Q&A

Itay Malinger, Co-Founder and CEO
itay@curv.co

www.curv.co