Blockchain for Real-world Assets

3/4/21 1:04 PM

Speaker: David Mazieres (Stanford Computer Science)
Date: 03/04/2021

Stellar: equitable access to the financial system

1. Open membership
    a. Anyone can issue, trade, and hold assets
    b. All developers access the same API, from central banks to PhD students
2. Issuer-enforced finality
    a. Security of issued tokens depends only on issuer
    b. Still need secure servers, but issuer owns or designates them
3. Cross-issuer atomicity
    a. Trade any asset for any other (ensures you can bootstrap markets)
    b. Get the best price on any trade without trusting

Non-solutions

- Extend national payment network (ACH, SEPA, UPI) globally
    - E.g. Central Banks systems
    - Requires compliance with national regulations, closed to new assets
- Everyone just issues and manages their own assets
    - E.g. PayPal, Venmo, AliPay
    - Can't pay or trade across systems, closed to new assets

What blockchain really gives us

1. Coin distribution
    a. Distribute new tokens or cryptocurrency while limiting supply
2. Irreversible transactions (under some assumptions)
    a. Can securely exchange or transfer purely digital tokens

Insight: solve #1 & #2 in mutually-reinforcing way with **mining**

Mining

Obtain cryptocurrency as a reward for making digital transactions harder to reverse

- Proof-of-work-based mining (popularized by Bitcoin)
- Proof-of-storage, -memory (burn non-computation resource)
- Proof-of-stake-based mining (many variants)
    - Scale proof-of-work by cryptocurrency holdings

Stellar transaction model

- Global replicated state machine (RSM) executes transactions to keep ledger state
    - Accounts named by public key authorizing operations on the account
    - Accounts can issue assets; issuing account part of asset name
- Transactions guarantee atomicity
    - Multiple operations from multiple accounts with either all succeed or all fail
    - Path payment atomically exchange multiple assets (different types of digital dollars are transferrable)

How to guarantee ledger integrity?

- Model only works if everyone agrees on ledger state
    - If ledger forks, system vulnerable to double-spend attack

Problem: Mining doesn't provide issuer-enforced finality
Double redemption risk not under issuer's control

Mining is scary for digital issuers

- Mining is anonymous
    - Anyone with sufficient resources can extend or fork history
    - Can't even name branch if no policy difference
- Yet mining rewards insufficient to secure flat-currency tokens
- Non-financial (geo-political) incentives to disrupt blockchain

The internet hypothesis

- Idea: only accept ledgers if the people you care about also accept them
- Hypothesis: any two nodes you'd care about transitively follow a common node