CodeChain

Programmable multi-asset blockchain

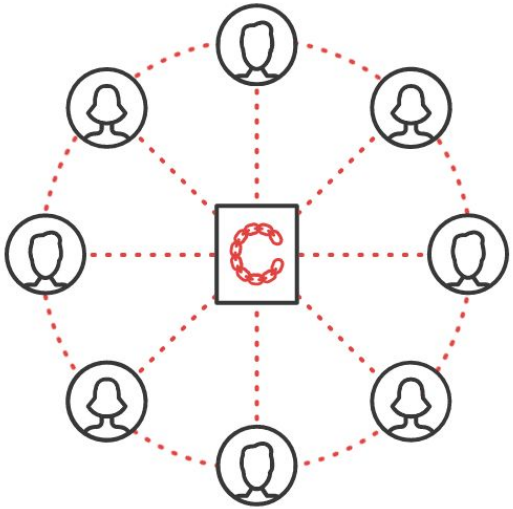
June 7, 2018

About US

Kodebox is a blockchain technology company on a mission to create and enable a smarter asset management system

KODEBOX

CodeChain



CodeChain is a programmable open source blockchain technology optimal for developing and customizing multi-asset management systems

Key Features

- **Built-in multi-asset management solution**
  Issue, transfer and manage currencies, tokens and/or digital items on a blockchain network. No need for smart contracts

- **Pluggable consensus model**
  Choose the consensus model optimal for your business: PoW, Tendermint, Hot-stuff, and PoA

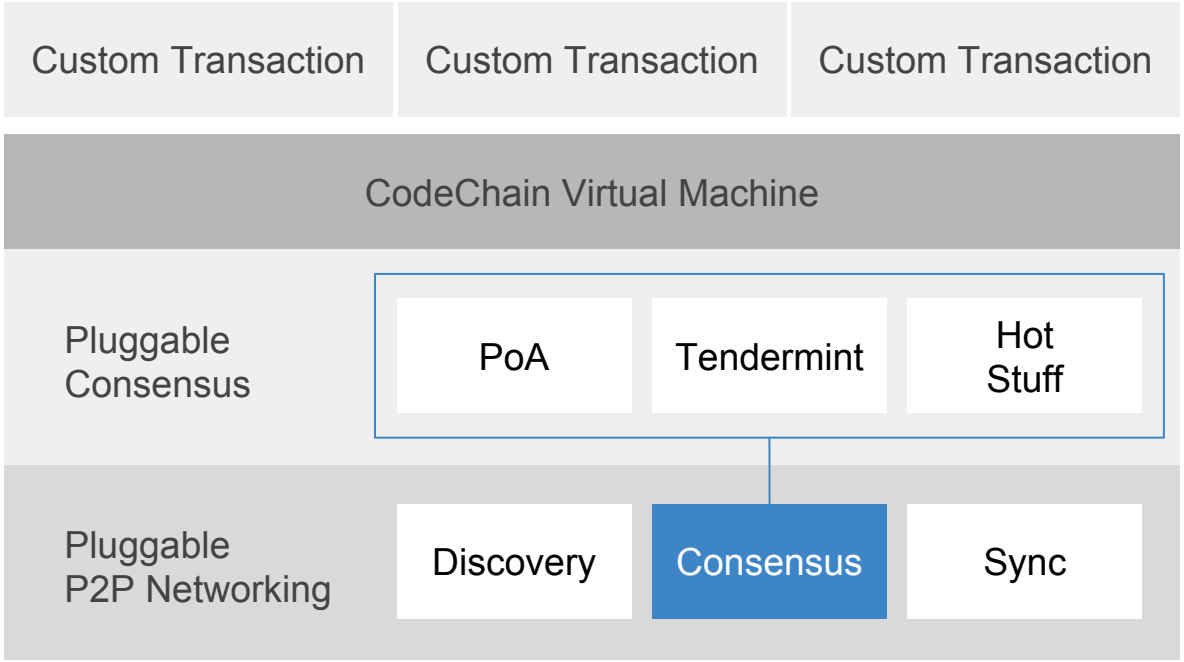
- **Multiple types of transactions**
  Make use of CodeChain's support for programmable transactions: asset evolution, fusion, random item generation, escrow, payment channels and atomic swap

- **Scalability - Sharding**
  Achieve higher transaction speed through horizontal scaling

Pluggable Consensus

KODEBOX

Architecture



Consensus

- Pluggable consensus architecture
  - PoW (Proof of Work)
  - PoA (Proof of Authority)
  - Tendermint
  - Hot-Stuff

- Separation between *beacons* and *replicas*
  - Beacon: a mechanism for triggering proposals
  - e.g., PoW (Beacon) + Wendy (Replicas)

CodeChain: Consensus Laboratory

Hybrid schemes were developed that combine PoW chains with BFT to

- increase throughput
- decrease latency to finality
- promote fairness

A chainless BFT protocol in the permissionless settings that uses PoW to generate propositions and rotate members

- **Solida/Solidus**

Uses a BFT engine as a finalizing authority over a permissionless chain

- **Casper the Friendly Finality Gadget**

Use a permissionless chain to determine a participant/proposer rotation

- **Byzcoin, Bitcoin-NG and Hybrid Consensus**

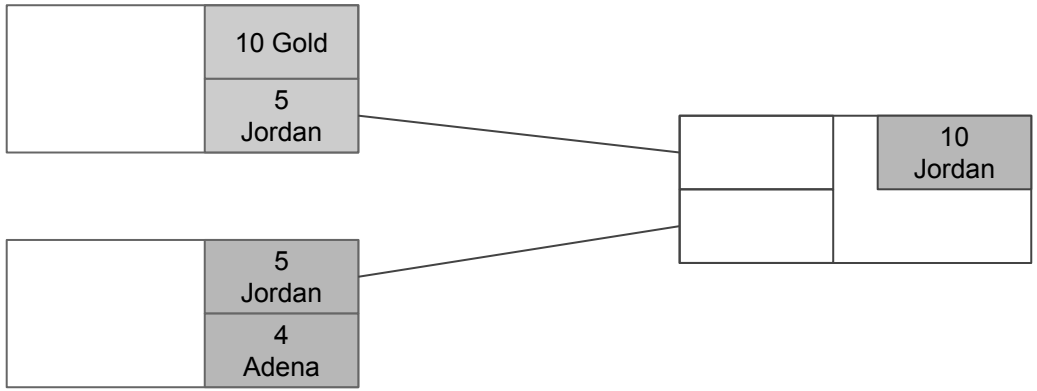
Uses a permissionless chain for recovery from failures

- **Thunderella**

Programmable Transaction

Transaction Format

AssetTransferInput	AssetTransferOutput
- lock_script_hash: H256, - parameters: Vec<Bytes>, - asset_type: H256, - amount: u64	- prev_out: AssetOutPoint, - lock_script: Bytes, - unlock_script: Bytes,



CodeChain VM

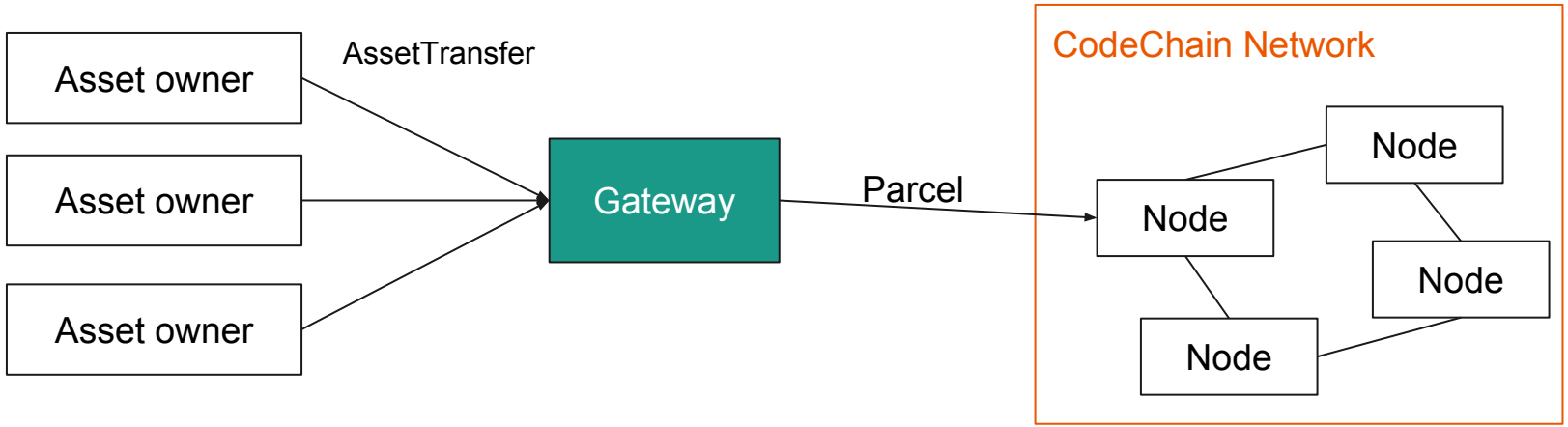
- Guaranteed termination
- Bitcoin-like script language for locking and unlocking assets
- P2SH by default

e.g., Pay To Pub Key

- Unlock Script: Push <signature>
- Lock Script($pub_key): Push $pub_key ChkSig

User doesn’t pay the fee

Gateway



1. Creates “Parcel”, which groups the transactions
2. Signs to parcel. Signer pays fee for the parcel
3. Sends signed parcel to CodeChain network

Parcel Format

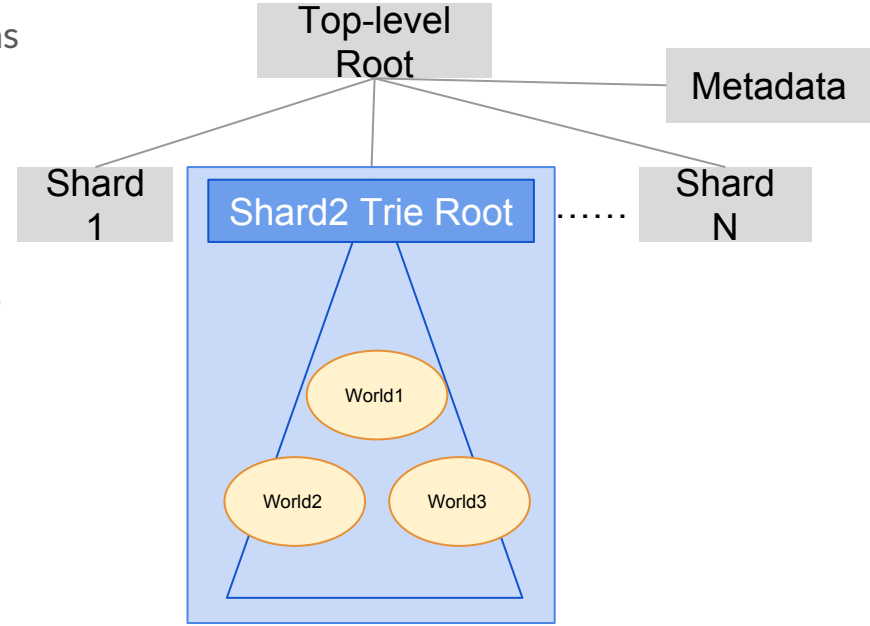
```
pub struct Parcel {
    pub nonce: U256,
    pub fee: U256,
    pub transactions
        : Vec<Transaction>,
    pub network_id: u64,
}

pub struct UnverifiedParcel {
    unsigned: Parcel,
    v: u8,
    r: U256,
    s: U256,
    hash: H256,
}
```

- Fee determines priority
- Minimum fee exists
- *nonce* prevents replay attack
- Sender is derived from the signature

Horizontal Scalability through Sharding

Sharding

- Provide horizontal scalability
  - Different shards can execute transactions in parallel
- World is a logical division
  - Shard has multiple worlds
  - Worlds in the same shard share the state trie
- Top-level trie contains the root of shard-tries and metadata



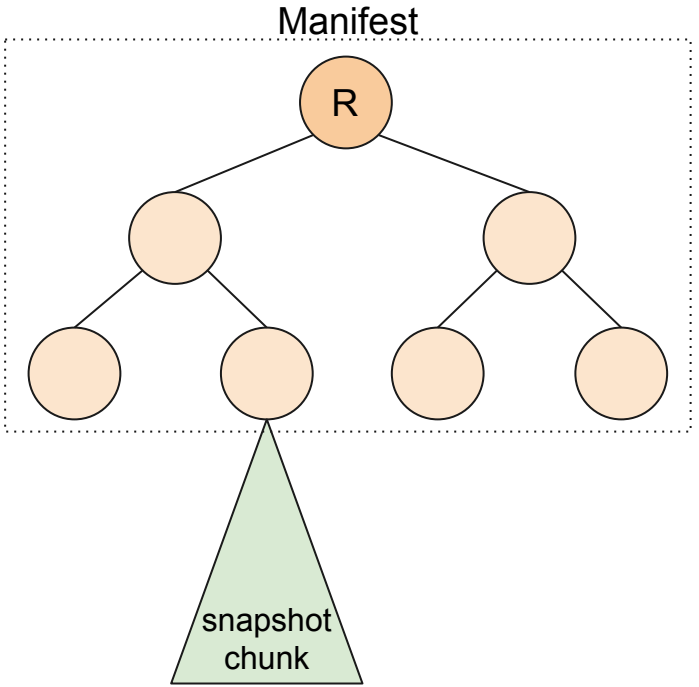
Shard Participant

- Gateway
  - Creates parcel
  - Collect signatures for Parcel from **Validator**s
- Validator
  - Validates Parcel
  - Run transactions for specific shards
  - Computes shared-trie state
- Beacon
  - Generates block and propagation
  - Cares only about top-level trie

Fast Sync

Snapshot sync

- Mix of Fast sync and Warp sync
  - Download all headers & invoices from genesis
  - Fetch entire subtree instead of fetching each nodes separately
- Grandchild of root becomes snapshot chunk
  - At most 257$(1 + 2^8)$ downloads for complete recovery
- Dynamic validator support



KODEBOX

Thank You

Home
http://codechain.io/

Blog
https://medium.com/codechain/

Facebook Page
https://www.facebook.com/codechain/

Twitter
https://twitter.com/codechain_io

KODEBOX

GoCryptobot

World's first blockchain mobile game for both iOS and android

- Android: https://play.google.com/store/apps/details?id=com.kodebox.gocryptobot
- iOS: https://itunes.apple.com/app/id1357491624