FEVR

Coiners

Blockchain

❤️

Javascript

Simone Da Re

Full Stack Developer
Blockchain Enthusiast & Student

 Follow me on LinkedIn

Blockchain

»

Blockchain is a distributed database that maintains a continuously-growing list of records called blocks secured from tampering and revision.

»

Blockchain in 200 lines of code

```javascript
class Block {
    constructor(index, previousHash, timestamp, data, hash) {
        this.index = index;
        this.previousHash = previousHash.toString();
        this.timestamp = timestamp;
        this.data = data;
        this.hash = hash.toString();
    }
}
```
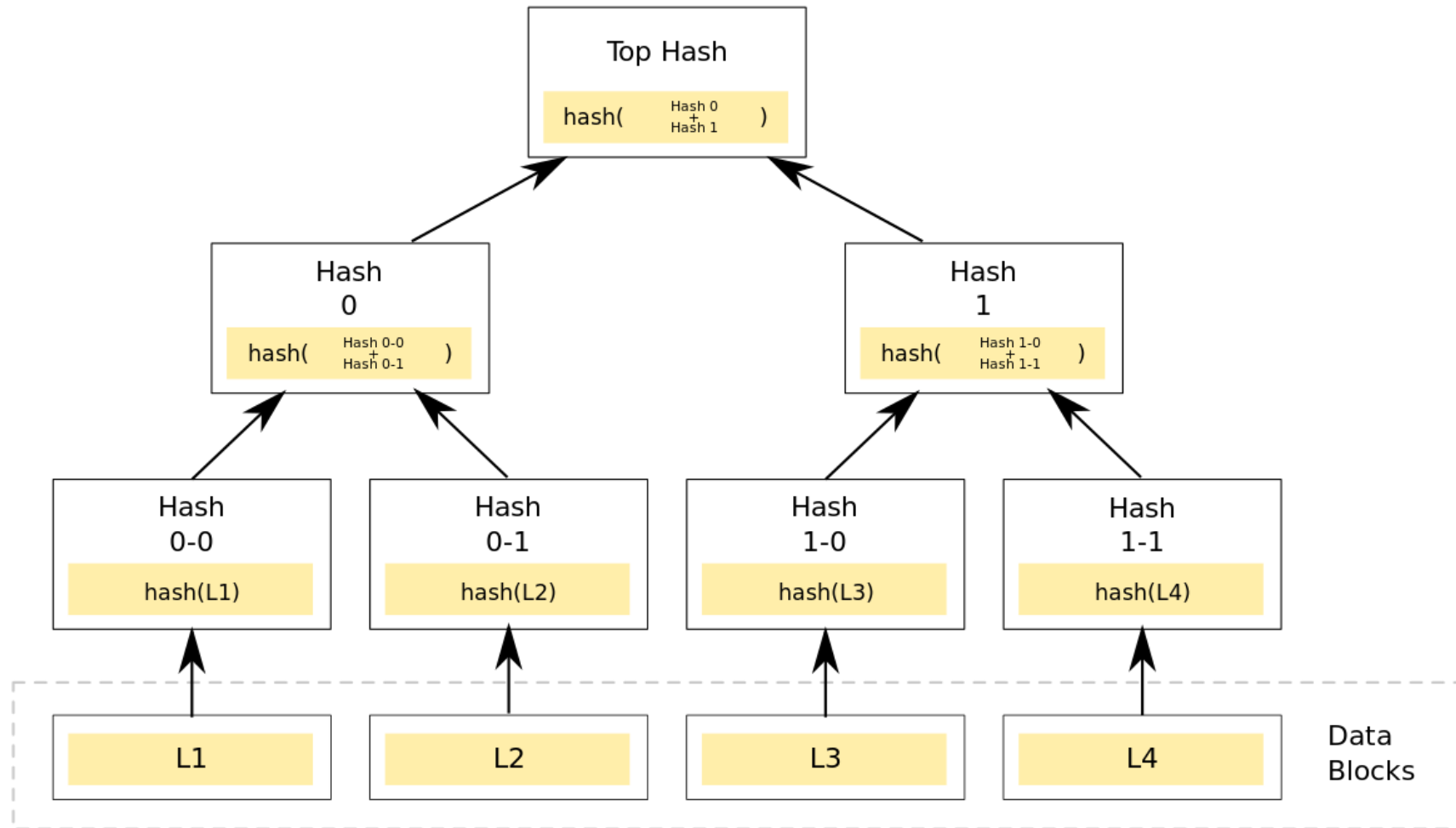
Ethash, POS soon?

```javascript
var calculateHash = (index, previousHash, timestamp, data) => {
    return CryptoJS.SHA256(index + previousHash + timestamp + data).toString();
};
```
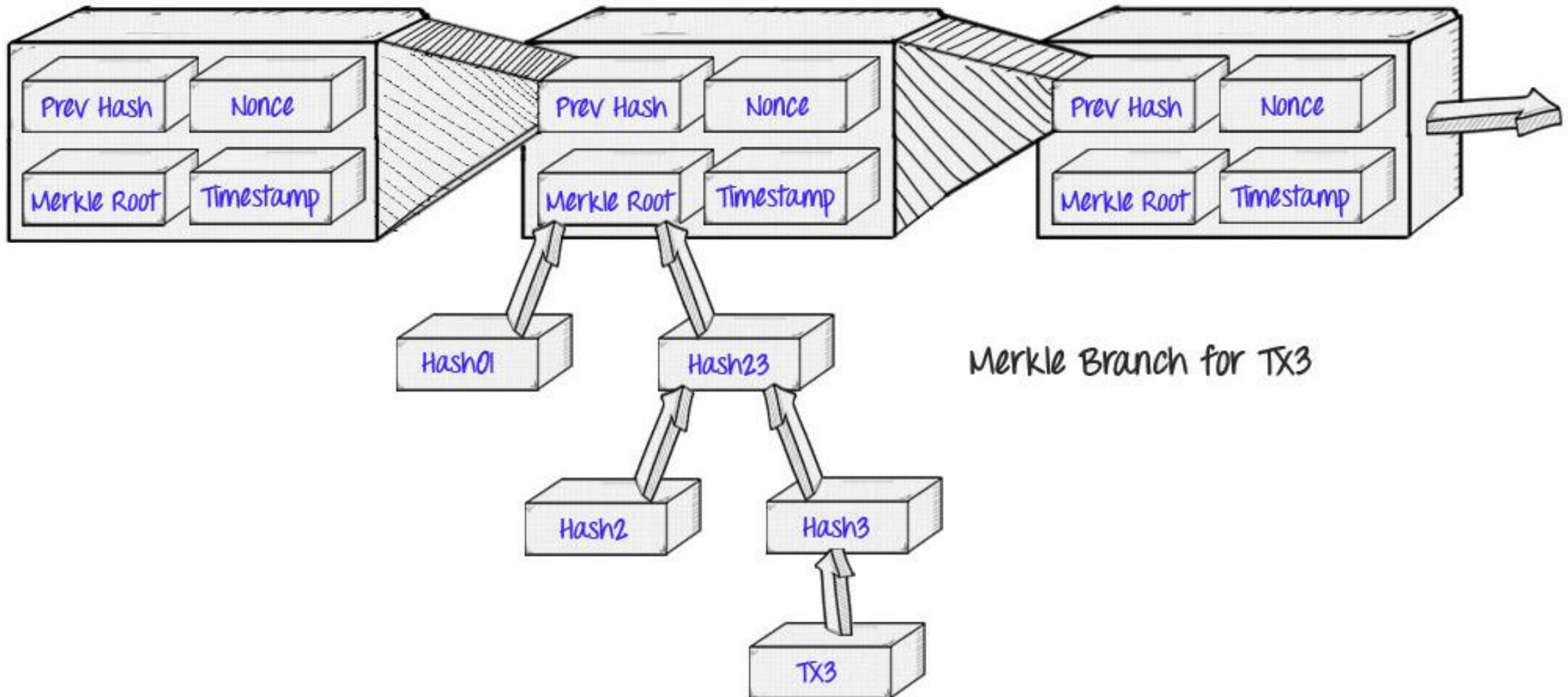
Ethereum Blocks

```javascript
var generateNextBlock = (blockData) => {
    var previousBlock = getLatestBlock();
    var nextIndex = previousBlock.index + 1;
    var nextTimestamp = new Date().getTime() / 1000;
    var nextHash = calculateHash(nextIndex, previousBlock.hash, nextTimestamp, blockData);
    return new Block(nextIndex, previousBlock.hash, nextTimestamp, blockData, nextHash);
};
```

Merkle Tree

Complete structure of blocks

Block 1:
- Prev Hash
- Nonce
- Merkle Root
- Timestamp

Block 2:
- Prev Hash
- Nonce
- Merkle Root
- Timestamp

Block 3:
- Prev Hash
- Nonce
- Merkle Root
- Timestamp

Hash01

Hash23

Merkle Branch for TX3

Hash2

Hash3

TX3

Blockchain Genesis Blocks

```javascript
var getGenesisBlock = () => {
    return new Block(0, "0", 1465154705, "my genesis block!!", "816534932..");
};


var blockchain = [getGenesisBlock()];
```

Bitcoin Genesis Block

«

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks
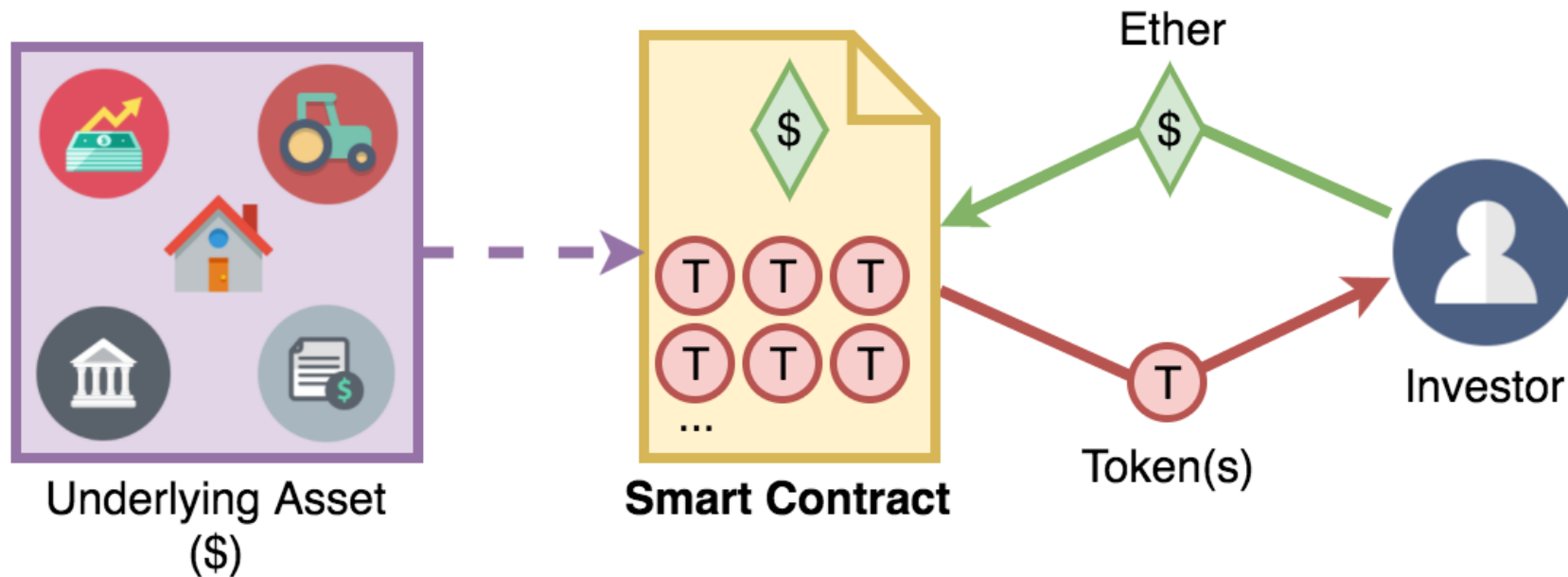
«

Ethereum Genesis Address

0x0000000000000000000000000000000000000000

Ethereum Virtual Machine

«

It is a quasi-Turing complete machine; the quasi qualification comes from the fact that the computation is intrinsically bounded through a parameter, gas, which limits the total amount of computation done.
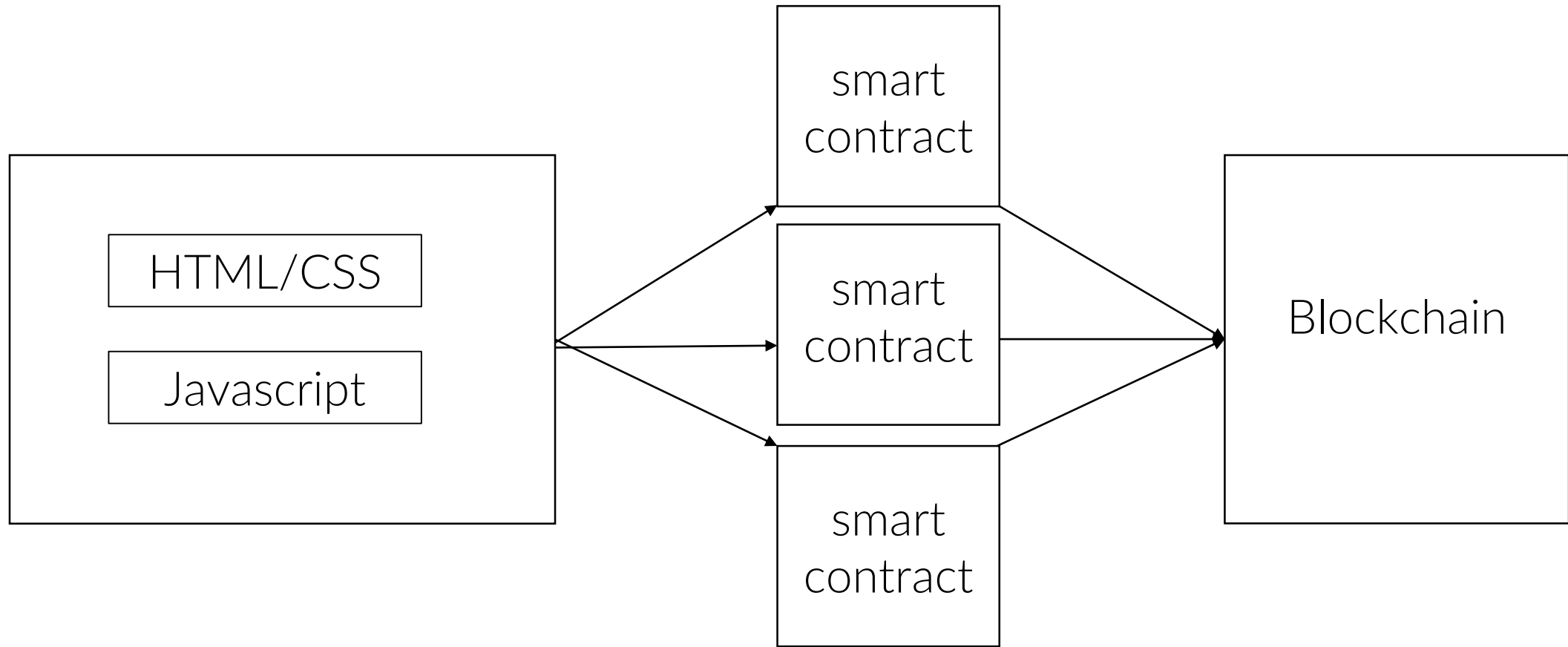
«

Smart Contract

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.
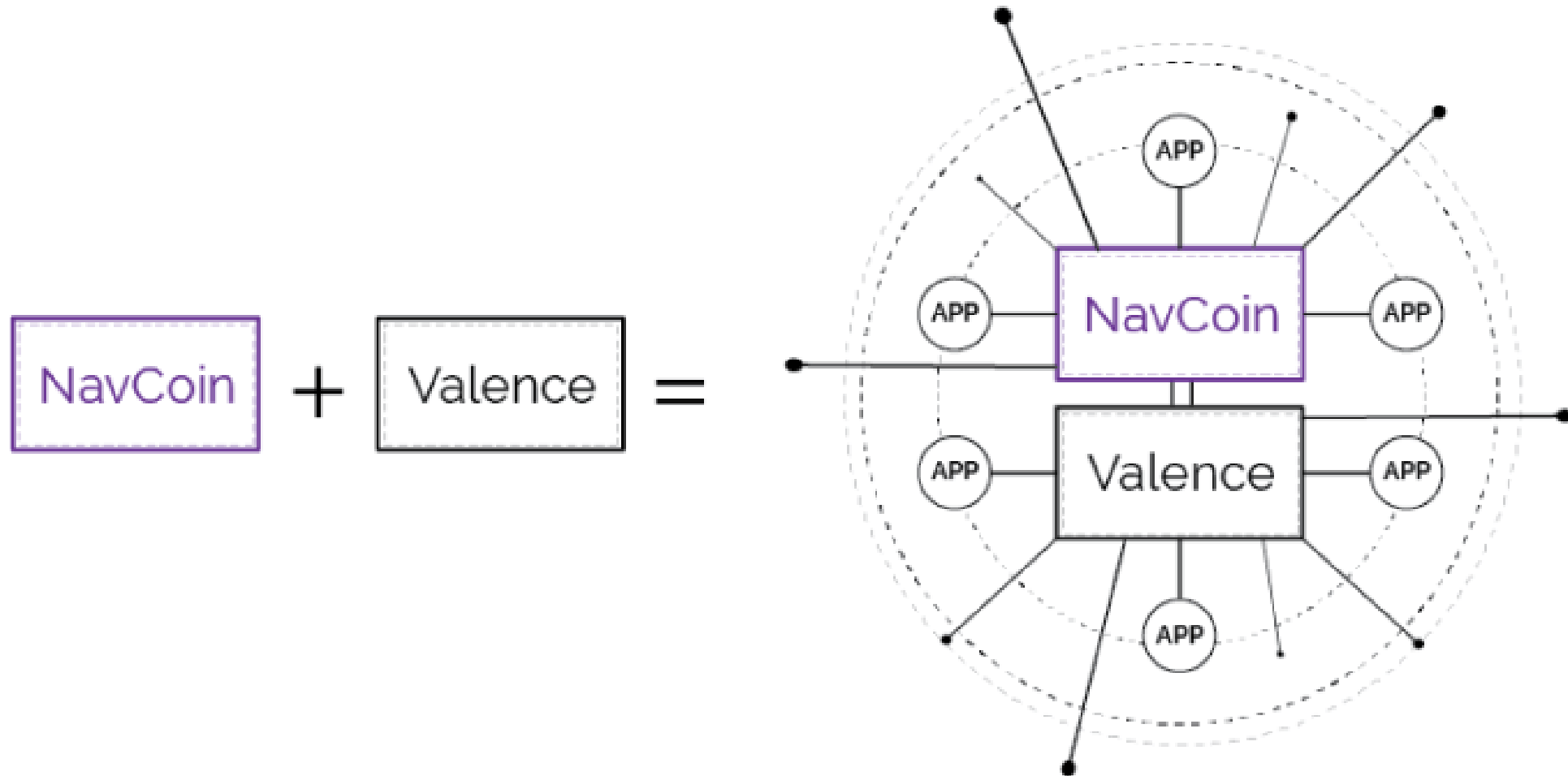
The structure of DApps

ADApps – Anonymous DApps
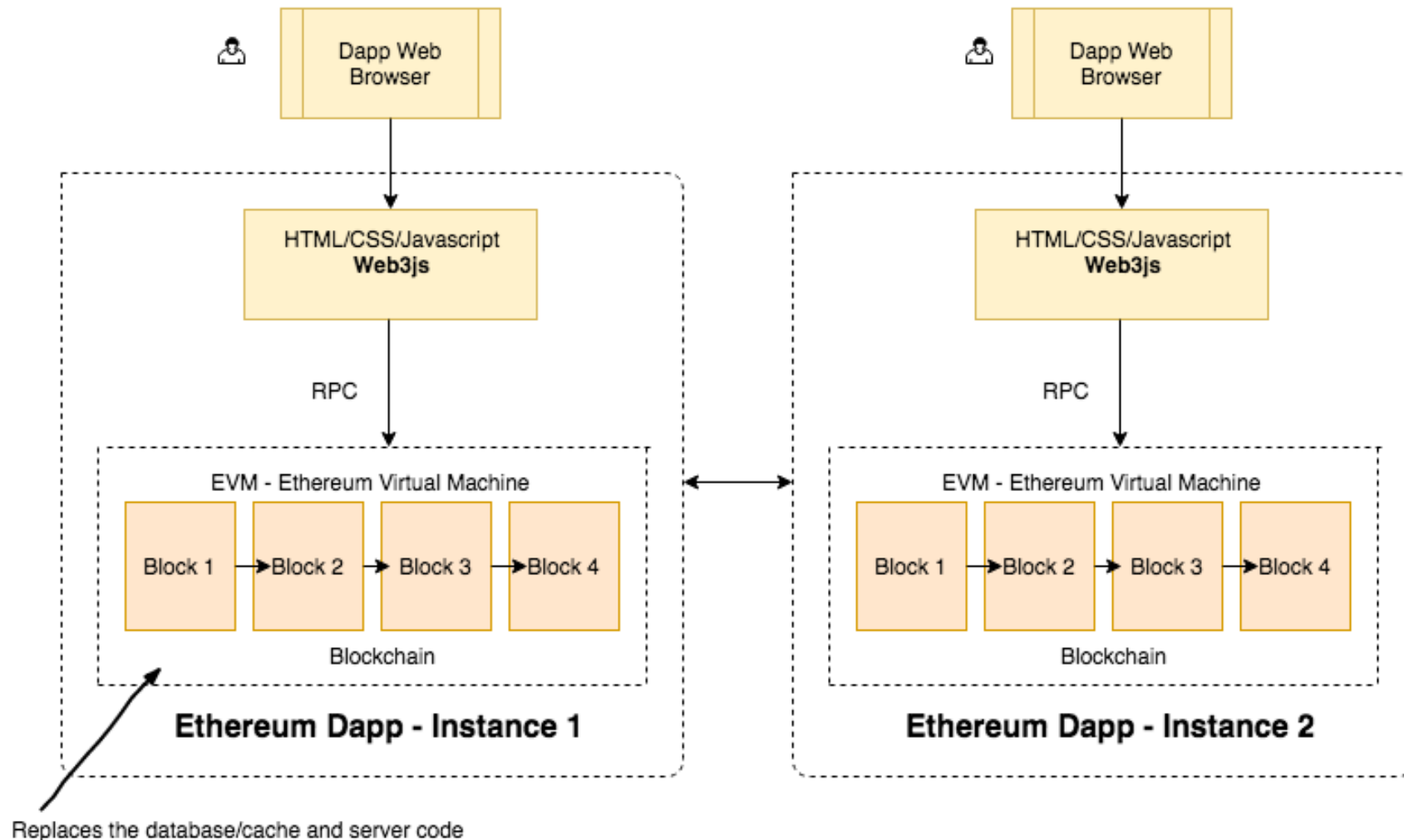
Valence Structure

Web3.js

Ethereum compatible JavaScript API which implements the Generic JSON RPC spec.
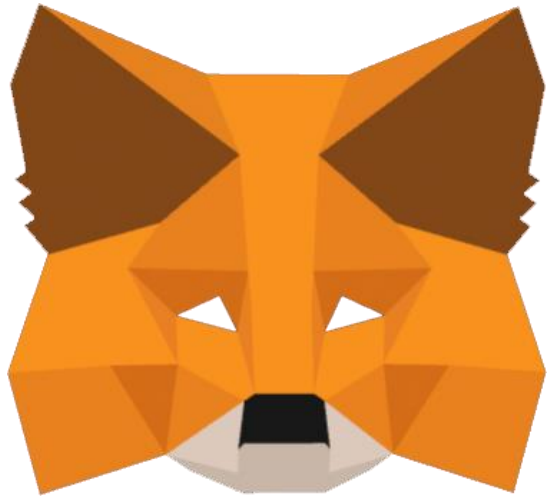
Dapps – Decentralized Applications

Truffle Framework

Templates ready to use

Blockchain in RAM

Compilation, Migration, Testing, Debugging and Deployment

Metamask

Chrome and Firefox extension

Full Ethereum Node

Smart Contract Bridge

Vieni a trovarci sui social!