Smart Contracts and the Blockchain Judiciary

Brian McMillin
1 July 2018

Bitcoin Limitations

- The Script language used on the Bitcoin blockchain supports cryptocurrency and is not suitable for general-purpose contracts

- Blocks are added to the Bitcoin blockchain every ten minutes

- It typically takes an hour for a transaction to be "confirmed"

- Proof-of-work consensus requires an unacceptable level of computing resources

Ethereum Limitations

- Nondeterministic scripts executed by Block Miners can delay transactions being added to the blockchain
- The concept of arbitrary Gas limits and usage adds more unnecessary nondeterminism
- The use of Accounts eliminates privacy expectations and violates cryptographic key usage standards

What Do We Expect?

- Fast addition of Transactions to the Blockchain
- Near-immediate Verification of Transactions
- Unlimited Transaction Size and Block Size
- Minimal Computing Resources for Mining Consensus
- Arbitrarily Complex Smart-Contract Construction

- Miners should always include all available Pending Transactions in the Block that they propose to add

- Miners should work to achieve Consensus, not Compete to undermine each other

- Miners should be rewarded in a Fair, Deterministic Manner for the Blocks that they add to the Blockchain

- Miners should need only a small, reasonable level of computing and networking resources to participate

Bonded Proof-of-Stake

- Wholly Deterministic Blockchain Operation
- Miners put up a minimum amount of Cryptocurrency as a Bond and Bid on the right to Produce a Block in the future
- Winners of the Auction are assigned a specific Future Block Number to Produce
- Multiple Auctions ensure that there are always multiple Producers assigned to each new Block
- A Fair, Deterministic Algorithm allocates Block Bounties among the successful collaborative Producers
- Minimum Computation, Storage and Network Communications required

The Need for a Blockchain Judiciary

- Smart Contracts generate a Go/No-Go result given the Contract Code and a set of inputs
- Contracts may be lengthy and the Input data voluminous
- Contracts may need specialized programming languages
- Miners must verify Transactions as fast as possible using as little Resource as possible
- THEREFORE - Miners themselves should not be involved in the actual execution of Smart Contracts

The Judiciary Is:

- A Data Structure on the Blockchain
- A Named List of Judges (I.e. Signing Authorities)
- A Set of contract Rules for adding and removing Judges
- A Published Description of the types of Contracts that this Judiciary will evaluate

---

- Each Judge may execute the code of a Smart Contract upon request, and return a Signed Yes/No Verdict
- The Signed Verdict may be presented as one of the Inputs to a Transaction to be Mined on the Blockchain

Contracts using the Judiciary

- Specify the Name of the Judiciary (i.e. jurisdiction) to be used
- Specify the desired voting rules among the Judges
- Specify the Contract Code - written in a Programming Language acceptable to that Judiciary
- Specify the Transaction Code that instructs the Miner to validate certain Inputs as Signatures and to generate certain Outputs

- Judges evaluate Smart Contract Code on request
- Contract Evaluation is generally not fast or real-time
- Signed Verdicts may be immediately added to the Blockchain, or held in abeyance to be combined with other Inputs or Verdicts
- Payments for the services of a Judge may be completely independent of the Contract itself
- Various Judiciaries may post different performance terms and fee schedules in order to compete for business

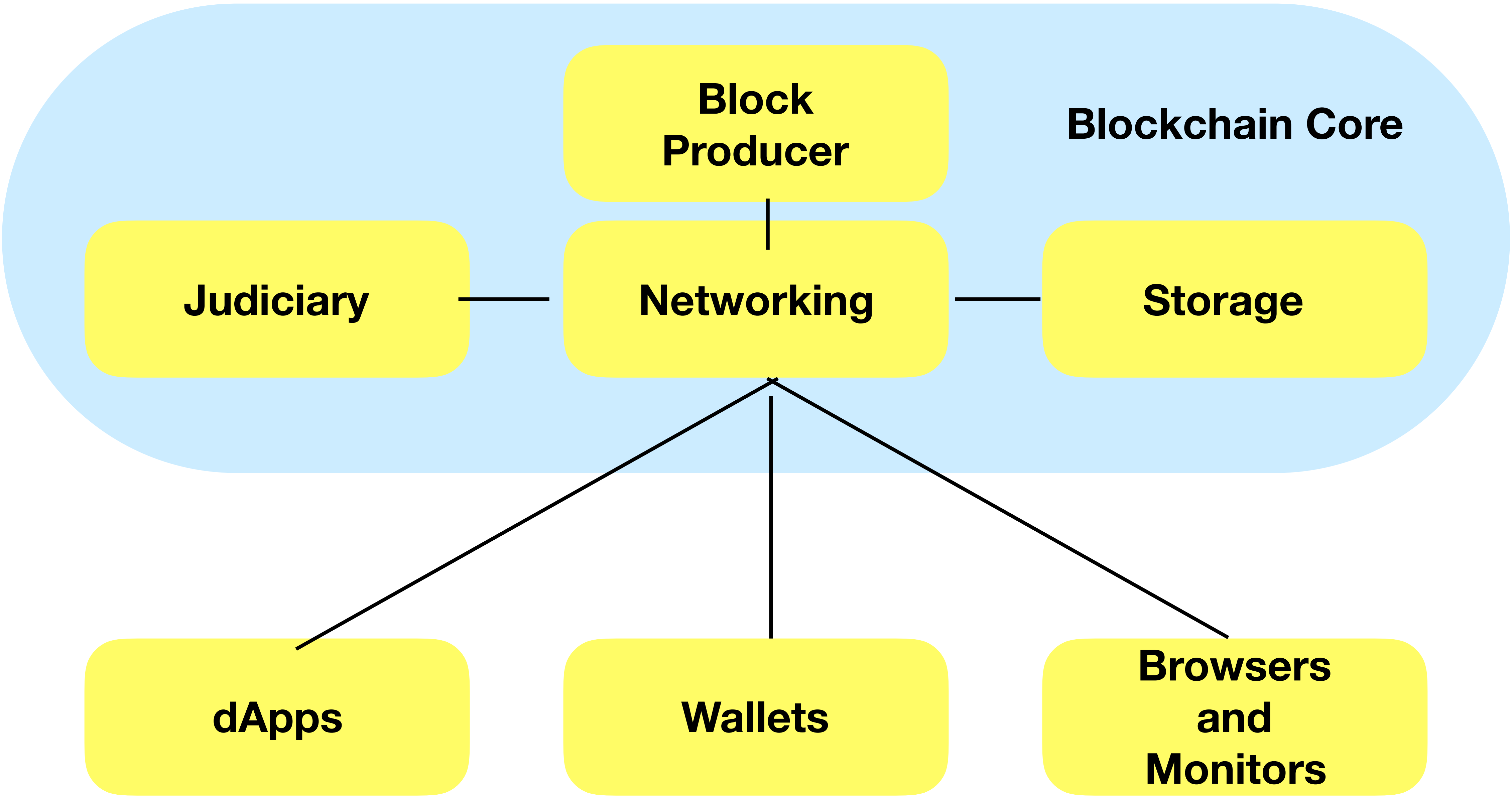
These are Independent

- Adding Transactions and Blocks to the Blockchain
- Persistent, Redundant Storage of the Blockchain
- Operations involving Cryptocurrency
- Evaluation of Smart-Contracts
- Persistent Oracles, Events, Triggers and Timers
- Off-Chain Gateways, Monitors, Wallets

Benefits

- No wasted computation
- Smart-Contract Consensus is completely independent of Blockchain Consensus
- Blockchain Mining operates as fast as possible
- Blockchain Mining is separate from Blockchain Storage
- No off-chain data is ever used in the Evaluation of a Contract

Blockchain Services


Blockchain Core
Block Producer
Judiciary
Networking
Storage
dApps
Wallets
Browsers and Monitors