Replacing Bitcoin

Sustainable Blockchain for the 21st Century

Brian McMillin

18 July 2018

- Bitcoin is Fatally Flawed
- Other Cryptocurrencies are Too Limited
- Requirements for Sustainability
- The **slán-chain** Solution

Choosing an International Trademark is a Big Deal

- For Discussion Purposes I Choose to Call the Technology **Slán-Chain** and **Slán-Coin**
- Gaelic is well-known but still obscure
- **Slán** means **Secure**
- Registered Trademarks are Important for Success

Bitcoin is Not the Future

- Bitcoin uses the Blockchain **ONLY** to Support the Cryptocurrency
- Bitcoin Consumes Resources at an Unsustainable Rate
- Bitcoin Limits the Size and Rate of Transactions
- Bitcoin Allows Random Delays in Transaction Confirmation
- Bitcoin Limits the Scope of Smart Contracts
- “Full Nodes” must Possess a Copy of the Entire Blockchain

Ethereum is Not the Future

- Smart Contracts Require the Use of an Arbitrary, Flawed, Non-Deterministic Virtual Machine

- The use of “Gas” to Mask the Limitations of the Architecture means that Contracts can Fail Randomly or Cost their Owners Unexpected Fees

- The use of “Accounts” means that Business Partners can be Linked and Are Afforded No Privacy for Transactions

- “Full Nodes” must retain a copy of all Active Accounts with No Compensation for Long-Term Storage of Bulk Data

Bitcoin Design is Brilliant

- “Satashi Nakamoto” did a Wonderful Job
- **Goal:** Create a Cryptocurrency
- **Then:** Use the Blockchain to Protect the Ledger
- Miners all have a Full Copy of the Blockchain to Verify
- Slow Transaction Rate so Everybody Can Participate
- Works on a Desktop Computer - **in 2005**

Slán-Chain Design is Different

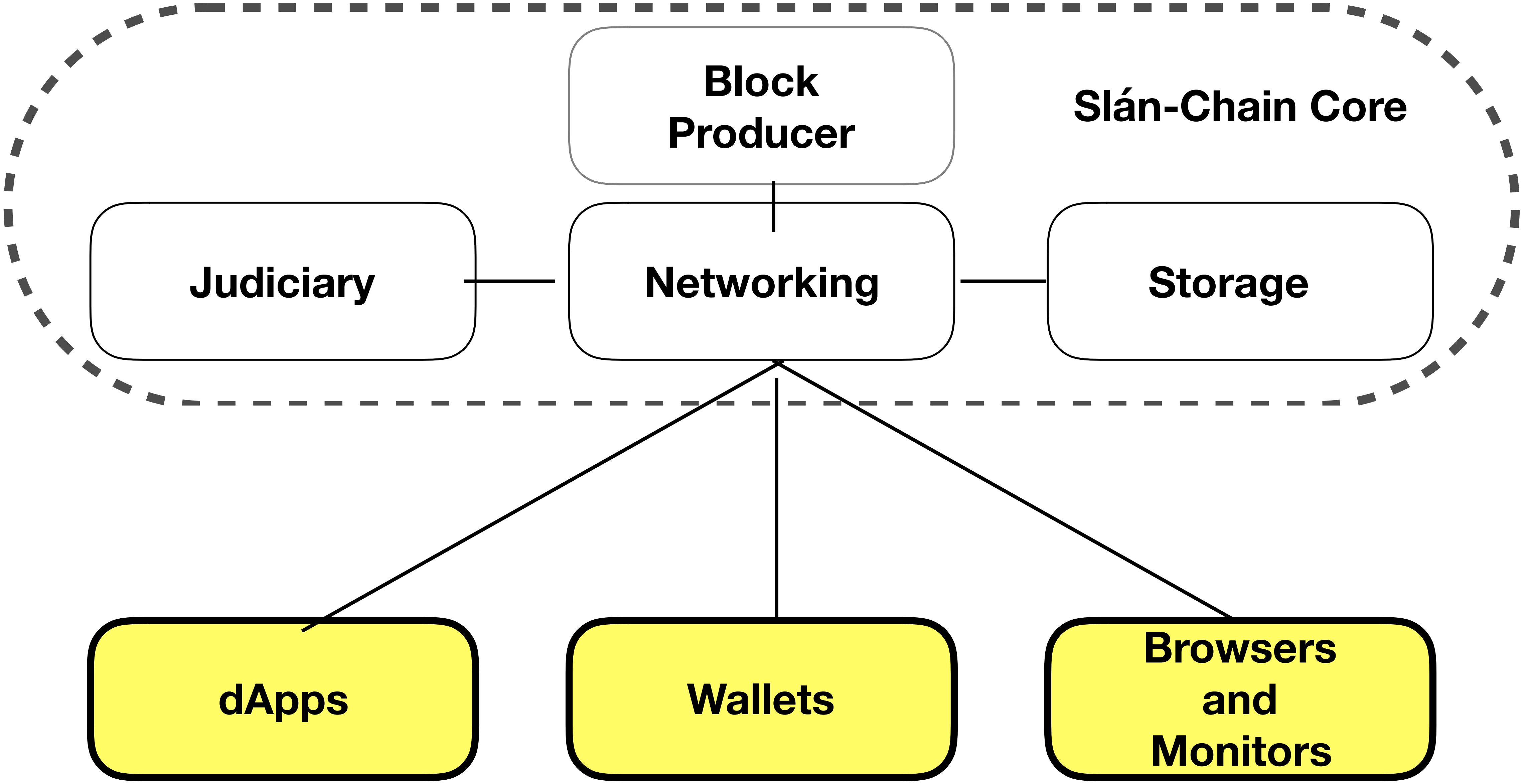
- The Chain Design comes First
- The Cryptocurrency supports the operation of the Chain
- The Cryptocurrency Represents the Inherent Value of the Chain and Does NOT Need to be Artificially Established
- Currency Transactions are Small and Fast and use an Insignificant Amount of Resources at a Negligible Cost
- Transactions are Confirmed “Immediately” or Never - no Limbo (pending) State

Purpose of the Slán-Chain

- Store Unlimited Amounts of Data
- Cryptographically Secure, Redundant, Distributed
- Prepaid, Permanent, Immutable Ledger
- Use Slán-Coin to pay for Storage, Networking, Block Production and Smart Contract Judiciary

- Oh, and Handle Individual Cryptocurrency Transactions

Blockchain Services



Block Producer

Slán-Chain Core

Judiciary

Networking

Storage

dApps

Wallets

Browsers and Monitors

Smart Contracts

- Smart Contracts Must Be Written and Understood by Human Beings
- Smart Contracts Must Be Flexible Enough to Support Multiple Specific Programming Languages for Different Applications
- Large Smart Contracts Must Never Slow Down the Blockchain
- Validation Through Independent Consensus is Important
- Consensus for Contracts Need Not be the Same as Consensus for the Blockchain

Bonded Proof-of-Stake

- “Miners” are called “Block Producers”
- Block Producers bid on the right to Produce (mine) a Block in the Future
- In order to Bid, all Producer Candidates Must put up a Bond. Think of it like an ante.
- The winning Producer is selected at random
- Non-winning Producer Candidates have their Bond Returned Immediately
- If the Winning Producer Produces a Valid Block on time she gets the Bond Plus the Fees from the Transactions in the Block
- If the Winning Producer Fails to Produce a Valid Block she Forfeits her Bond