Advancements in Consensus Algorithms with Applications to Special Purpose Contracts

Darren Tapp

Dash Investment Foundation

March 5th, 2021

Overview

1 Overview

2 Abstract Blockchain

3 Zooko's Triangle

4 Smart Contract Security

5 Dash Evolution

6 Contract Security (reprise)

Love of Mathematics!!

I pursued Math as an art. Today, I will be an artist using blockchain as my medium.
The abstract blockchain section is to establish a blank canvas. (blockchain)

I'm a mathematician by training.
Half of good mathematics is choosing good definitions
Hironaka anecdote

Nakamoto Consensus

Nakamoto Consensus

Proof of Work consensus described in:
Nakamoto, Satoshi "Bitcoin: A Peer-to-Peer Electronic Cash System"

Nakamoto Consensus Properties

Properties:

- Runs at a stable Nash equilibrium
- Self enforcing governance
- Stronger consensus than BFT (Byzantine Fault Tolerance)
- ⋮

Post-Nakamoto Consensus

Post-Nakamato consensus protocols:

- Ouroboros
- Tindermint
- Dash consensus
- ⋮

A Blockchain Abstractly

Abstracting a Blockchain

A Blockchain maintains a "Global State"

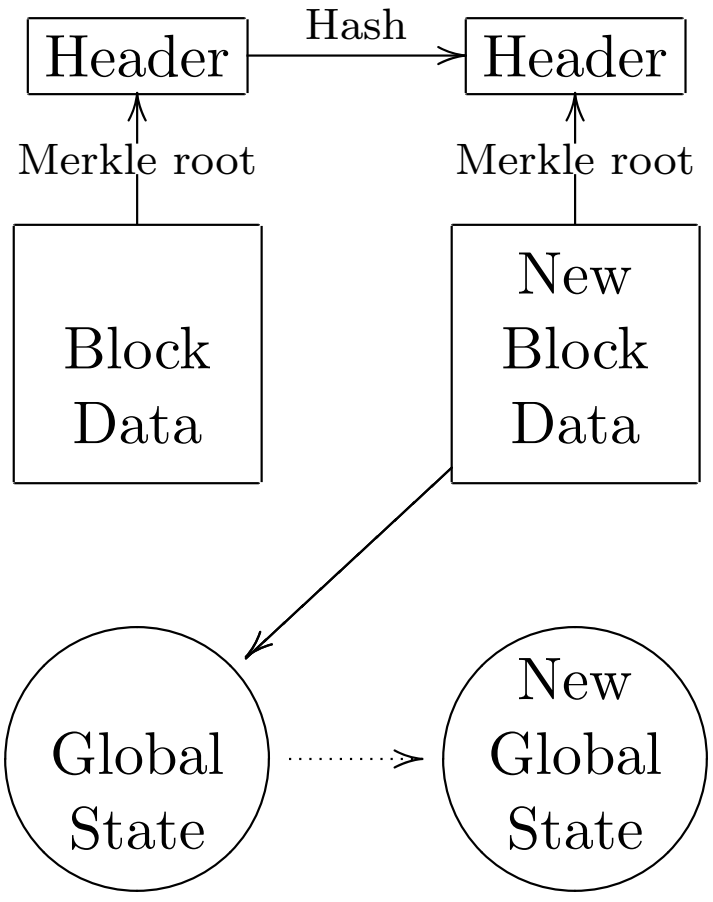
Blockchain	"Global State"
Bitcoin	Unspent Transaction Outputs (UTXO) set
Ethereum	World State†

† Section 4 of "Ethereum: A Secure Decentralized Generalized Transaction Ledger" (Petersburg version 41c1837 2021-02-14)

Abstract Blockchain

- A blockchain maintains a global state
- A block is instructions for changing a global state

Common Blockchain Architecture

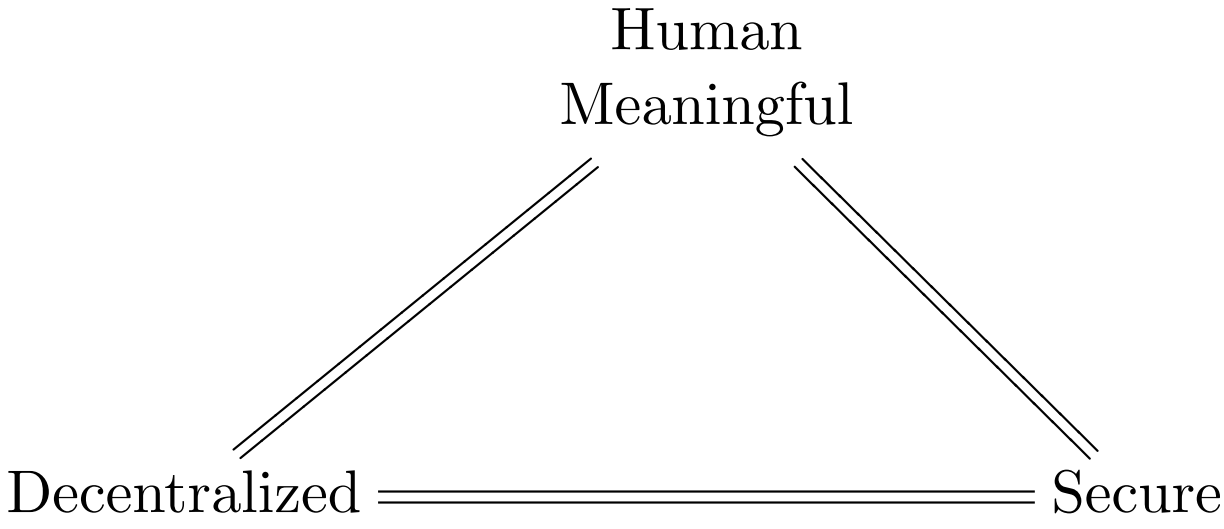


Blockchain

A blockchain is a tool.

Zooko's Triangle

Pick two:



Has Zooko's Triangle Been Solved?

Solutions of Zooko's triangle:

- Nick Szabo, "Secure Property Titles with Owner Authority" (Up to BFT)
- Namecoin (using Nakamoto Consensus)
- Etherum Name Service (uses Nakamoto Consensus)
- DIP 0005 (withdrawn, uses Nakamoto Consensus)
- Dash Platform Name Service (uses modified tindermint consensus)
- ⋮

Smart Contracts

Smart Contract

A protocol that is intended to provide a service or produce an intended effect which will be reproduced over a computer network under some type of consensus.

NOTE:

- May not be a standard definition
- May or may not be Turing complete
- A bitcoin locking script is a smart contract under this definition

Smart Contract Platforms

Smart Contract Platforms

- Bitcoin
- Ethereum
- Cardano
- Early Dash (v0.12-0.13)
- New Dash

Smart Contract Security – Bitcoin

Bitcoin Contract Security

Early Bitcoin had several opcodes disabled.

By reducing the attack surface the security can be made better.
This also reduces functionality.

Smart Contract Security – Ethereum

Ethereum Contract Security

The Ethereum platform does not allow for a contract to be altered.
Thus an attacker cannot alter the code after deployment.

Smart Contract Security – Cardano

Cardano Contract Security

Cardano uses a functional language. This means:

1. The intended behavior of the contract can be written in a formal language.
2. Proofs can be provided that code will execute consistent with formal writeup.

One would expect that this approach could prevent bugs along the lines of the Ethereum DAO hack

Dash Upgrades

I'm using the term Early Dash to refer to Dash v0.12.

I'm using the term New Dash to refer to Dash v0.18.

The security analysis fundamentally changed around v0.14.

New Dash

Dash Upgrades

- Increased Capacity (DIP-001)
- Introduction of BLS signatures
- Post-Nakamoto-Consensus Consensus v0.14
- Pre-Nakamoto-Consensus Consensus
- Platform Chain (v0.17 currently on testnet)
- Full interoperability between platform chain and core chain (scheduled for v0.18)

BLS Citations

Dan Boneh, Ben Lynn, Hovav Shacham (2004). "Short Signatures from the Weil Pairing". *Journal of Cryptology*.

Alexandra Boldyreva (2002). "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme". *Public Key Cryptography 2003 Proceedings, Lecture Notes in Computer Science Vol. 2567*.

BLS Signatures

BLS Signatures

BLS Signatures allow aggregate signatures.

Types of signatures:

- Multisignature (many keys one message)
- Threshold Signatures (m of n signature)
- Aggregate signatures (many keys and many messages)

BLS does them all!

Allows for mitigation of poison block attack.

and for "cheap."

New Dash (cont)

Dash Upgrades

- Increased Capacity (DIP-001)
- Introduction of BLS signatures
- Post-Nakamoto-Consensus Consensus v0.14
- Pre-Nakamoto-Consensus Consensus
- Platform Chain (v0.17 currently on testnet)
- Full interoperability between platform chain and core chain (scheduled for v0.18)

Store of Value Anecdote

Bitcoin's transition from peer-to-peer cash to store of value

Bitcoin's security assumptions stopped adding up. (RBF etc.)

Early Dash Security

Early Dash Security

Early Dash relied on BFT for security for extra-transaction services.

Early Dash Security

Service	Start Date	End Date
Dash DAO	Sept 7, 2015	···
ETH DAO	April 30, 2016	June 16, 2016

Dash's reduced functionality, like BTC, made more security possible.

Dash in Transition

Post-Nakamoto-Consensus Consensus
DIP-0008 (ChainLocks)

Pre-Nakamoto-Consensus Consensus
DIP-0010 (LLMQ InstantSend)

And then Dash Platform ...

Dash Platform

Dash Platform

Dash Platform is a new smart contract platform. Platform functionality utilizes a second chain separated from the core chain.

Chain Interaction

Chain interaction life cycle

1. "Money" mined
2. Small amounts burned on core chain essentially moved to platform chain for fees
3. Users pay fees for platform services and money goes to "holding pin"
4. Nodes claim fees from "holding pin"

item 4 is v0.18

Platform Security

Separating Platform services from payments has huge advantages from a security standpoint.

Dash Dating Example

Dual Security Model

Game Theory

Scaling Solution

Paying actors that run nodes changes the game theory in a way that solves Bitocin's Raspberry Pi scaling problem.

Platform Scaling

Having a separate platform chain allows scaling to be addressed in two steps

Platform chain does not need to be stored indefinitely.
Global state is a state tree.

Thank You!

Thank You!