Lecture on Mining / Consensus

Intro

Steve is Stuck in Cheyenne - so ... I am stepping in for this. My background is on the technical side ... `Thesis*` - 3rd generation consensus stuff, Ethereum contributor.

How Proof of Work works.

1. Create the Merkle hash of the block. This grantees integrity within a block.
2. Set the Nonce for the block to 0.
3. Hash the block (sha1, Keack256 or other hash)
4. See if it satisfies the “criteria” - Example.
5. If “good” - then done, else
    - Nonce = Nonce + 1
    - Loop back to (3) above.

How Proof of Stake Works creates consensus.

By using up time and work - it spends $ and hardware - taking time. Anybody that want’s to fake will have to do this. Cost is millions an hour.

Bad Data is still bad data.

Can we input bad data. Yes... but the data becomes “checkable”. Example of supply chain with aircraft parts.

Limitations on Bad Data.

Accounting and bad data.

Immutable Data.

Why is the data immutable. Block after block with links over time as hashes.

Shared Data.

Sharing the data. How that works.

Proof of Stake (Proof-of-Steak)

Why Proof of Stake - security v.s. speed.

What is a side-chain.

What is sharding.

Environmental Considerations / Performance Considerations

PoW is an environmental and performance disaster. Crypto Kitties.

Ethereum v.2.0.0 announcement

Eth will require a 32 Eth stake. Eth burnt on main Eth 1.x net, then minted on Eth2.0 net - in an Escrow account.

Ripple/Thesis (Other Consensus Algorithms)

3rd generation Byzantine Generals Solution - Honey Badger BGS. Overview of how it works.

Non-Blockchain Consensus

Fast proof of authority data.