CSCI 1800 Cybersecurity and International Relations

Bitcoins and Blockchains

John E. Savage

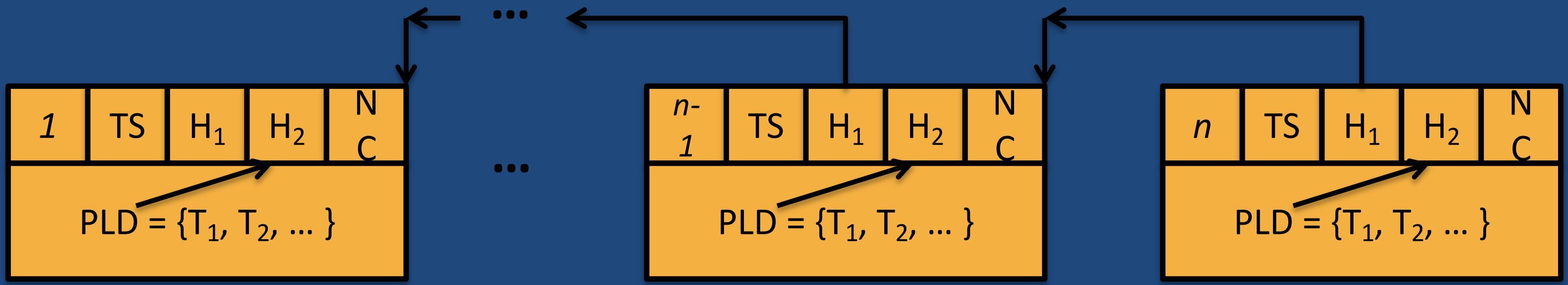
Overview

- We describe the bitcoin system, which supports monetary exchange without a central authority
- It uses a blockchain to record the exchange of Bitcoin, a cryptocurrency introduced on 1/3/2009
- While cryptocurrencies are important, blockchains may become more important
- We identify issues with blockchains that introduce important new governance questions
- Discuss governance models

What is a Cryptocurrency?

- A digital currency is a currency available only in digital form
- Currency transactions are recorded in an append-only public ledger called a blockchain, a chain of blocks
- Agents, called miners, are responsible for adding blocks to a blockchain
- Any person or group can be a miner.
- They follow rules described below.

A Generic Blockchain



- Blocks have Header & Transaction Payload (PLD)
- Header has sequence no. n, time stamp TS, hash H_1 of header of preceding block, hash H_2 of PLD, and nonce NC, solution to hard computational problem.
- If nth block PLD changes, H_2 in (n+1)st block changes, requiring H_2 in all later blocks be changed.

The Role of Miners

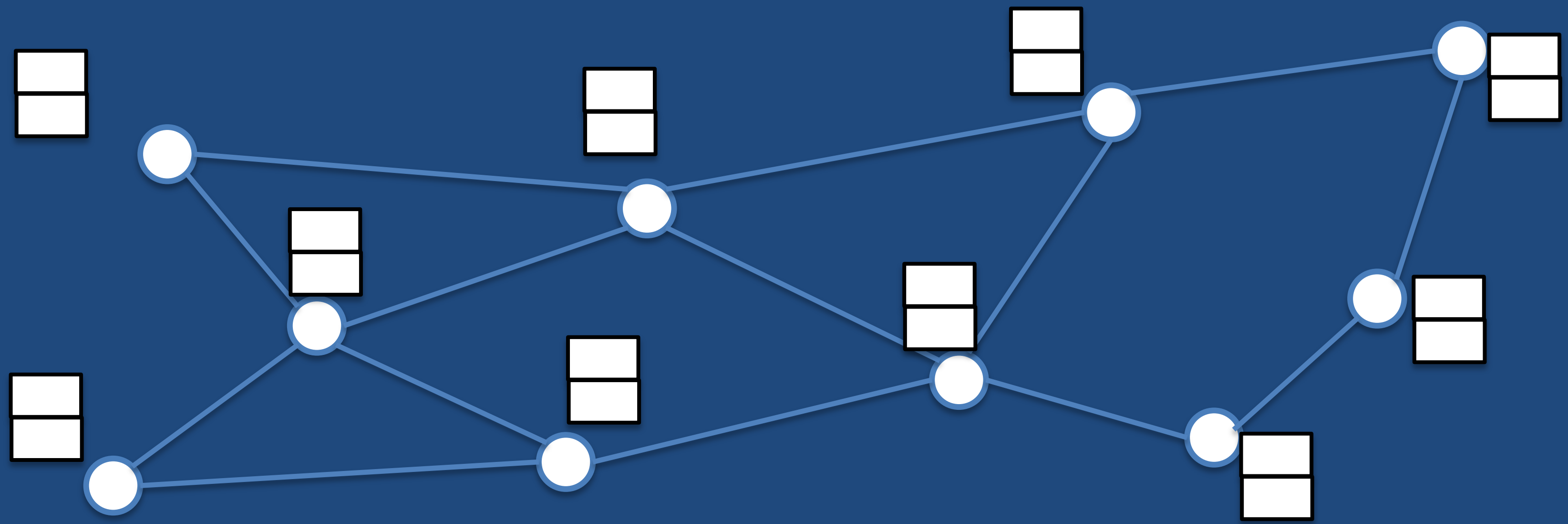
- Collect requests for new currency transfers
  - Note: Transfers have space for 😈 text.
- Ensure owners intended to make the transfers
- Solve a hard computational problem to acquire permission to add a block of bitcoin transfers to chain and receive bitcoins for their effort.
  - Note: miners must pay for power to solve problem
- Each block also has header that links it firmly (i.e., cryptographically) to the previous block

Bitcoin Enlivened Cryptocurrencies

- Bitcoin is a public digital currency
  - Goal was to replace intermediaries, e.g. banks
  - With cryptography and code
  - It uses a secure database, the blockchain
- Blockchain provides bank-type guarantees but
  - All currency transactions are public Is this a problem?
  - "Miners" validate transactions
  - A blockchain is an immutable public chain of blocks
  - Forking is possible, in which case it becomes a tree

Bitcoin Social Network

- Bitcoin miner network is overlaid on Internet



- This is a peer-to-peer network
- Normally each miner sees the same blockchain

General Blockchain Protocols

- A blockchain is a chain of blocks, with possible forking
- Blocks record transactions, e.g bitcoins, votes, real-estate
- A digital address is associated with a user transaction
  - Private keys in PKI authenticate users and their transactions
- A miner implements a protocol to add blocks:
  1. Computes proof-of-work by solving hard problem, getting NC
  2. Assembles new transactions and verifies them
  3. Creates a header and transaction payload, forming block
  4. Each new block is cryptographically linked to preceding block
  5. Transactions are immutable. Changes are detectable by all

Claims for Blockchains

- It is a revolutionary technology
- Could have an impact as large as the Internet
- Services can be completely decentralized
  - No need to trust a single organization
- Agreements can be encoded as smart contracts attached to blocks and executed automatically
- Blockchains are proposed for many tasks
  - E.g. matching buyers and sellers

Cryptocurrencies

- More than 3,000 cryptocurrencies. Examples:
  - Bitcoin, Litecoin, Ethereum, BitcoinCash, Ripple
- Claims for cryptocurrencies
  - Provide permanent public and verifiable records
  - Create decentralized trust anchors
  - Eliminate banking fees
  - Shorten time to settle banking transactions
  - Reduce obstacles to international funds transfer
  - Can exchange them for fiat currencies

The Bitcoin Protocol

- Miners agree to apply the Bitcoin protocol
- A miner computes for about 10 minutes to obtain a proof-of-work, a nonce or string, by solving a hard computational problem.
- A miner forms a block of transactions not previously recorded and adds it to blockchain
- The structure of blocks is described earlier
- System based on a public-key encryption system

Recall: Public-Key Cryptosystem

- Each participant in a public-key encryption system has a secret key, SK, and a public key, PK.
- Alice sends secret message M to Bob as follows
  - She encrypts M with Bob's public key, s = E(M, PK_{Bob})
  - Sends it to Bob
  - Bob decrypts it with his private key, M = D(s, SK_{Bob})
- Bob can "sign" message M by decrypting it with SK_{Bob}. Alice can recover M from signature by encrypting with PK_{Bob}.

Hash Functions & Bitcoin Addresses

- Recall: A hash function H
  - – Compresses strings, H(Text) = "short string"
  - – if $\text{Text}_1 \neq \text{Text}_2$ very likely that $H(\text{Text}_1) \neq H(\text{Text}_2)$
    - Thus, H(Text) is used as an "address"
  - – If $H(\text{Text}_1) = H(\text{Text}_2)$, Text_1 and Text_2 "collide".
  - – Collisions are computationally hard to find
- Bitcoins owned by addresses, i.e. hashes.
- Address A = H(PK) associated with a public key PK
  - – E.g. A = 1BtjAzWGLyAavUkbw3QsyzzNDKdtPXk95D

Bitcoin Transactions

- A transaction = transfer of Bitcoins from one address to one or more other addresses.
- Customers pay miners to process transactions
  - Some miners charge high fees
  - Or will not take small transactions
- Bitcoins make it easier to process dirty money
- Bitcoin owners are easily identified
- However, tumblers or mixing services exist
  - They break the link between addresses and owners
  - Often used for Bitcoin “laundering”

Cryptographic Signatures

- Signatures are used to authenticate senders
- Let Q have public and private keys, PK_Q, and SK_Q.
  - Sign message M: Q sends (M, σ), where σ = D(M, SK_Q)
  - Receiver encrypts σ using PK_Q giving M' = E(σ, PK_Q).
  - M' = M only if Q created the signature σ.

Proving Ownership of Address

- Alice asks Bob: Prove you own addr B = $H(PK_{Bob})$
  - They agree on a message M.
  - Bob gives PK_{Bob} to Alice as well as the signature σ of M, namely, $\sigma = D(M, SK_{Bob})$.
  - She computes $H(PK_{Bob})$ and finds is equal to B.
  - Then, if $M = E(\sigma, PK_Q)$, Alice knows that Bob owns B because only Bob could have produced σ.

Simple Bitcoin Transaction

- Alice wants to pay β Bitcoin to Bob
  - Her address is A and his is B
- Alice's transaction: $T_A = \{MSG_A, \sigma_A\}$

  $MSG_A = [A, B, PK_A, \beta]$ means

  Send β Bitcoin from A to B; use PK_A to verify A is sender

  $\sigma_A = D(MSG_A, SK_A)$, the decryption of MSG_A, is its signature

  Verify that A intended to make transfer by encrypting σ_A
- All transactions are broadcast to all participants
- Each participants can verify each transaction

Goals of Bitcoin System

- Disallow double spending – build confidence
- Establish consensus on valid transactions
- Transparency – display all transactions
    - Allow participants to keep copies of transactions
- Trust is decentralized – not centralized

Complex Transactions

- Simple transactions $T_A = \{MSG_A, \sigma_A\}$ where $MSG_A = [A, B, PK_A, \beta]$, $\sigma_A = E(MSG_A, SK_A)$

- Complex transactions
  - – Bitcoins sent from multiple sources to recipients
  - – Source and recipient amounts are specified
  - – Excess of source over recipient amounts is miner fee
- Transaction size
  - – Blocks limited to 1 MB,

Block Details

- A block contains a header HD and a payload PLD
- Header HD = [SQ, TS, K, L, NC] contains
  - – SQ: Sequence number
  - – TS: Timestamp
  - – Two cryptographic hashes, K and L
    - K: Hash H_1 of the header of the previous block
    - L: Hash H_2 of transactions in the current block
  - – NC: nonce – a solution to a cryptographic puzzle
- nth header $HD_n = [n, TS_n, H_1(HD_{n-1}), H_2(PLD_n), NC_n]$

Recap – The Bitcoin Network

- Social network maintains blockchain consensus
  - Transactions are created, posted and verified
    - Unverified transactions are discarded
  - Miners solve hard problems and add blocks
  - Blocks are verified by miners
  - Miners retain secure copies of blockchain
- Membership in network is open to all
- Mining is costly. Miners are incentivized.

Solving Puzzle

- *n*th Header $HD_n = [n, TS_n, H_1(HD_{n-1}), H_2(PLD_n), NC_n]$
- h is the SHA-256 cryptographic hash function
- The nonce NC_n must satisfy

$$h(TS_n \cdot H_1(HD_{n-1}) \cdot H_2(PLD_n) \cdot NC_n) \leq v$$

- Here v is target value adjusted every two weeks so that it takes about 10 minutes to find NC_n.
- h discovered by exhaustive search
  - – Very energy intensive

Incentivizing Miners

- Miners awarded new Bitcoins to add a new block
  - Also paid miners fees 3/9/20 about $.50/Kilobyte
- Miner award started @ 50 BTC, halves every $2.1\text{x}10^5$ blocks or about 4years. Today 12.5 BTC.
- 3/9/20 1 BTC = $7,759. Award/block ~$96,987.5
- Annual global mining revenue* ~ $5 Billion
- > 300,000 miners, Profit* < $16,000/miner/yr

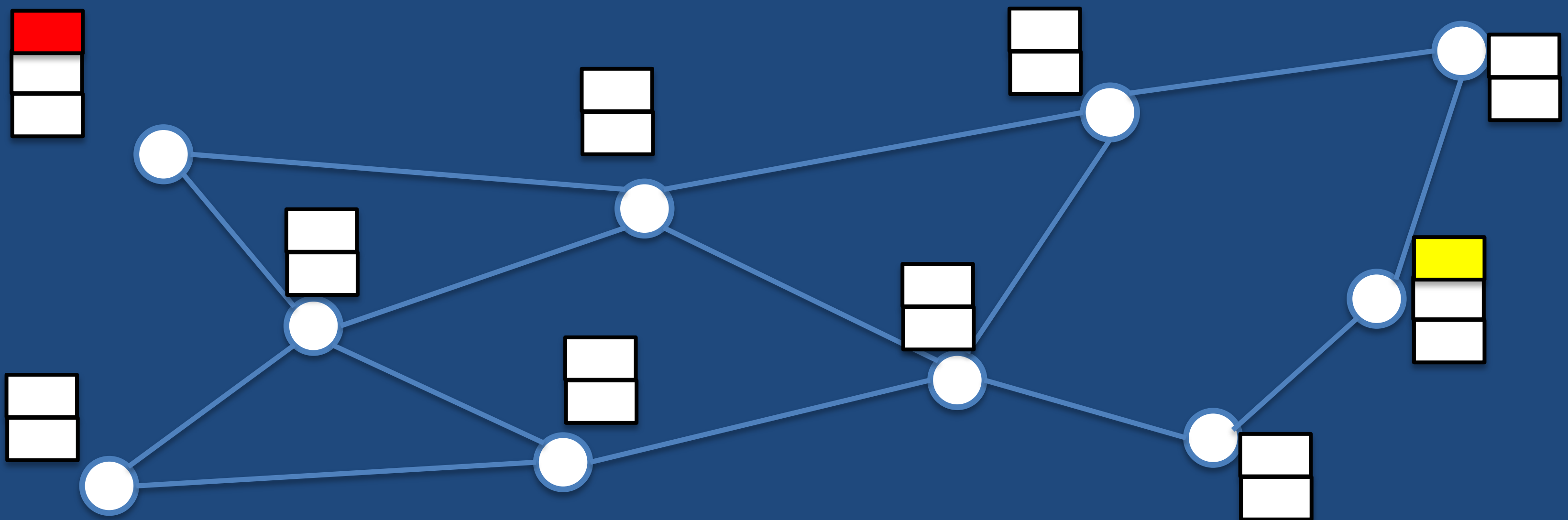
* https://www.theblockcrypto.com/linked/53425/bitcoin-miners-made-an-estimated-5-billion-in-revenue-during-2019/

Energy Dissipation

- Estimated 77 Terawatt Hours/year
- Equivalent to the electricity used by every American home over 22 days!

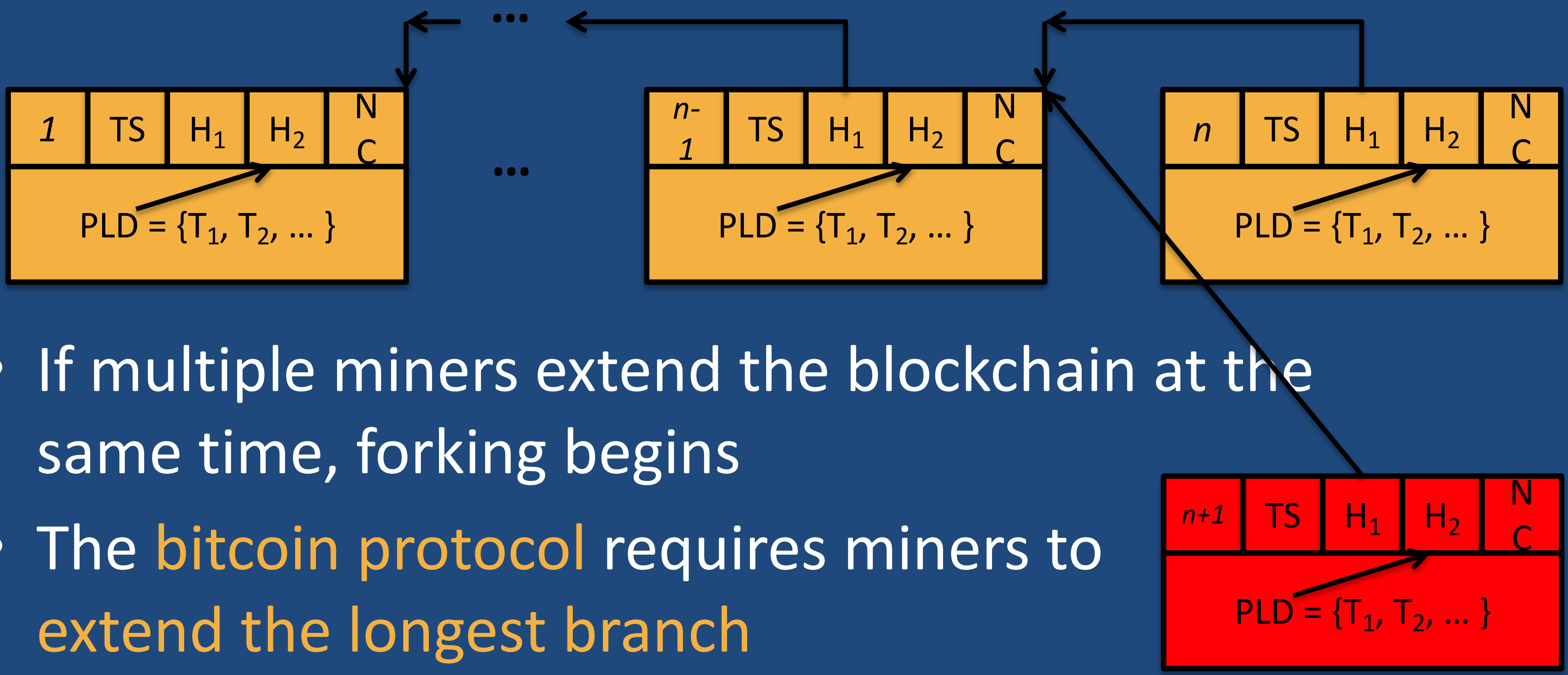
* https://digiconomist.net/bitcoin-energy-consumption

Forking Blockchain Extensions



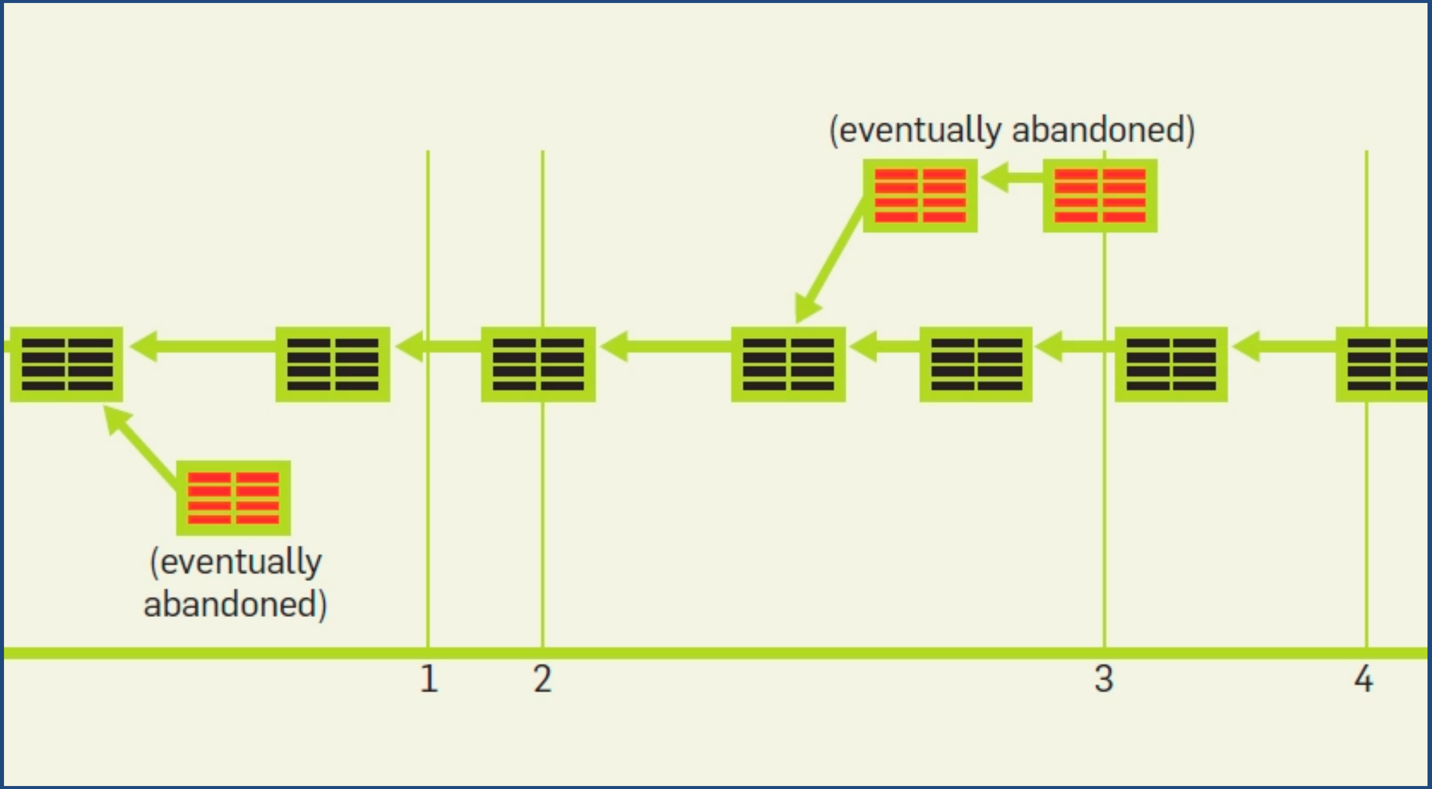
3/9/20

Blockchain Forking



- If multiple miners extend the blockchain at the same time, forking begins
- The bitcoin protocol requires miners to extend the longest branch
- Likelihood of multiple long branches is very low
- Thus, one branch wins, voiding others
- Miner awards must be confirmed 100 times!

Orphan Blocks in Blockchain Forking



See Bitcoin's Underlying Incentives by Y. Sompolinsky, A. Zohar CACM, Vol. 61 No. 3, 2018

Issues with Cryptocurrencies

Attack Against Miners

- The 51% attack
  - If entity acquires 51% of computational power it can
    - Select which transactions to include or exclude
    - Create an orphan block by branching before it
- $4.26 Billion in Bitcoin stolen from exchanges, investors and users in 2019*

* https://www.businessinsider.com/the-biggest-cryptocurrency-scams-and-arrests-of-2019-so-far-2019-8

Loss from Bitcoin Wallets

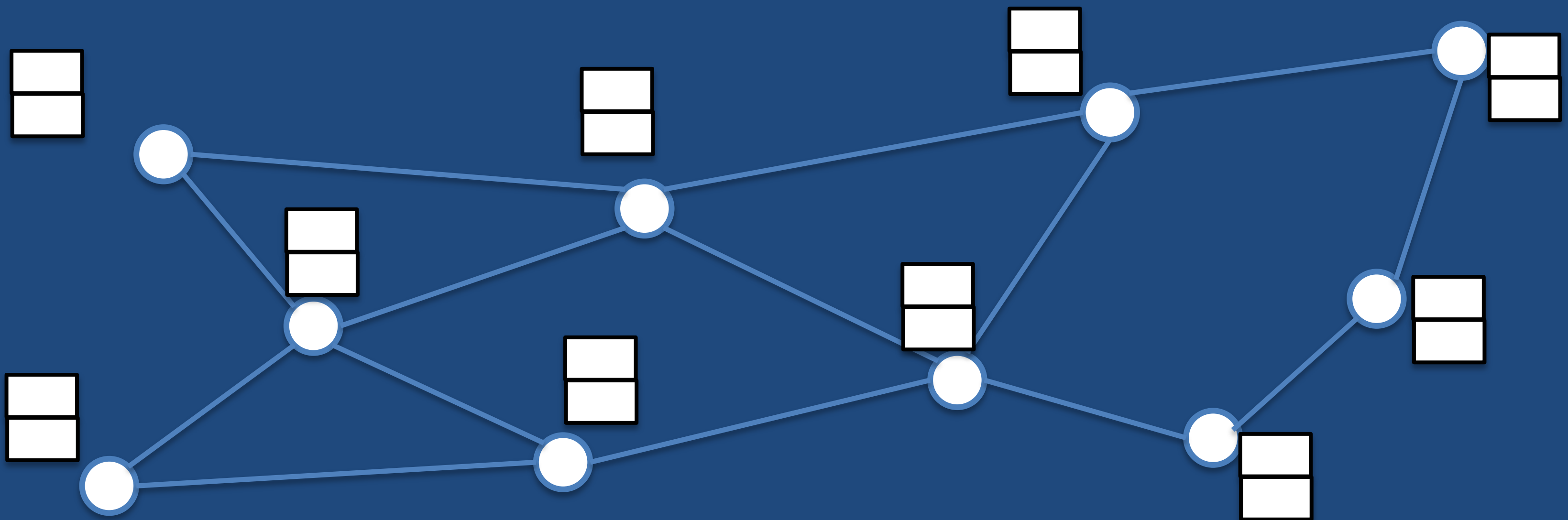
- Bitcoins are associated with an address A, such as 1BtjAzWGLyAavUkbw3QsyzzNDKdtPXk95D and a secret key SK
- Address & key are typically stored in a wallet
- In 2014 Mt. Gox, the world's largest bitcoin exchange had $450 million of customer funds stolen out of its "hot wallet" causing it to entry bankruptcy
- Owner must retain his/her key to the wallet
  - '17 Fortune* estimates $20 Billion in Bitcoin permanently lost
  - '19 Investopedia estimates 20% Bitcoins lost, unrecoverable

* http://fortune.com/2017/11/25/lost-bitcoins/

Money Laundering

- Ransomware asks for ransom in Bitcoin
- Bitcoin has been involved in money laundering
- But identities of bitcoin owners can be traced
- Technique to avoid revealing identities
  - Comingle funds from many sources in a mixing service (or tumbler) that distributes them slowly

Blockchain Peer-to-Peer Network



Bitcoin Peer-to-Peer Network

- A random topology emerges from simple rules
- A new node (miner) contacts a seed node
- It establishes connections to nodes in the network
  - Non-responding nodes forgotten after 3 hours
- Transactions and blocks propagate slowly
  - Propagation time can be 10s of seconds!
- Temporary conflicts occur
  - E.g. Double-spending or blockchain forking
- Although resolved eventually, can be abused

Eclipse Attack† Isolates Miners

- Each node in a bitcoin peer-to-peer network
  - Maintains long-lived connections to eight* peers
  - Accepts ≤ 117* incoming connections from IP addresses
- Eclipse attack monopolizes these connections
  - It has been launched with only 400 bots
  - It uses very low-rate TCP connections

† https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman

* These are configurable parameters.

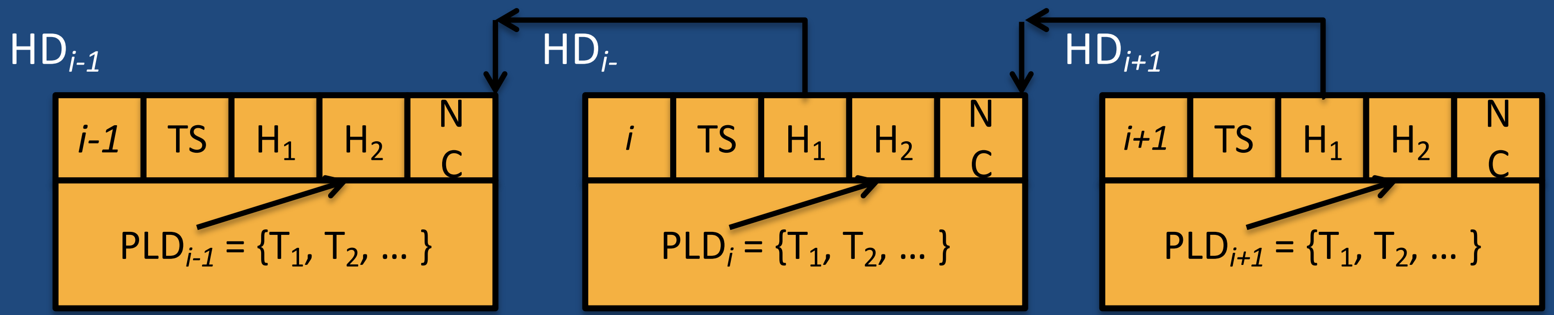
Effect on Eclipsed Miners

- Forces miners to waste effort on orphan blocks
- Makes a 51% attack much easier
- A selfish miner who eclipses others can command higher fees to process transactions
- Make double-spending of currency possible by blinding some miners

Immutability is a Problem

- Child pornography links are in bitcoin blockchain
  - This may present a legal problem for some miners
- Changes to a block may be needed, e.g.
  - Right-to-be-forgotten, sensitive information leaks
- Decentralized Autonomous Organization (DAO)
  - Was to run autonomously on smart contracts
  - $50 million hack of it required a hard fork to fix
- The Accenture-Ateniese redaction capability is proposed to edit, remove, insert or merge blocks

Accenture-Atienese Redactions



HD_{i-1}

HD_{i-}

HD_{i+1}

i-1	TS	H_1	H_2	N C

$PLD_{i-1} = \{T_1, T_2, \ldots \}$

i	TS	H_1	H_2	N C

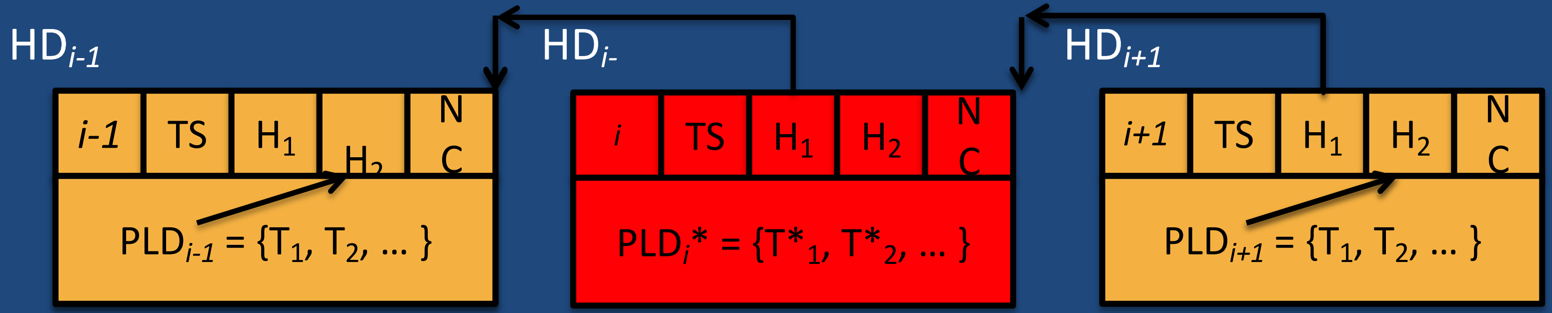
$PLD_i = \{T_1, T_2, \ldots \}$

i+1	TS	H_1	H_2	N C

$PLD_{i+1} = \{T_1, T_2, \ldots \}$

- If PLD_i in block $B_i = [HD_i, PLD_i]$ is replaced by PLD_i , $H_2(PLD_i)$ will be different and the chain is broken!

Accenture-Atienese Redactions



HD_{i-1}

HD_{i-}

HD_{i+1}

i-1 TS H_1 H_2 NC

$PLD_{i-1} = \{T_1, T_2, \ldots\}$

i TS H_1 H_2 NC

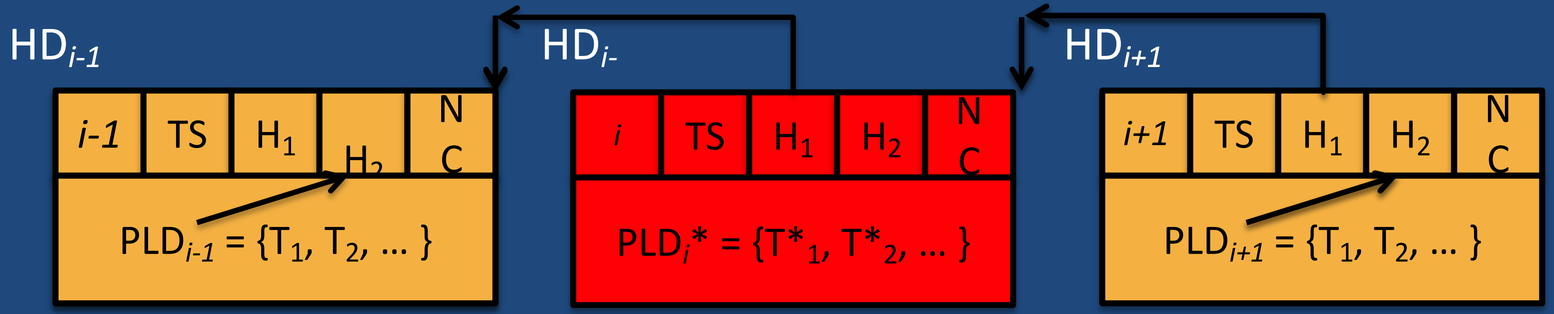
$PLD_i^* = \{T^*_1, T^*_2, \ldots\}$

i+1 TS H_1 H_2 NC

$PLD_{i+1} = \{T_1, T_2, \ldots\}$

- If in block $B_i = [HD_i, PLD_i]$ PLD_i is replaced by PLD_i $H_2(PLD_i)$ will be different and chain is broken!
- But if $H_2(PLD_i) = H_2(PLD_i)$, the header HD_{i+1} of block B_{i+1} doesn't change. PLD_i is called a collision
- For a traditional hash function H, finding a collision PLD_i for PLD_i is very difficult

Chameleon Hash Functions


HD_{i-1}
HD_{i-}
HD_{i+1}
i-1
TS
H_1
H_2
N C
$PLD_{i-1} = \{T_1, T_2, \ldots\}$
i
TS
H_1
H_2
N C
$PLD_i^* = \{T^*_1, T^*_2, \ldots\}$
i+1
TS
H_1
H_2
N C
$PLD_{i+1} = \{T_1, T_2, \ldots\}$

- A chameleon hash function has a “trapdoor,” i.e. secret key that reduces effort to find collision
- If such hash functions are used in blockchains, redactions are possible
- To avoid reliance on one secret key, a t-out-of-n secret sharing scheme can be used

Applications of Redaction

- Private blockchain
  - Write permissions issued by central authority
  - Read permissions public or restricted
- Consortium blockchain
  - Consensus decisions shared by consortium partners
- Public blockchain
  - Key shares could be allocated to big miners or states
  - In international arena, introduces new challenges!

Smart Contracts

- Vitalik Buterin added smart contracts to Ether, his new cryptocurrency:
  - He said Bitcoin programs were too primitive!
- But: $50 M hack* of DAO, Ether spinoff, in 2016
  - Hacker avoided checks while transferring funds
  - Stolen funds "retrieved" by a hard fork of DAO
- Problems:
  - Secure distributed code is much harder to write than secure serial code

* https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

Blockchain Challenges

- Theft of keys and currency
- Money laundering
- Eclipse attack on the blockchain network
- 51% attack
- BGP Hijacking
- Immutability problems
- Insecure and exploitable smart contracts

Blockchain Governance

- What issues arise in international settlements?
- Will they be dependent on technology?
  - E.g. permissioned vs permissionless blockchains
- If blockchains are editable, who will hold keys?
- What venues will be used to settle disputes?
- Who evaluates smart contracts for security and correctness?

Methods of Governance

- Bilateral, Multilateral, United Nations
- Multi-stakeholder governance
  - Very popular in some circles
  - Presumably gives voice to all stakeholders
  - Helps to energize stakeholders
  - But can result in anarchy if no rules of order
  - Voting rights must come with responsibilities
  - Important to provide avenues for minority opinions

Our Tools Shape Us

- "We shape our tools, and thereafter they shape us" – John Culkin in a Saturday Review story in 1967 describing the work of Marshall McLuhan*

- We are not good at anticipating consequences
- New technologies bring new problems
- Blockchain technologies are no different
- It is prudent to prepare ourselves

* https://mcluhangalaxy.wordpress.com/2017/09/19/a-schoolmans-guide-to-marshall-mcluhan-by-john-culkin-s-j-1967/