CSCI 1800 Cybersecurity and International Relations

Bitcoins and Blockchains

John E. Savage
Unanticipated Consequences

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.”

John Perry Barlow, founder Electronic Frontier Fdn.

• It didn’t work out this way!
• Complex Internet governance emerged
• Blockchains is the new revolutionary technology
• What policy issues does it present?

Overview of the Talk

• 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 in 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 transfers** 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

• Anyone person or group can be a miner.

• They follow rules described below.
The Role of Miners

• Collect requests for new currency transfers
• Ensure that owners intended to make the transfers
• Solve a hard computational problem to earn right to add group of transfers to a block and append the block to the blockchain
• 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
  - With cryptography and code
  - Using a *secure database*, the blockchain

- **Blockchain** provides bank-type guarantees but
  - All currency transactions are public
  - “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** authenticate users and their transactions
• A **miner** implements a **protocol** to add blocks, namely,
  – **It acquires** a proof-of-work by solving a hard problem
  – Assembles new **transactions** and verifies them
  – Creates a header which it adds to transactions, forming block
  – Each new block is cryptographically linked to a preceding block
• Transactions are immutable. Any changes are detectable by all miners
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 discussed for many tasks
  – Matching buyers and sellers
Cryptocurrencies

• More than 1,000 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 some transactions not previously recorded and adds it to **blockchain**

• The **structure** of blocks is described below

• System based on a **public-key encryption system**
Public-Key Encryption System

• 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, \( M = D(s, SK_{Bob}) \)

• Message M can also be decrypted with \( SK_{Bob} \) and encrypted with \( PK_{Bob} \) to recover M

• This observation is used to “sign” documents
Hash Functions & Bitcoin Addresses

• A hash function $H$
  – Compresses strings, $H(\text{Text}) = \text{“short string”}$
  – Likely that $H(\text{Text}_1) \neq H(\text{Text}_2)$
    • Thus $H(\text{Text})$ 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

• Bitcoin owned by an addresses that are hashes

• Address $A = H(\text{PK})$ associated w. public key PK
  – E.g. $A = 1BtjAzWGLyAavUkbw3QsyzzNDKdtPXk95D$
Bitcoin Transactions

• A **transaction** is the transfer of Bitcoins from one address to one or more other addresses.
• If the amount sent is less than amounts allocated to receivers, the remainder is a **fee to a miner**.
Bitcoin Transactions

• 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, tumbler 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 $(M, \sigma)$, where $\sigma = D(M, SK_Q)$
  – Receiver encrypts $\sigma$ using $PK_Q$ giving $M' = E(\sigma, PK_Q)$.
  – $M' = M$ only if Bob created the signature $\sigma$. 
Proving Ownership of Address

• Alice asks Bob: Prove you own addr $B = H(\text{PK}_{\text{Bob}})$
  – They agree on a message $M$. Bob gives $\text{PK}_{\text{Bob}}$ to Alice as well as the signature of $M$, namely $\sigma = D(M, \text{SK}_{\text{Bob}})$.
  – She computes $H(\text{PK}_{\text{Bob}})$ and finds it is equal to $B$. Then,
  – If $M = E(\sigma, \text{PK}_Q)$, Alice knows that Bob owns $B$. 
Simple Bitcoin Transaction

• Alice wants to pay $\beta$ 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 $\beta$ 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 $\sigma_A$
• All transactions are broadcast to all participants
• All 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 in 2010 by Satoshi Nakamoto
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

• $n$th 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
  – They are also paid fees
  – Miners fees as of 3/3 about $2.9/KB

• **Award** initially 50 BTC, halves every 210,000 blocks or about four years. **Today it is 12.5 BTC.**

• 3/3: 1 BTC = $11,440. Thus **miner award ~$143,000**

• 12/17: **US electricity to mine 1 BTC** $3,224 – $9,489
  – **Profit** $8,220 – $1,590
Energy Dissipation

• Digiconomist* estimates annual electricity consumption to mine Bitcoin and Ether to be about 54 terawatts

• The population of Greece of 11 million consumes the same amount of electricity.

* https://digiconomist.net/bitcoin-energy-consumption
Decisions by Miners

• The $n$th block contains $[\text{HD}_n, \text{PLD}_n]$
  - Header $\text{HD}_n = [n, TS_n, H_1(\text{HD}_{n-1}), H_2(\text{PLD}_n), NC_n]$
  - Payload $\text{PLD}_n = [T_1, T_2, \ldots]$ contains transactions

• All miners verify transactions and blocks by showing
  - Transaction $T_A = \{\text{MSG}_A, \sigma_A\}$ in $\text{PLD}_n$ is new
  - $T_A$ is valid, i.e. $\sigma_A$ is the correct signature of $\text{MSG}_A$
  - Address $A$ satisfies $A = H(\text{PK}_A)$ in $\text{MSG}_A = [A, B, \text{PK}_A, \beta]$
  - That $H_1(\text{HD}_{n-1})$ and $H_2(\text{PLD}_n)$ are computed correctly
  - That $NC_n$ solves the puzzle
Decisions by Miners

• Miners verify the following steps:
  – Transaction $T_A = \{\text{MSG}_A, \sigma_A\}$ in PLD$_n$ is new
  – $T_A$ is valid, i.e. $\sigma_A$ is the correct signature of $\text{MSG}_A$
  – Address $A$ satisfies $A = H(PK_A)$ in $\text{MSG}_A = [A, B, PK_A, \beta]$
  – That $H_1(HD_{n-1})$ and $H_2(\text{PLD}_n)$ are computed correctly
  – That $NC_n$ solves the puzzle

• These steps are captured in program attached to $T_A$ written in a primitive programming language
Forking Blockchain Extensions
Blockchain Forking

- If two miners extend the blockchain at the same time, forking begins.
- The bitcoin protocol requires miners to extend the longest branch.
- Likelihood of 2 long branches is very low.
- Thus, one branch wins, voiding the other.
- Miner Bitcoins 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

• The BGP hijack attack on a mining pool
  – A mining pool is a group of miners working together
  – BGP is used to implement a man-in-the-middle attack
  – $83 million stolen in 2014
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
  • Fortune* estimates $20 Billion in Bitcoin permanently lost

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
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

* These are configurable parameters.
Effect on Eclipsed Miners

• Force miners to waste effort on orphan blocks
• Makes a 51% attack is 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 on bitcoin blockchain**
  – This may present a legal problem for some miners

• Changes to a block may be required, 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
• If $\text{PLD}_i$ in block $B_i = [\text{HD}_i, \text{PLD}_i]$ is replaced by $\text{PLD}_i$, $H_2(\text{PLD}_i)$ will be different and the chain is broken!
• 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

- 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 hard to write
  – Secure serial code is hard to write, as well

* 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 about 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