Cryptocurrencies (Session I)

Computer Science and Law

Outline

- Part 1
  - “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”
- Part 2
  - “Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries”

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies

by Bonneau et al.

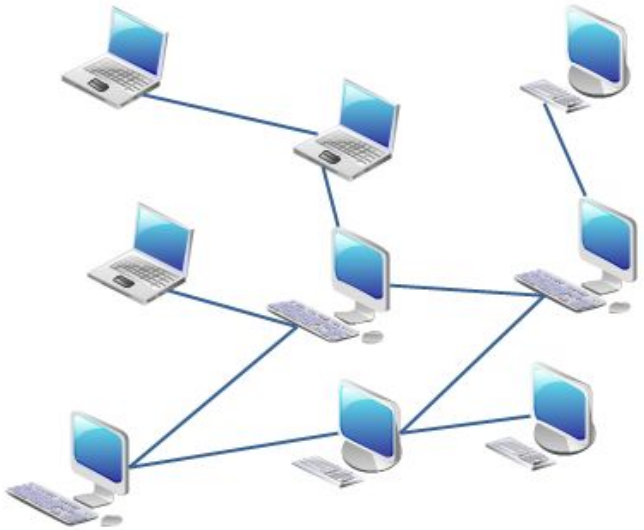
Bitcoin

- First decentralized digital currency
- Bitcoin was invented in 2008 by an unknown person or group of people under the name Satoshi Nakamoto
- In 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin
- Bitcoin provides pseudo-anonymity
    - Individuals have a public-private key pair (used for digital signatures)

Technical Overview of the Bitcoin Protocol

- All the nodes are connected by a peer-to-peer network
- Nodes maintain a digital file - ledger storing all previous transactions
- No account balances maintained on the ledger

		Digital Signature
Alice → Bob	5.0 BTC	04323784...



Technical Overview of the Bitcoin Protocol

- Each transaction references other transactions corresponding to inputs

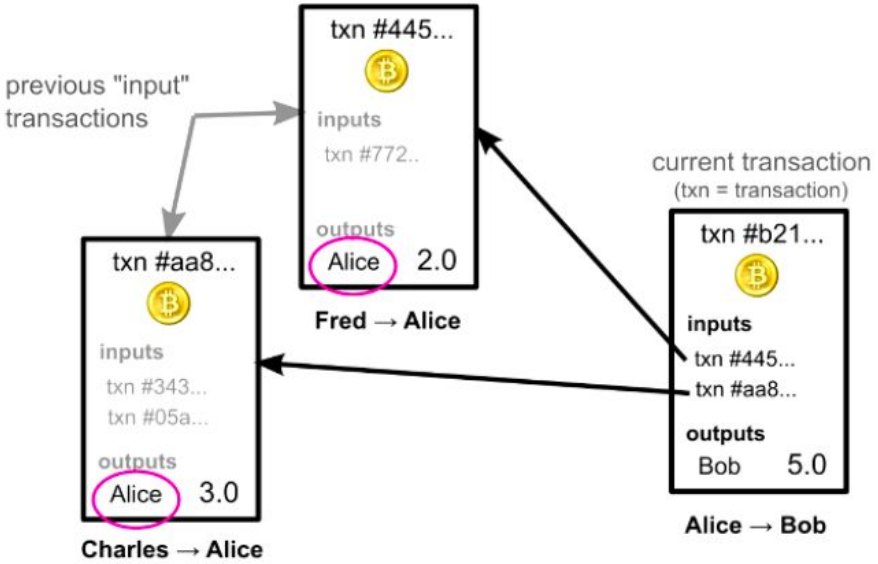


Image credit:
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Technical Overview of the Bitcoin Protocol

- Key challenge - double spending attack
- Novel consensus protocol - to impose an ordering over the transactions
- Place transactions in groups called blocks

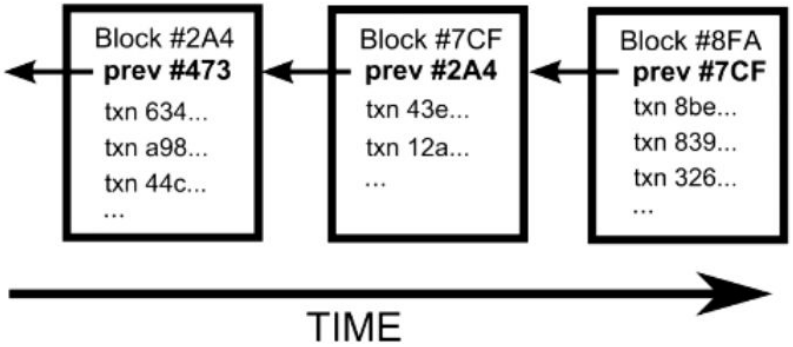


Image credit:
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Technical Overview of the Bitcoin Protocol

- Nodes maintain the longest chain

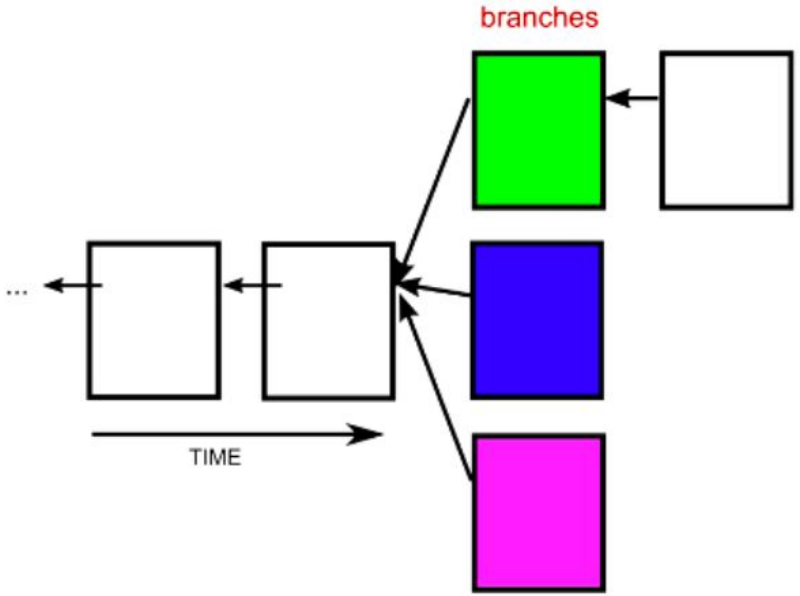


Image credit:
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Technical Overview of the Bitcoin Protocol

- Make it computationally expensive to add a block to the blockchain
- Find a nonce, such that hash (nonce,block) contains some fixed number of leading zeroes - computationally intensive
- Difficulty level set such that - one block added to the blockchain every 10 mins
- Less likely that forks exist
- Incentivization mechanism - reward miners

Stability of Bitcoin

1. Stability of transaction validity rules
2. Stability of the consensus protocol
3. Stability of mining pools
4. Stability of peer-to-peer layer

Will discuss in more detail on the first two points

1. Stability of transaction validity rules

- Baseline philosophy - preserve the rules set in by Satoshi
- Some changes have been implemented:
  - March 2013 bug fix
    - Bug limited the size of of the block
    - Created a fork in the blockchain
- Some level of governance needed for making rule changes

2. Stability of the consensus protocol

Five basic stability properties:

- Eventual consensus
- Exponential convergence
  - “k confirmation” rule
- Liveness
- Correctness
- Fairness
  - Miner with α computational power will mine blocks proportional to α

2. Stability of the consensus protocol

Stability with bitcoin-denominated utility:

- Majority compliance implies convergence, consensus and liveliness
- Majority compliance does not ensure fairness
  - Temporary block withholding strategy
- With a majority miner, stability is not guaranteed
- If miners can collude, stability is not known
- Stability not known as mining rewards decline

2. Stability of the consensus protocol

Stability with externally-denominated utility:

- Bitcoin’s observed stability in practice not explained by results in bitcoin-denominated utility model
- Three factors that affect miner’s ability to convert bitcoins into real world wealth:
  - Liquidity limits
  - Exchange rates in the face of attack
  - Long-term stake in bitcoin denominated mining rewards
- Modelling effects of exchange rates and real world utility functions more formally is an open problem

2. Stability of the consensus protocol

Stability with incentives other than monetary:

- Goldfinger attack
  - CoiledCoin altcoin was destroyed by Eligius, a bitcoin mining pool
- Feather-forking
  - A miner attempts to censor a black-list of transactions

Client-Side Security

- Users will suffer immediate and irrevocable monetary losses on losing keys
- Key management
  - Keys stored on device
  - Split control
    - k-of-n multi-signatures
    - Secret sharing the key
  - Password-protected wallets
  - Hosted wallets

Modifying Bitcoin

- Upgrading Bitcoin
  - Hard forks
    - Ex: changing block rewards
  - Soft forks
    - Requires only a majority of miners to upgrade
  - Relay policy updates
- Altcoins

Alternate Consensus Protocols

- Parameter Changes
  - Inter-block time and difficulty adjustment window
  - Limits on block and transaction size
  - Monetary policy
- Alternate Computational Puzzles
  - ASIC-resistant puzzles
    - One approach - “memory-hard” puzzles. Ex: scrypt hash function
    - ASIC-resistance is desirable?
  - Useful puzzles
    - Primecoin - generate sequence of prime numbers
  - Non-outsourceable puzzles

Alternate Consensus Protocols

- Virtual Mining
  - Proof-of-stake
  - Proof-of-deposit
  - Proof-of-burn
- Designated Authorities

Anonymity and Privacy

- Deanonymization
  - Flow of money can be traced on the public ledger
- Proposal for improving anonymity
  - Peer-to-peer network - Ex: CoinJoin
  - Altcoins with integrated unlinkability

Discussion

Some Discussion Questions

- Can bitcoin be used to carry out all types of transactions and at the same pace that a regular currency supports?
- How important is it to solve the key open problems on the stability of the bitcoin protocol before fully accepting bitcoin as a currency.
- Should mining pools be encouraged or discouraged by the bitcoin protocol?
- The role the government and regulatory bodies can/should play in general in improving the stability and efficiency of the protocol.

Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries

By Sara Jane Hughes & Stephen T. Middlebrook

Need for Regulation

- Introduction of market intermediaries
  - Custodians of cryptocurrency or cryptocurrency credentials of its clients and help them perform transactions
  - Online wallets, Exchanges, money service businesses
- Mt Gox: Bitcoin Exchange based in Japan
  - Largest bitcoin intermediary and world's leading bitcoin exchange (70% transactions handled)
  - Filed for bankruptcy protection in early 2014
  - ~ 650 million of bitcoin value lost

Need for Regulation

- Cryptocurrencies have been used for illegal activities: buying illegal drugs, money laundering, terrorist financing
- Regulation provides a degree of legitimacy
- Too much regulation can cause movement of developers to less regulated channels or jurisdictions
- Before 2013 no regulatory guidance over cryptocurrencies were issued by the federal government and the states

Actions by the Federal Government

- FinCEN’s March 2013 Guidance under the federal Bank Secrecy Act
  - Financial Crimes Enforcement Network (FinCEN)
  - Distinguished between convertible vs non-convertible and centralized vs decentralized virtual currencies
  - FinCEN's rules define certain businesses or individuals as “money services businesses” (MSBs) depending on the nature of their financial activities.
  - MSBs have registration requirements and a range of anti-money laundering, recordkeeping, and reporting responsibilities under FinCEN's regulations.

Virtual Currency

Taxonomy of Virtual Currencies

	Centralized	**Decentralized**
Convertible	e-Gold, Liberty Reserve, Second Life Linden Dollars	Bitcoin, altcoins
Non-convertible	World of Warcraft Gold and other in-game currencies, loyalty rewards, airline reward points	No examples currently exist

Actions by the Federal Government

- April 2014 Internal Revenue Service (IRS) announcement
  - Treat Bitcoin as a “property” and not as a foreign currency
  - Virtual currencies are taxable => legally obligated to report any cryptocurrencies mined, traded, or invested in last year

Regulation in Other Nations

- Limited cryptocurrency regulation
- Countries like China, Russia, Thailand and Iceland prohibit the use of Bitcoin as payments in domestic markets
- Swiss government has announced its intention to not regulate Bitcoin
- Canada - regulations similar to that of US

Product and Services with Which Cryptocurrencies may Compete or Impact

- Payment Systems
- Money Services Businesses and Money Transmission
- Broker-Dealer Registration and Compliance Requirements
- CFTC Commodities Trading Regulation
- Taxation

1. Payment Systems

- payment system refers to “an operational network that is governed by laws, rules and standards and that links bank accounts, providing the functionality for monetary exchange using bank deposits”.
- Payment systems are highly regulated in the US
  - Payment systems are regulated to provide transparency and accountability
  - Involve credit and liquidity risks

1. Payment Systems

- Customers may or may not appreciate the difference in risk levels compared to their own transaction
- Electronic fund transfer act and Federal reserve regulation E:
  - Provide consumer protection against fraud and error
  - Ex: Visa and MasterCard have policies to protect cardholders from liabilities for unauthorized transactions
  - Bticoin protocol does not address these issues
  - Regulation E does not apply to cross-border remittance transfer of beloe $15 or to entities that provide fewer than 100 transfers per year

1. Payment Systems

- Can regulate cryptocurrency market participants (i.e. miners, users and intermediaries) who facilitate payments as in a payment system
- Unfair for participants in the larger field of regulated payment systems to compete with unregulated actors
- No known US regulation for cryptocurrencies that are comparable to rules in place for payment systems
    - Dealing with errors

2. Money Services Businesses (MSB) and Money Transmitters

- Money Services Businesses (MSBs) are non-bank financial institutions (non-depository providers) that transmit or convert money.
- Like banks, they are subject to regulatory review by the Internal Revenue Service (IRS) and must be registered with the Financial Crimes Enforcement Network (FinCEN)

2. Money Services Businesses (MSB) and Money Transmitters

- Individuals who merely exchange bitcoin for goods and services (and vice versa) are merely "users" of a virtual currency, not money transmitters.
- Businesses that accept bitcoin from one person and send it to another are money transmitters, and are not exempt from money transmission regulation
- Any business/bitcoin miner that exchanges fiat currency for virtual currency - or even one virtual currency for another - is a money transmitter.

2. Money Services Businesses (MSB) and Money Transmitters

- Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) requires entities operating as MSB to:
  - Register with FinCEN
  - Establish risk-based money laundering program
  - Maintain certain records and file certain reports

2. Money Services Businesses (MSB) and Money Transmitters

- Prudential regulation of MSBs at state level:
  - Robust licensure programs
  - Require background checks on principal owners
  - Dictate types of allowed transactions

3. Broker-Dealer Registration and Compliance Requirements

- Securities Investor Protection Corporation (SIPC)
- Could be used as a framework for people who facilitate exchange of cryptocurrencies as “securities”
- Serve markey enhancing purposes, namely efficiency, transparency and accountability
- Requirements related to registration, record keeping, disclosure and investor protection, AML programs

3. Broker-Dealer Registration and Compliance Requirements

- Online wallet operators and exchanges in the cryptocurrency industry do not have comparable regulatory requirements
  - customers are exposed to higher credit and liquidity risks

4. CFTC Commodities Trading Regulation

- CFTC - Commodities Futures Trading Commision
- Classify cryptocurrency as “commodities” rather than “foreign currency”
- Securities vs Commodities
  - Purchasing stock buys a share in a corporation's ownership and control.
  - Purchasing commodities is to buy goods themselves before they actually exist. The buyer agrees to purchase so many units of a good at a set price to be delivered much later.
- Commodities trading regulation is similar to securities broker-dealer trading regulation

5. Taxation

- How to tax value transfers
  - Ordinary income for sellers of goods and services
  - Capital income from selling securities or commodities
- According to Internal Revenue Service (IRS) cryptocurrencies must be treated as “property” for taxation purposes
- Criticism: makes cryptocurrency useless for online commerce

BitLicense

- In 2014, New York Department of Financial Services (NYDFS) proposed a framework “BitLicense” for regulating cryptocurrencies
- BitLicense required if any one of the following types of activities involving New York or a New York Resident:
  - Receiving Virtual Currency for Transmission or Transmitting Virtual Currency
  - Storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
  - Buying and selling Virtual Currency as a customer business;
  - Performing Exchange Services as a customer business;
  - Controlling, administering, or issuing a Virtual Currency.
- The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity.

BitLicense

- Rules to follow on receiving a license:
  - Anti-money laundering rules which might or might not go beyond what’s already required by existing laws.
  - Follow some cyber security guidelines and have a disaster recovery plan
  - Record keeping — keep records, and make them available to the NYDFS under certain circumstances.
  - Designate a compliance officer —someone within your organization who's in charge of compliance and has the necessary responsibility and authority.
  - Disclose risk to consumers, so that consumers understand the risks of doing business with you.

Discussion

Some Discussion Questions

- The good and bad of the "BitLicense" regulation.
- Should holding cryptocurrencies constitute as deposits?
- Bitcoins share features with currency, commodities and payment systems. How can a framework for regulating bitcoin be derived from the regulatory treatment of currencies, commodities and payment systems.