BLOCKCHAIN & NETWORKS

Reading

Chicago Fed Letter

- Bitcoin: A primer by François R. Velde, senior economist
- http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf
- A casual reading (much less technical)

The original BitCoin paper

- http://bitcoin.org/bitcoin.pdf
- Published online with source code

Online Transactions

- Physical cash
  - Non-traceable (well, mostly!)
  - Secure (mostly)
  - Low inflation
- Can't be used online directly
- Electronic credit or debit transactions
  - Bank sees all transactions
  - Merchants can track/profile customers

What is Bitcoin?

A cryptocurrency is based on digital cryptography

Derives trust from

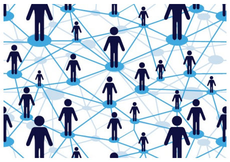
- NOT from legal tender statutes
- NOT from chemical/physical properties
- mathematical properties
- based on established, trusted, cryptographic principles
  - cryptographic hashing
  - digital signatures
  - public key infrastructure

Cryptocurrency: Challenges

- All virtual currency must address the following challenges:
  - Creation of a virtual coin/note
    - How is it created in the first place?
    - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
  - Validation
    - Is the coin legit? (proof-of-work)
    - How do you prevent a coin from double-spending?
- BitCoin takes a infrastructure-less approach
  - Rely on proof instead of trust
  - No central bank or clearing house

BitCoin

- Released by Satoshi Nakamoto 2008, launched in 2009
- A Peer-to-peer Electronic Cash System
  - A distributed, decentralized digital currency system
  - Effectively a bank run by an ad hoc network
    - decentralized
    - distributed
    - democratic
    - without the existence of a central authority



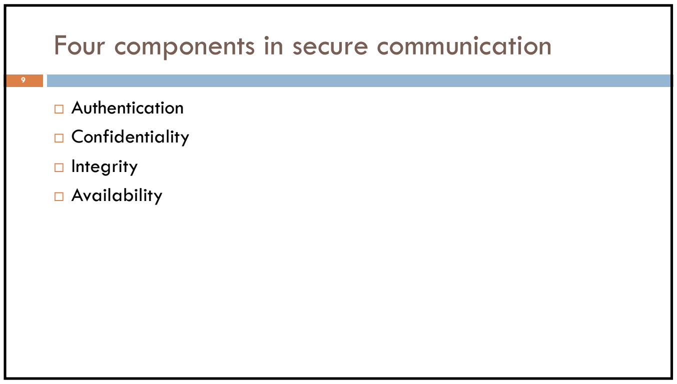
- Why study BitCoin?
  - Virtual currency captures many aspects of network&security in its requirement.
  - New form of currency that may take off or even replace existing currencies.
    - Numerous papers in Economics and Computer Science.

Size of the BitCoin Economy

- Number of BitCoins in circulation 16.9 million (December 2017)
- Total number of BitCoins generated cannot exceed 21 million
- Average price of a Bitcoin (over the previous 6 months): around $11,053.67
  - 1 BTC = 1000 USD (Dec. 1, 2013)
  - Price is very unstable.
- Total balances held in BTC >3.6B$ compared with 1,200B$ circulating in USD
- 550,000 Transactions per day (Visa transaction 200,000 per minute.)

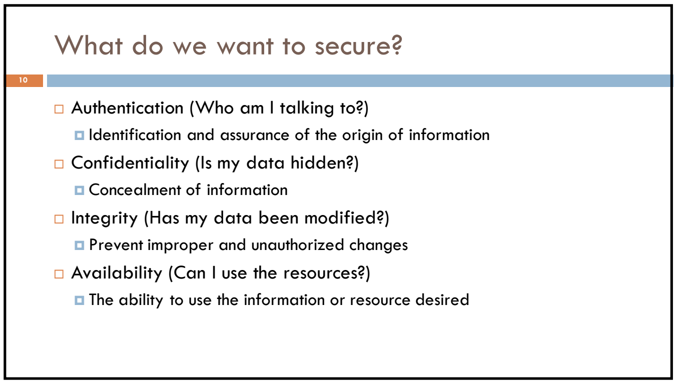
Overview of Today's Lecture

- Intro to BitCoin (non-technical)
- Security Overview
- BitCoin: Technical Details
- The practice of mining BitCoins (system's perspectives)



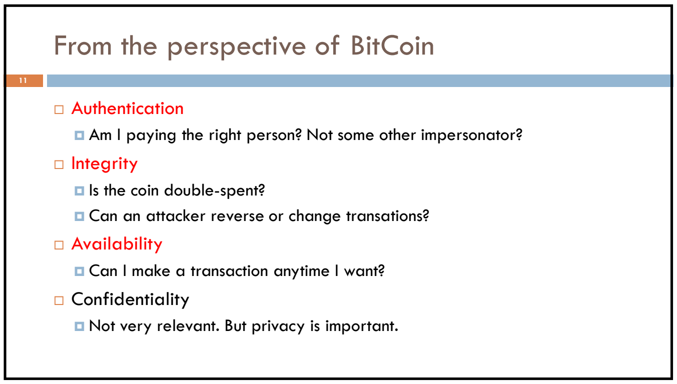
Four components in secure communication

- Authentication
- Confidentiality
- Integrity
- Availability



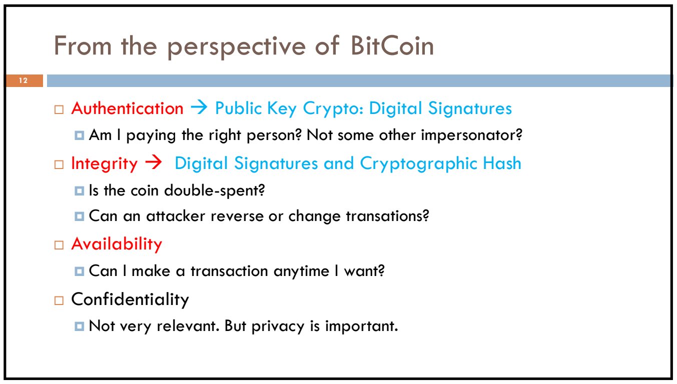
What do we want to secure?

- Authentication (Who am I talking to?)
  - Identification and assurance of the origin of information
- Confidentiality (Is my data hidden?)
  - Concealment of information
- Integrity (Has my data been modified?)
  - Prevent improper and unauthorized changes
- Availability (Can I use the resources?)
  - The ability to use the information or resource desired



From the perspective of BitCoin

- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transations?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Not very relevant. But privacy is important.



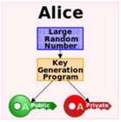
From the perspective of BitCoin

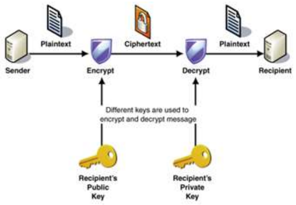
- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transations?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Not very relevant. But privacy is important.

Public Key Crypto: Encryption

13

- Key pair: public key and private key





Public Key Crypto Example: RSA

14

- RSA Keygen
  - Choose two distinct prime numbers *p* and *q*. (Let $n = pq$.)
  - Compute $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$, where ϕ is Euler's totient function.
    - $\phi(n)$: the number of integers *k* in the range $1 \le k \le n$ for which gcd$(n, k) = 1$.
  - Choose a coprime of $\phi(n)$, e, such that $1 < e < \phi(n)$, i.e., gcd$(e, \phi(n)) = 1$
  - Solve for *d* where $d \cdot e \equiv 1 \pmod{\phi(n)}$
- Public key (*n*, e); Private key (*n*, *d*)

Public Key Crypto Example: RSA

15

- Public key (*n*, e); Private key (*n*, *d*)

  Encryption: Compute ciphertext $C = m^e$ (**mod** *N*). (public key)

  Decryption: Recover m $= C^d$ (**mod** *N*). (private key)

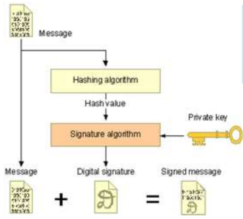
$$m^{ed} = \underbrace{m^{(ed-1)}m = m^{h(p-1)(q-1)}}_{ed \equiv 1 \pmod{(p-1)(q-1)}} m = \underbrace{(m^{p-1})^{h(q-1)}m \equiv 1^{h(q-1)}}_{\text{Fermat's Little Theorem}} m \equiv m \pmod{p},$$

- Why does this work?
  - Factorization is hard; given n hard to infer p and q.
  - Computing *m* is hard given the public key (*n*, e) and a ciphertext $C \equiv m^e$ (**mod** *N*).

Public Key Crypto: Digital Signature

16

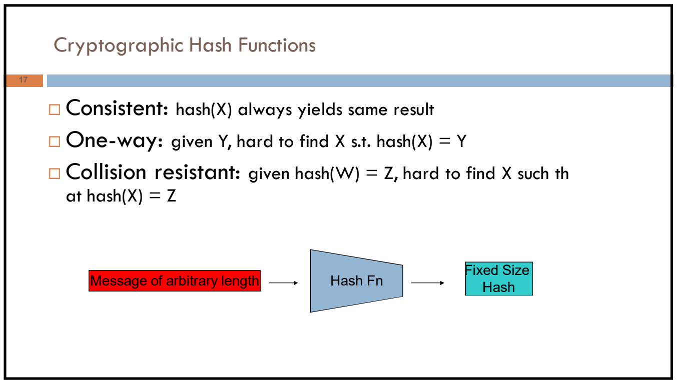
- First, create a message digest using a cryptographic hash
- Then, encrypt the message digest with your private key



Authentication

Integrity

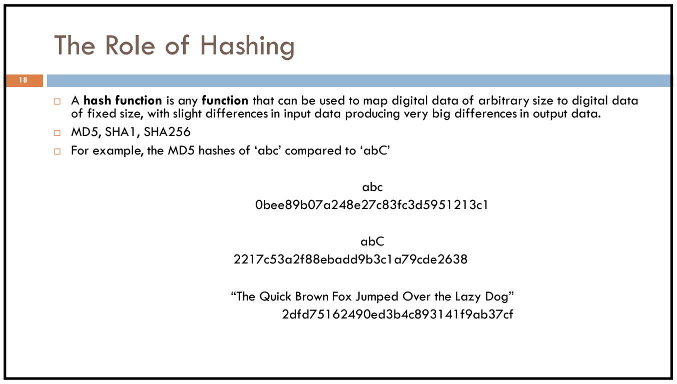
Non-repudiation



Cryptographic Hash Functions

- □ **Consistent:** hash(X) always yields same result
- □ **One-way:** given Y, hard to find X s.t. hash(X) = Y
- □ **Collision resistant:** given hash(W) = Z, hard to find X such th at hash(X) = Z

Message of arbitrary length
Hash Fn
Fixed Size Hash



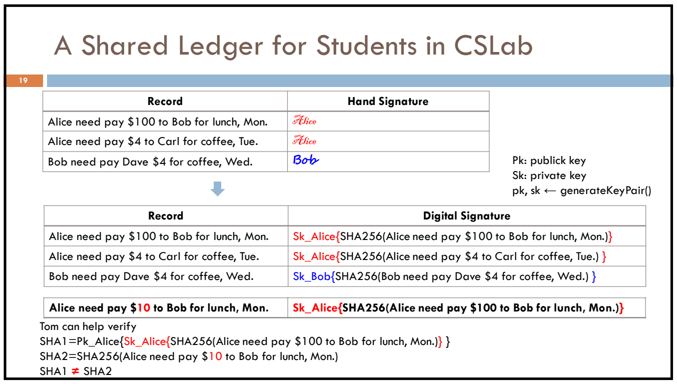
The Role of Hashing

- □ A **hash function** is any **function** that can be used to map digital data of arbitrary size to digital data of fixed size, with slight differences in input data producing very big differences in output data.
- □ MD5, SHA1, SHA256
- □ For example, the MD5 hashes of ‘abc’ compared to ‘abC’

abc
0bee89b07a248e27c83fc3d5951213c1

abC
2217c53a2f88ebadd9b3c1a79cde2638

“The Quick Brown Fox Jumped Over the Lazy Dog”
2dfd75162490ed3b4c893141f9ab37cf



A Shared Ledger for Students in CSLab

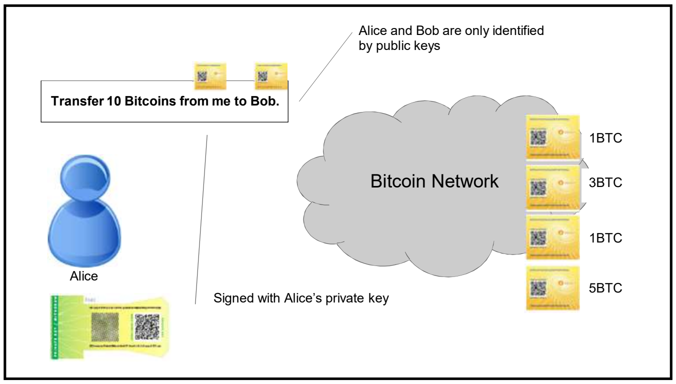
Record	Hand Signature
Alice need pay $100 to Bob for lunch, Mon.	Alice
Alice need pay $4 to Carl for coffee, Tue.	Alice
Bob need pay Dave $4 for coffee, Wed.	Bob

Pk: publick key
Sk: private key
pk, sk ← generateKeyPair()

Record	Digital Signature
Alice need pay $100 to Bob for lunch, Mon.	Sk_Alice{SHA256(Alice need pay $100 to Bob for lunch, Mon.)}
Alice need pay $4 to Carl for coffee, Tue.	Sk_Alice{SHA256(Alice need pay $4 to Carl for coffee, Tue.) }
Bob need pay Dave $4 for coffee, Wed.	Sk_Bob{SHA256(Bob need pay Dave $4 for coffee, Wed.) }

Alice need pay $10 to Bob for lunch, Mon.	**Sk_Alice{SHA256(Alice need pay $100 to Bob for lunch, Mon.)}**

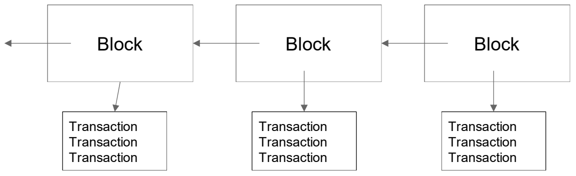
Tom can help verify
SHA1=Pk_Alice{Sk_Alice{SHA256(Alice need pay $100 to Bob for lunch, Mon.)} }
SHA2=SHA256(Alice need pay $10 to Bob for lunch, Mon.)
SHA1 ≠ SHA2



Alice and Bob are only identified by public keys

Transfer 10 Bitcoins from me to Bob.

Signed with Alice’s private key



One block every 10 minutes

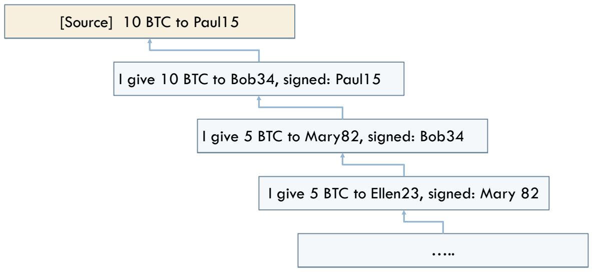
Generate a new Block--Miner

- Step1: new_block_content = SHA256(previous block) + Information of this new block + transactions of this new block
- Step 2: find a random number N such that SHA256(new_block_content +N) has 72 leading 0
  - In 10 min, normally one miner will success finding N
  - Prob=$\frac{1}{2^{72}}$, averagely doing 2^{72} calculation may find one N
- Step 3: broadcast new_block= SHA256(previous block) + Information of this new block + transactions of this new block + N
- Miner incentive: awarded with bitcoin or transaction fee

Verify a new Block

- Any node received the broadcasted new_block=SHA256(previous block) + Information of this new block + transactions of this new block + N
  - Verify SHA256(new_block) has 72 leading 0
  - Verify the block contents: transactions, BlockChain info
  - Append this new block to the end of existing chain

A Chain of Transactions



[Source] 10 BTC to Paul15

I give 10 BTC to Bob34, signed: Paul15

I give 5 BTC to Mary82, signed: Bob34

I give 5 BTC to Ellen23, signed: Mary 82

…..

Overview of Today’s Lecture

- Intro to BitCoin (non-technical)
- Security Overview
- BitCoin: Technical Details
- The practice of mining BitCoins (system’s perspectives)

Back to BitCoins

- Validation
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → Broadcast to all nodes
- Creation of a virtual coin/note
  - How is it created in the first place? → Provide incentives for miners
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins

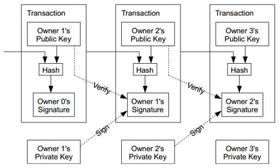
Decentralized

- The “digital wallet” operates in a peer to peer mode
- When it starts it bootstraps to find other wallets
  - Originally it used the Internet Relay Chat (IRC) network
  - Now based on DNS and “seed nodes”
- The wallet will synchronize with the network by downloading ALL of th e transactions starting from the GENESIS block if necessary
  - 506,006 blocks at time of slide prep (2018)
  - Over 160 GB
- Using a “gossip protocol” the wallets share all transaction information with their peers http://en.wikipedia.org/wiki/Gossip_protocol

BitCoin

- Electronic coin == chain of digital signatures
- BitCoin transfer: Sign(Previous transaction + New owner’s public key)
- Anyone can verify (n-1)th owner transferred this to the nth owner.
- Anyone can follow the history

Given a BitCoin

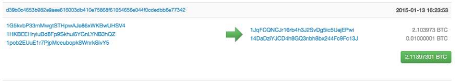


Pseudo Anonymous

- □ Using public key cryptography, specifically Elliptic Curve Cryptography due to its key strength and shorter keys

- □ Transactions are sent to public key “addresses”

  1AjYPi8qryPCJu6xgdJuQzVnWFXLmxq9s3



d39b0c4653b982e9aee616003db410e75868f61054656e044f0cdedbb6e77342 2015-01-13 16:23:53

1G5kvbP33mMwgtSTHpwAJe86xWKBwUHSV4
1HKBEEHryiuBd8Fp9Skhui6YGnLYNB3hQZ
1pob2EUuE1r7PjpMceubopkSWnrkSivY5

→ 1JqFCQNCJr16rb4h3J2SvDg5ic5UejEPwi 2.103973 BTC
14DaDziYJCD4h8GQ3nbh8bx244Fc9Fc13J 0.01000001 BTC

2.11397301 BTC

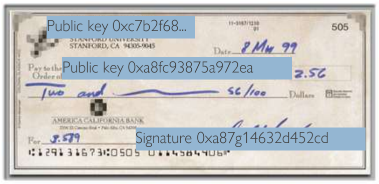
Addresses are like Accounts

- □ The wallet listens for transactions addressed to any of its public keys and in theory is the only node that is able to decrypt and accept the transfer

- □ “Coins” are “sent” by broadcasting the transaction to the network which are verified to be viable and then added to a block

- □ Keys can represent a MULTI-SIG address that requires a N of M private keys in order to decrypt the message

Bitcoin Transactions



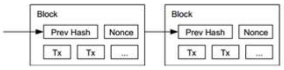
Public key 0xc7b2f68...

Public key 0xa8fc93875a972ea

Signature 0xa87g14632d452cd

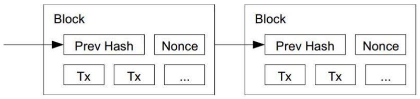
Public Ledger ← Shared Ledger for Students in CSLab

- □ Every *viable* transaction is stored in a public ledger
- □ Transactions are placed in blocks, which are linked by SHA256 hashes.
- □ https://blockchain.info



Use of Cryptographic Hashes

- Proof-of-work
  - Block contains transactions to be validated and previous hash value.
  - Pick a nouce such that H(prev hash, nounce, Tx) < E. E is a variable that the system specifies. Basically, this amounts to finding a hash value who's leading bits are zero. The work required is exponential in the number of zero bits required.
  - Verification is easy. But proof-of-work is hard.



Preventing Double-spending

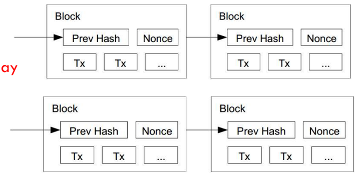
- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the BitCoin by the payer.
- Only when it is verified it generates the proof-of-work and attatch it to the current chain.

BitCoin Network

- Each P2P node runs the following algorithm [bitcoin]:
  - New transactions are broadcast to all nodes.
  - Each node collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Tie breaking

- Two nodes may find a correct block simultaneously.
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

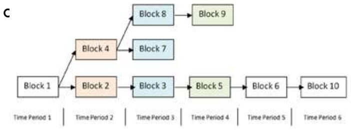


Two different block chains (or blocks) may satisfy the required proof-of-work.

Arriving at Consensus

37

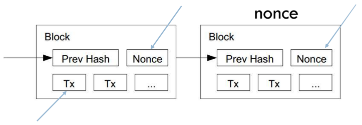
- Although the accepted chain can be considered a list, the block chain is best represented with a tree.
- The longest path represents the accepted chain.
- A participant choosing to extend an existing path in the block chain indicates a vote towards consensus on that path. The longer the path, the more c



Reverting is hard…

38

- Reverting gets exponentially hard as the chain grows.



2. Recompute nonce

3. Recompute the next nonce

1. Modify the transaction (revert or change the payer)

Practical Limitation

39

- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer. Because if you wait longer it becomes more secure. For large $$$, you wait for six blocks (1 hour).
- Fiduciary currency
  - No intrinsic value.

Implementation issues

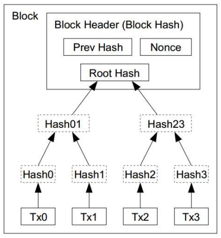
40

- Broadcast
- Keeping track of node membership
- Creating a block
  - How do you agree on which transactions go into a block?
  - What if they are different?
  - What if you cheat by including a small number of transactions and start mining early?
- Not answered in the paper. But, perhaps the implementation addresses this in part ➔ Topic for more research.

Optimizations

41

- Merkle Tree
  - Only keep the root hash
    - Delete the interior hash values to save disk
    - Block header only contains the root hash
    - Block header is about 80 bytes
    - 80 bytes * 6 per/hr * 24 hrs * 365 = 4.2 MB/year

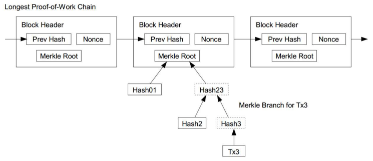


Transactions Hashed in a Merkle Tree

Simplified payment verification

42

- Any user can verify a transaction easily by asking a node.
- First, get the longest proof-of-work chain
- Query the block that the transaction to be verified (tx3) is in.
- Only need Hash01 and Hash2 to verify; not the entire Tx's.



BitCoin Economics

43

- Rate limiting on the creation of a new block
  - Adapt to the "network's capacity"
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25.
  - Halved every 210,000 blocks (every four years)
  - Thus, the total number of BitCoins will not exceed 21 million. (After this miner takes a fee)

Privacy Implications

44

- No anonymity, only pseudonymity
- All transactions remain on the block chain– indefinitely!
- Retroactive data mining
  - Target used data mining on customer purchases to identify pregnant women and target ads at them
    (NYT 2012), ended up informing a woman' s father that his teenage daught er was pregnant
  - Imagine what credit card companies could do with the data

Overview of Today's Lecture

45

- Intro to BitCoin (non-technical)
- Security Overview
- BitCoin: Technical Details
- The practice of mining BitCoins (system's perspectives)

Image/data from http://www.tomshardware.com/reviews/bitcoin-mining-make-money,3514-4.html

46

- GPU: Radeon HD 6990 about 700 MH/s
- Butterfly Labs:
  - FPGA, ASIC

Summary

47

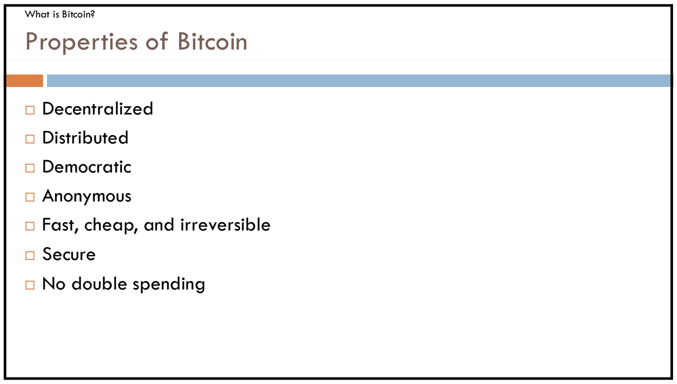
- BitCoin combined techniques from crypto and the right incentives.
  - Nice design
  - A trait for popular systems
- BitCoin is becoming industrialized.
  - Miners form a pool.
  - Mining hardware becomes sophisticated.
  - BitCoin exchange
    - Derivative market, etc.
  - Government agencies are keeping an eye on them.
- Who will control BitCoin in the end?

Bitcoin Protocol

48

- A **protocol** that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency*
- A **public**ly disclosed linked **ledger** of transactions stored in a blockchain
- A **reward** driven system for achieving **consensus** (mining) based on "Proofs of Work" for helping to secure the network
- A "scare token" economy with an eventual cap of about 21M bitcoins

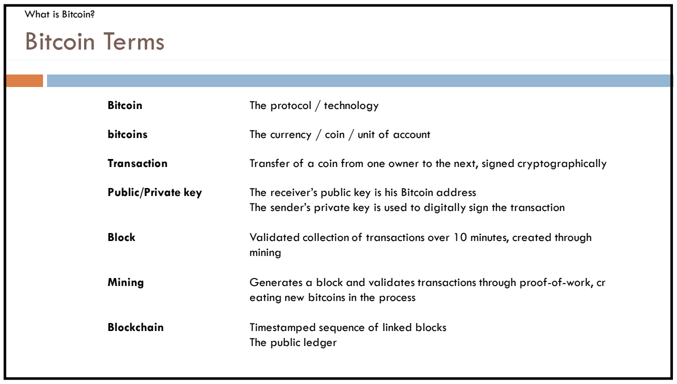
** I would argue it behaves more like a security like a Stock or Bond than a currency, a crypto-equity*



What is Bitcoin?

Properties of Bitcoin

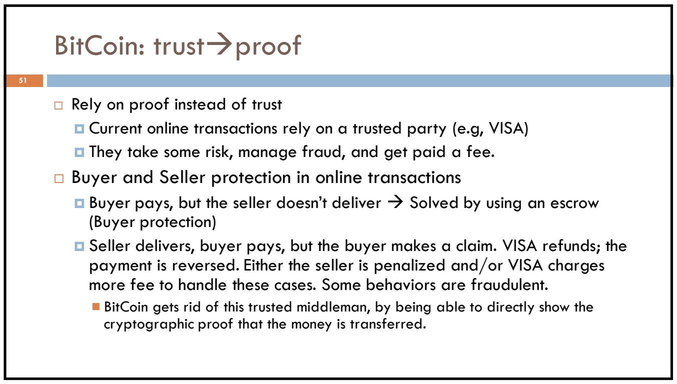
- Decentralized
- Distributed
- Democratic
- Anonymous
- Fast, cheap, and irreversible
- Secure
- No double spending



What is Bitcoin?

Bitcoin Terms

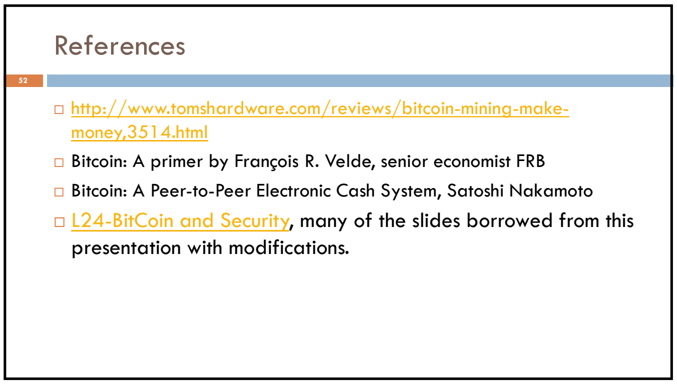
Bitcoin	The protocol / technology
bitcoins	The currency / coin / unit of account
Transaction	Transfer of a coin from one owner to the next, signed cryptographically
Public/Private key	The receiver's public key is his Bitcoin address The sender's private key is used to digitally sign the transaction
Block	Validated collection of transactions over 10 minutes, created through mining
Mining	Generates a block and validates transactions through proof-of-work, cr eating new bitcoins in the process
Blockchain	Timestamped sequence of linked blocks The public ledger



BitCoin: trust→proof

51

- Rely on proof instead of trust
  - Current online transactions rely on a trusted party (e.g, VISA)
  - They take some risk, manage fraud, and get paid a fee.
- Buyer and Seller protection in online transactions
  - Buyer pays, but the seller doesn't deliver → Solved by using an escrow (Buyer protection)
  - Seller delivers, buyer pays, but the buyer makes a claim. VISA refunds; the payment is reversed. Either the seller is penalized and/or VISA charges more fee to handle these cases. Some behaviors are fraudulent.
    - BitCoin gets rid of this trusted middleman, by being able to directly show the cryptographic proof that the money is transferred.



References

52

- http://www.tomshardware.com/reviews/bitcoin-mining-make-money,3514.html
- Bitcoin: A primer by François R. Velde, senior economist FRB
- Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
- L24-BitCoin and Security, many of the slides borrowed from this presentation with modifications.