

Bitcoin and Blockchain:

A Combination of Technology and Finance

Larry Schroth
Director of IT
GMIS Illinois
Village of Palatine

Small Business Owner



Who is GMIS Illinois?



- GMIS Illinois is an association which provides a common forum for local government technology professionals to:
 - Collaborate
 - Education
 - Innovate
- GMIS Illinois consists of over 115 agencies comprised of Villages, Cities, Counties, libraries, school districts and other public sector partners

What Can GMIS Illinois Do For You?



Stop reinventing the wheel!

- Share technology evaluations
- Share cost-effective practices
- Survey members on relevant issues
- Share Requests for Qualifications or Proposals and bids
- Provide opportunities for vendors and industry leaders to educate members in an impartial and ethically sound environment
- Serve as a resource on technology related legislation and government technology policy
- Provide training and educational opportunities

For More Information



Visit

<http://www.gmisillinois.org>

Or

Info@GMISIllinois.org

Without money



- Transactions require double coincidence of wants.
- “Prices” are subjective and extremely variable.
- Transaction costs are high.

When is money needed?



- Economies grow too large
- Labor specializes too much
- Transactions become too complicated

What is money?

- Anything that is generally acceptable as payment for goods and services or for repayment of debts.



Kinds of money?



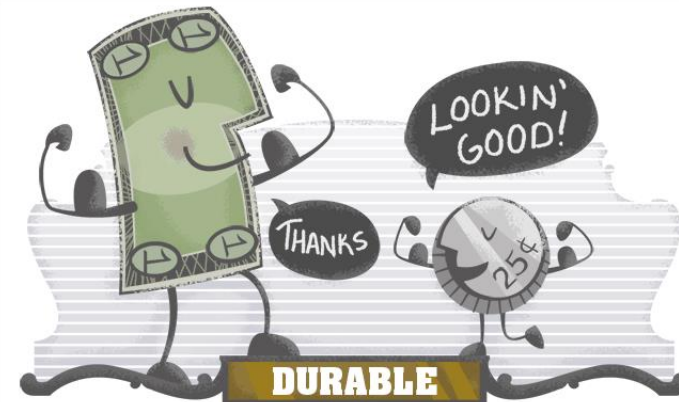
- Commodity money
- Representative money
- Fiat money

Who needs money?



- Nations
- Groups of nations
- Communities
- Prisons
- The Internet?

Characteristics of money?



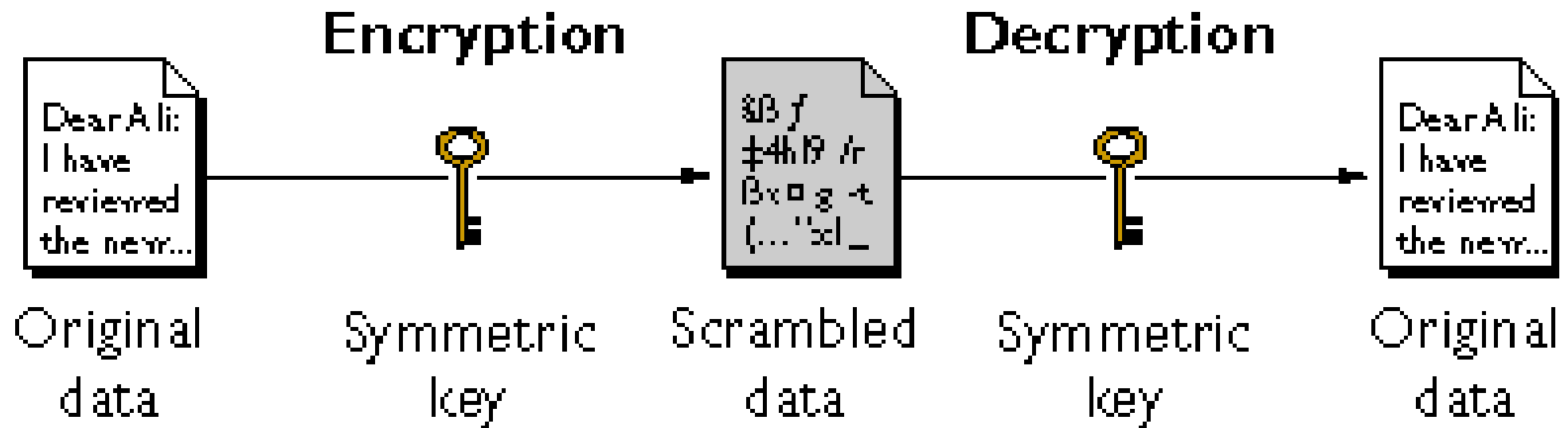
Characteristics, cont.



Characteristics, cont.

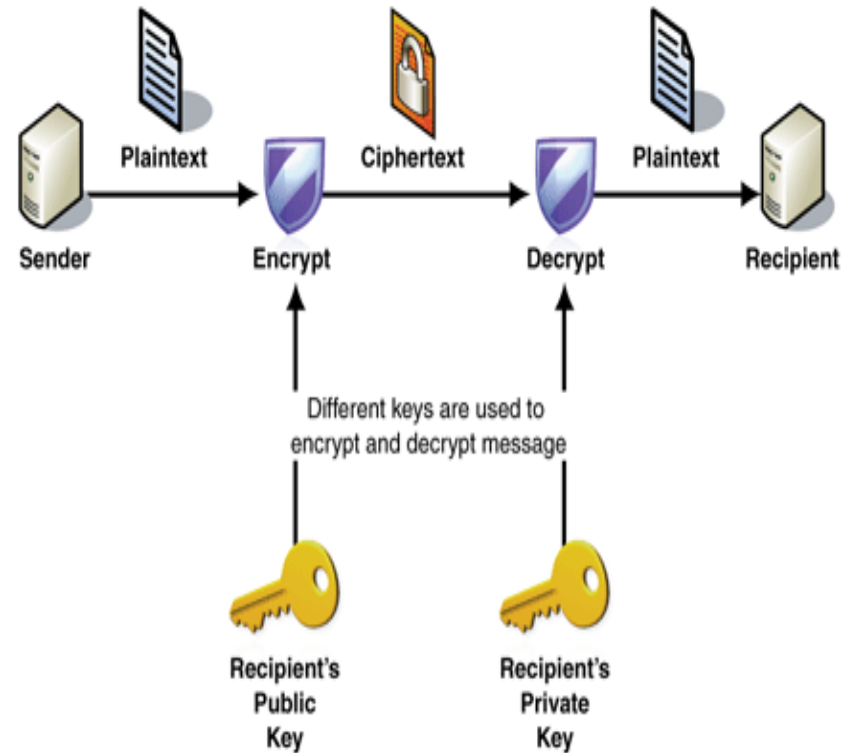
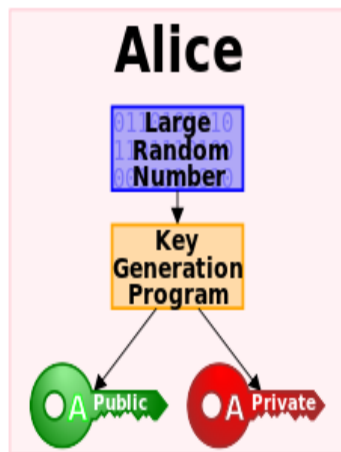


Cryptographic



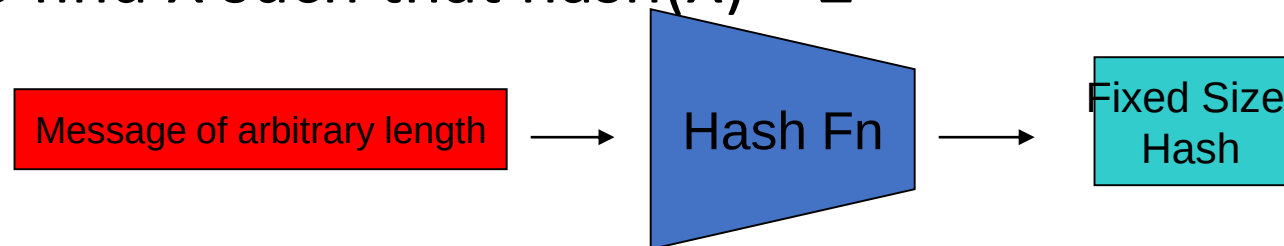
Public Key Crypto: Encryption

- Key pair: public key and private key



Cryptographic Hash Functions

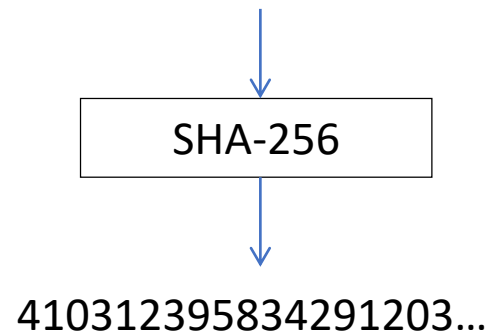
- **Consistent:** $\text{hash}(X)$ always yields same result
- **One-way:** given Y , hard to find X s.t. $\text{hash}(X) = Y$
- **Collision resistant:** given $\text{hash}(W) = Z$, hard to find X such that $\text{hash}(X) = Z$



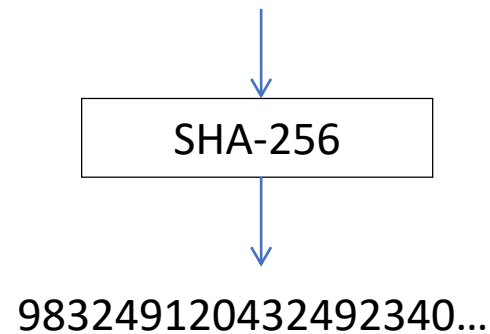
Hashes

- A hash function (like SHA-256) takes a block of data in, and produces an effectively random fixed size integer.
- Any change to the input randomizes it

“The quick brown fox did some crypto”



“The quick brown Fox did some crypto”



What is Bitcoin?

- A **peer-to-peer** internet currency that allows **decentralized** transfers of value between **individuals and businesses**.

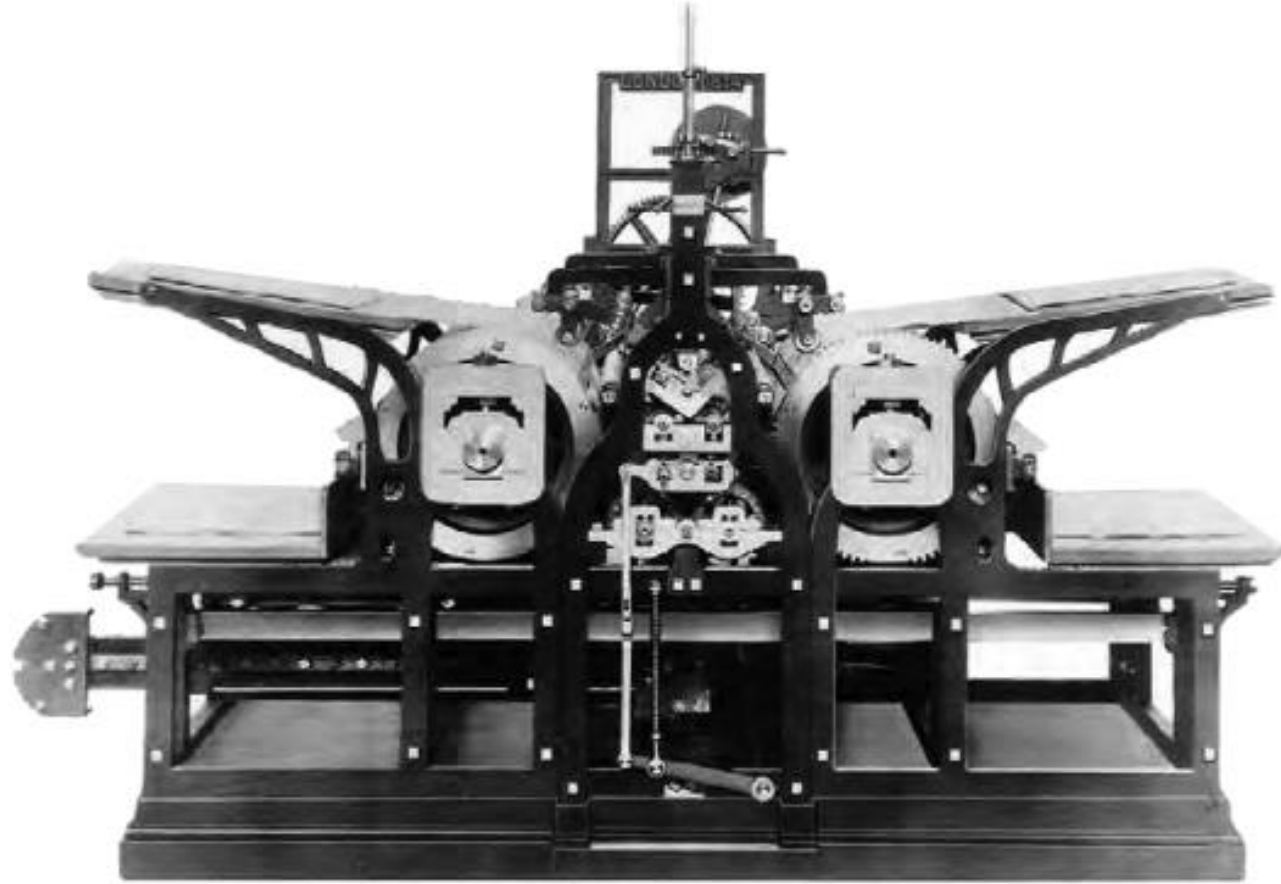


Bitcoin vs. bitcoins

- **Bitcoin** is the system
- **bitcoins** are the units



History of Internet Currency



Adam Back - Hashcash

- Originator: Adam Back
- 1997: creation of **Hashcash**, "A partial hash collision based postage scheme"
- Spam prevention system by making a sender do easily verifiable computations (hashing)
- Paper explicitly referenced possible outlawing of Digicash
- Hashcash becomes the basis of Mining algorithm.



Wei Dai – B-Money

- Originator: Wei Dai
- 1998: creation of B-Money
- **B-Money introduces**
 - Public Key pseudonyms
 - Creation of Money using hashcash
 - Two possible ways of keeping Ledger
 - All participants check (PoW)
 - Servers put up collateral ((D)PoS)
- Missing: A way to control Money Creation
 - Proposes a few ways that are still centralized



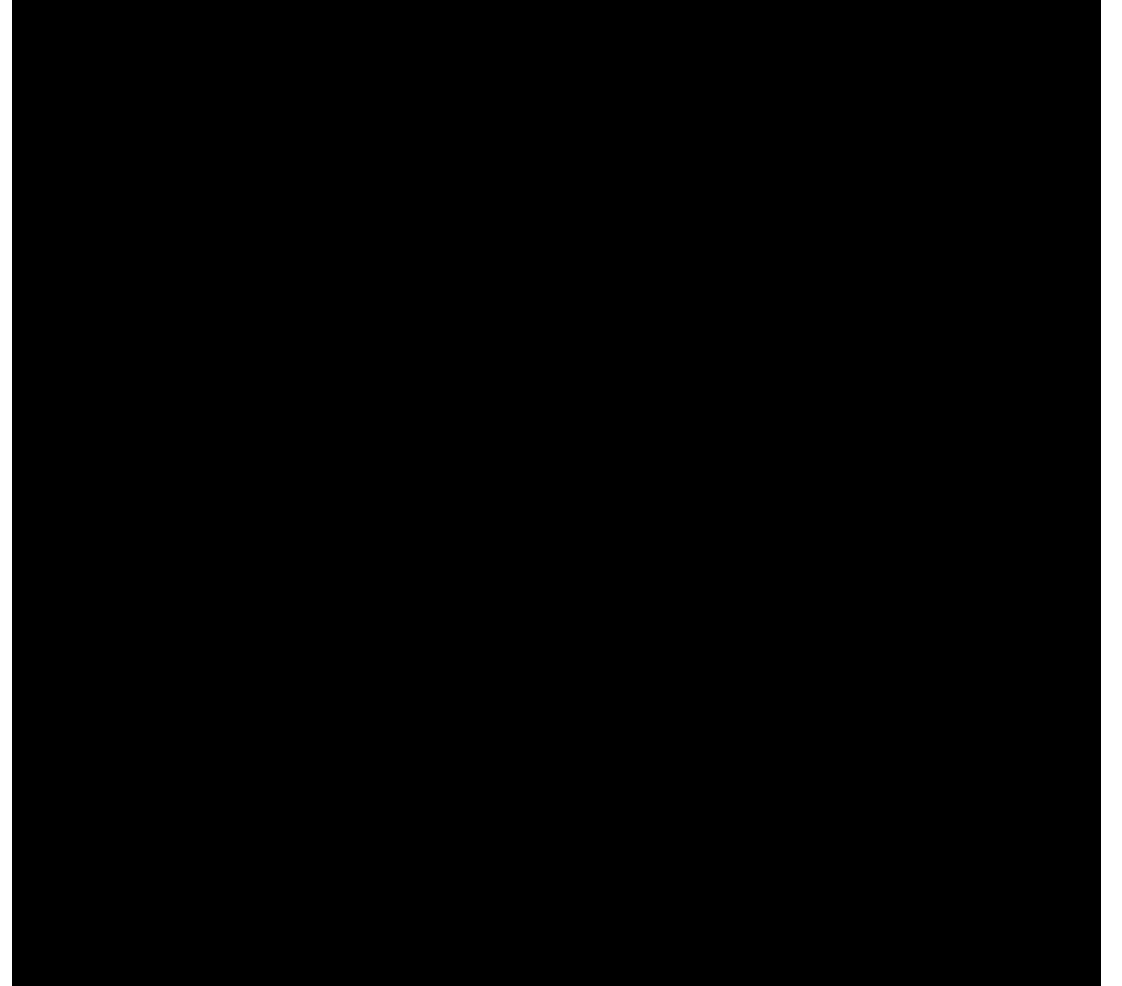
Nick Szabo - BitGold

- Originator: Nick Szabo
- 1998: inception of Bit Gold
- **Bit Gold introduces**
 - Timestamping
 - Creation of Money using hashcash
- Missing: incentives to keep nodes honest
- Missing: A way to keep tokens fungible (no agreed way to set difficulty. One token might be made with significantly more difficulty than the other)



Satoshi Nakamoto - Bitcoin

- Originator: Satoshi Nakamoto
- 2008: inception of Bitcoin
- 2009: Implementation of Bitcoin
- Bitcoin uses
 - Public Key pseudonyms
 - Timestamping
 - Creation of Money using hashcash
 - Roles for nodes: miners are kept honest (difficulty adjustment). Hashing is metric
 - Merkle trees for transaction “batching”



Creating a currency from scratch

- Motivation
 - Distrust of financial institutions
 - Transaction costs
- Primary concerns
 - Transaction security
 - Double spends



Distrust of financial institutions



- Any transaction requires a trusted third-party administrator—commonly a bank or financial service provider.
- The system forces participants to trust financial institutions that are not always trustworthy.

Transaction costs



- Traditional payments are revocable, even on irrevocable services.
- Financial institutions act as an arbitrator between counterparties in disputed claims.
- Arbitration costs are passed on to consumers.

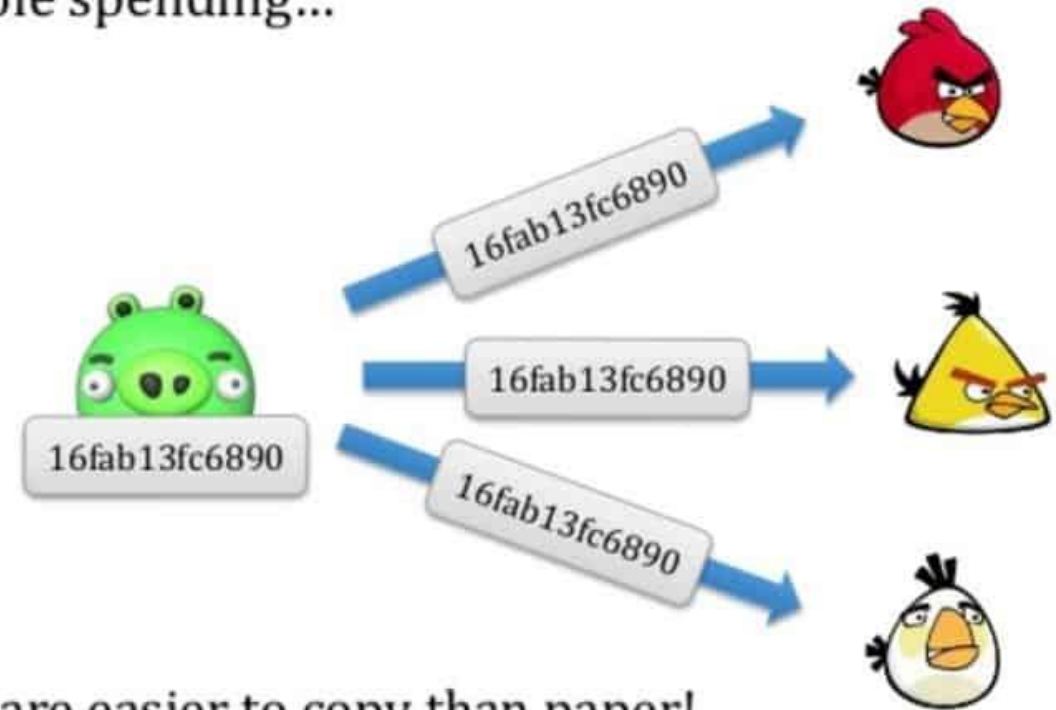
Transaction security

- Two levels of verification
 - Source is legitimate
 - Coins are legitimate
- Public/private key verification ensures the legitimacy

Double spends

- If the money is just digital codes, why not copy and paste to make more money?
 - Timestamps
 - Hashes
 - Block chain

Double spending...



Bits are easier to copy than paper!

Double spends

- Timestamp
 - Each transaction is packaged and publically recorded in the order it was carried out.
- Hash
 - The time-stamped group of transactions are given a unique algorithmically derived number



Double spends

- Block chain
 - Transactions are recorded in a community-built record of all transactions that acts as a proof-of-work.
 - Computers connected to the network accept the longest chain as accurate.



Where do bitcoins come from?



- They're "mined"
- Computers solve complicated math problems.
- Each time a problem is solved, the finder is paid a bounty.

Mining bitcoins

- Miners solve complicated algorithms to find a solution called a hash.
- Finding a hash creates a block that is used to process transactions.
- Each new block is added to the block chain.



Mining bitcoins

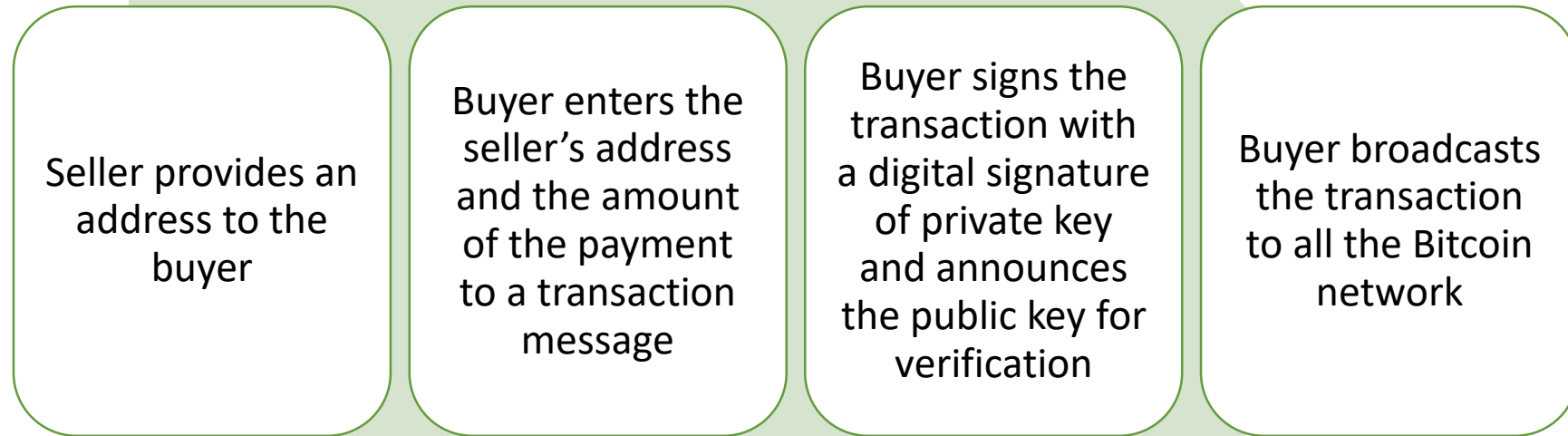
- Until there are 21 million bitcoins, miners are paid for finding a hash in new coin.
- After 21 million, miners will charge transaction fees for creating a new block.
- The amount of bitcoins paid per hash goes down by half about every 4 years.

Owning bitcoins

- Users create accounts called wallets.
- Wallets are secured using passwords and contain the private keys used for transferring bitcoins.



Spending bitcoins



Is it money?

- Store of value
- Medium of exchange
- Unit of account



Is it money?



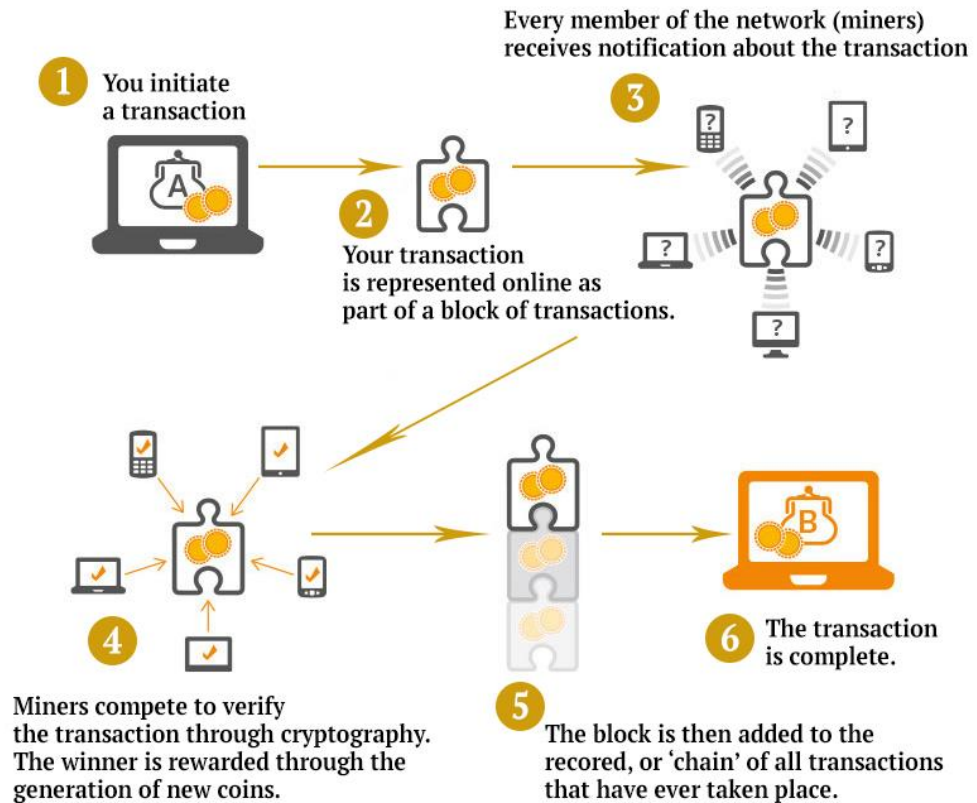
Bitcoin

- Very different from fiat currencies
- Around since January of 2009
- Not issued or controlled by any entity
- Trading over the internet
- Protocol is open source
- Somewhat anonymous
- Protected by strong encryption (cryptoCurrency)
- If you know the secret “account number” the coins are yours
- People who transmit transactions are called miners
- All Transactions are publicly available forever
- The maximum number of Bitcoins will be about 21 million
- May change money forever



Blockchain

- Distributed ledger held by everyone "mining" bitcoin
- Publicly available to view all transactions
- Block are "WORM" – Write Once, Read Many



- Distributed Ledger Systems

- Blockchain is one type of distributed ledger system.
- A database system that is decentralized, rather than centralized. Information is held by a system of nodes, rather than a single entity.
- Records are independently constructed and held by all nodes in a network. These nodes confirm records through consensus and all are updated simultaneously.
- Can accommodate static data (registry) or dynamic data (transaction records).

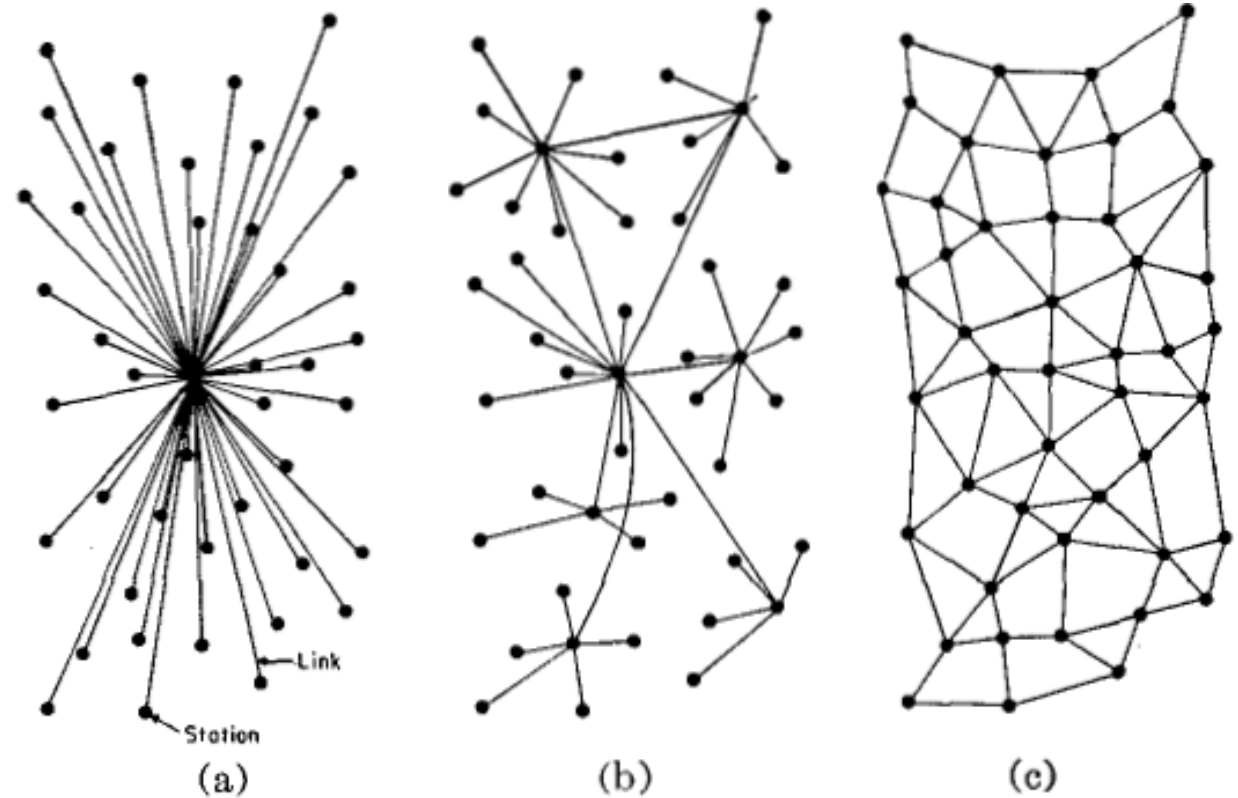
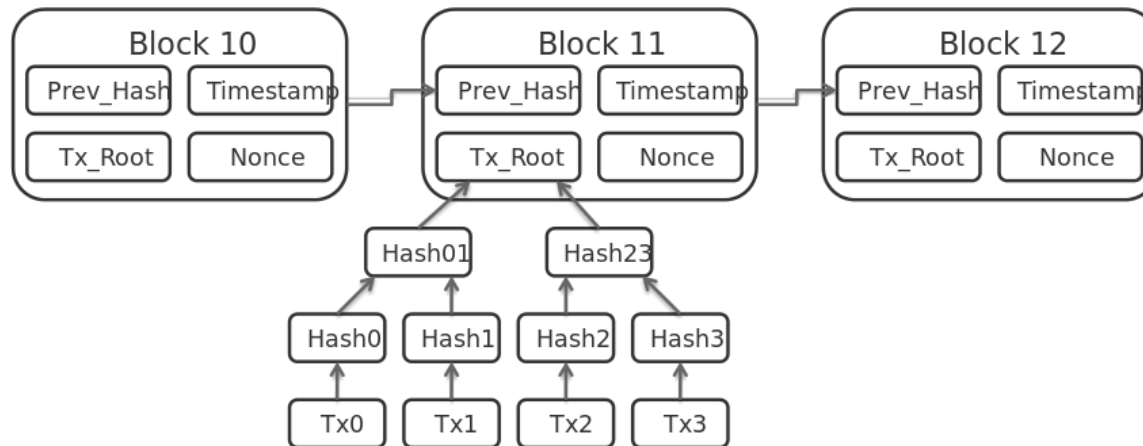


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

Blockchain



- Block is created by nodes (miners)
- Transaction are verified by nodes
- Transaction are hashed into Merkle tree
- Block contains
 - Version
 - Perv_hash
 - TX_root (Hash of all Transactions)
 - Time
 - Bits (Difficulty)
 - Nonce – (Blocks Guess)

Hash-based Proof of Work

- Can't compute an input from an output
- To find a hash with N zeros at the start of the input, requires 2^N computations...proves computational work
- If we hash an incrementing “nonce” as the hash input, we can go looking for zeros:

in 3e-05 seconds, nonce = 0 yielded 0 zeros. value = 4c8f1205f49e70248939df9c7b704ace62c2245aba9e81641edf...

in 0.000138 seconds, nonce = 12 yielded 1 zeros. value = **0**5017256be77ad2985b36e75e486af325a620a9f29c54...

in 0.000482 seconds, nonce = 112 yielded 2 zeros. value = **00**ae7e0956382f55567d0ed9311cfd41dd2cf5f0a7137...

in 0.014505 seconds, nonce = 3728 yielded 3 zeros. value = **000**b5a6cfc0f076cd81ed3a60682063887cf055e47b...

in 0.595024 seconds, nonce = 181747 yielded 4 zeros. value = **0000**af058b74703b55e27437b89b1ebcc46f45ce55d6....

in 3.491151 seconds, nonce = 1037701 yielded 5 zeros. value = **00000**e55bd0d2027f3024c378e0cc511548c94fbeed0e....

in 32.006105 seconds, nonce = 9913520 yielded 6 zeros. value = **000000**77a77854ee39dc0dc996dea72dad8852afbde6....

in 590.89462 seconds, nonce = 186867248 yielded 7 zeros. value = **0000000**225060b16117b23dbea9ce6be86ac439d....

in 4686.171007 seconds, nonce = 1424462909 yielded 8 zeros. value = **00000000**2dd743724609a9f57260e2492908d....

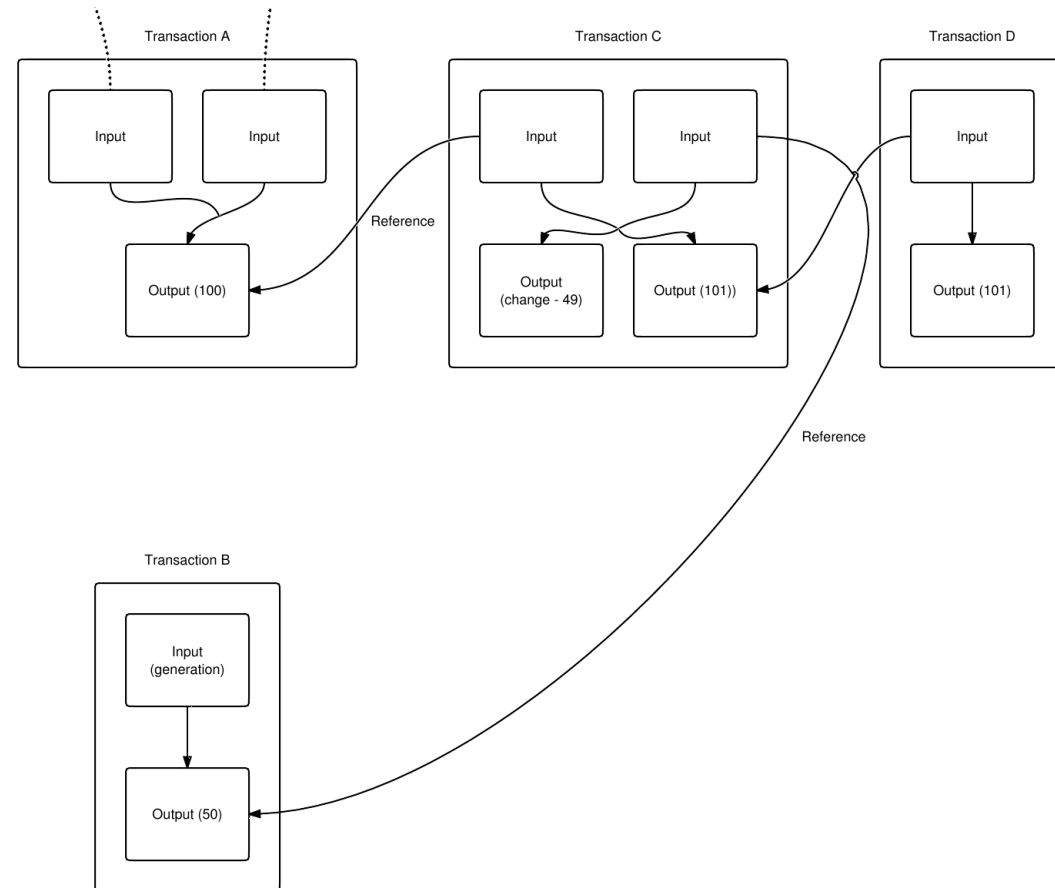
We can now make this into a distributed “game”

Bitcoin security

- Computers accept the longest block chain, which inhibits hacking.
 - Hackers would have to create a longer chain of fraudulent information faster than the combined effort of all other computers.
- Public/private cryptography means individual bitcoins are secured when not being transacted.
- Over 50% of the nodes must verify a block for it to be added
 - Keeps bad-players from simply adding invalid blocks

Blockchain Transactions

- Each transaction contains the address of the last transaction
- Transaction A – payment made up of 2 pervious payments
- Transaction B – Mined Bitcoin
- Transaction C – Payment with change
- Transaction D – Payment



Privacy Implications

- 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 daughter was pregnant
 - Imagine what credit card companies could do with the data

Operational Realities

- Assumes cheap storage and networking
 - Nodes store every transaction ever
 - Transactions and blocks are broadcast
 - Might limit scale...
- Transactions are slow
 - To verify a transaction, have to wait for a public block
- Control of private keys is crucial
 - Lose your private key = unspendable coins
 - Steal your private key = steal coins

Bitcoin / Blockchain

- Is a global currency (symbol BTC)
- Around since January of 2009
- Not issued by any entity
 - Peer-to-peer / decentralized
- Trading over the internet
- Protocol is open source
 - Code verifiable by anyone
- Somewhat anonymous
- Protected by strong encryption (cryptoCurrency)
 - If you know the secret “private key” the coins are yours
- People who transmit transactions are called miners
- Limited number of Bitcoins ~21 million
- Transactions public forever – used to verify ownership
- May change money forever



Blockchain - Current / past Illinois Projects

- A health provider network in the works with the state Department of Financial and Professional Regulations (DFPR)
- Tracking continuing education credentials with DFPR and the University of Illinois.
- Department of Health, how birth or other vital records information could be documented using blockchain.
- A use case on the recording of academic credentialing, in the works with public universities.
- Tracking Renewable Energy Credits, which are generated by creating 1 Megawatt-hour of electricity through wind turbines or solar panels.
- Cook County Land Transfer project (complete)

What a Petahash looks like



Acknowledgement

- Many of the slides, content, or pictures are borrowed from internet resources, and some pictures are obtained through Google search without being referenced.