Computer Security and Cryptography

CS381

来学嘉
计算机科学与工程系 电院3-423室
34205440 1356 4100825 laix@sjtu.edu.cn

2014-06

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions and MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
- SSL
- IPSEC
- Firewall
- VPN

Computer security
- Access control
- Malware
- DDos
- Intrusion

Examples
- Password
- Bitcoin
- Hardware
- Wireless?

References

- Bitcoin: A Peer-to-Peer Electron, Satoshi Nakamoto
  - http://www.bitcoin.org/bitcoin.pdf
- Wiki https://en.bitcoin.it/wiki/Main_Page
- Ken Shirriff's blog
  - Bitcoins the hard way: Using the raw Bitcoin protocol http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html
  - Bitcoin mining the hard way: the algorithms, protocols, and bytes http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

Bitcoin

- Bitcoin is a decentralized electronic cash system using peer-to-peer networking to enable payments between parties without relying on mutual trust.
- Payments are made in bitcoins (BTC's), which are digital coins issued and transferred by the Bitcoin network.
- The data of all these transactions, after being validated with a proof-of-work system, is collected into what is called the block chain.

Bitcoin-idea

- Bitcoin is one of the first successful implementations of a *distributed crypto-currency*, described in part in 1998 by Wei Dai on the cypherpunks mailing list.
- Bitcoin is designed around the idea of using cryptography to control the creation and transfer of money, rather than relying on central authorities.

5

Bitcoin-work

- Nakamoto(中本聪) has claimed that he has been working on Bitcoin since 2007.
- In 2008, he published a paper on The Cryptography Mailing List at metzdowd.com describing the Bitcoin digital currency.
- In 2009, he released the first Bitcoin software that launched the network and the first units of the Bitcoin currency.
- Value: $0.01-2009; 10$-2012; 1000$--2013

Bitcoin-motives

- Political?
- "[Bitcoin is] very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though." - Satoshi Nakamoto
- guess: Nakamoto had great concern or contempt for the current central banking system.

Bitcoin / electronic cash

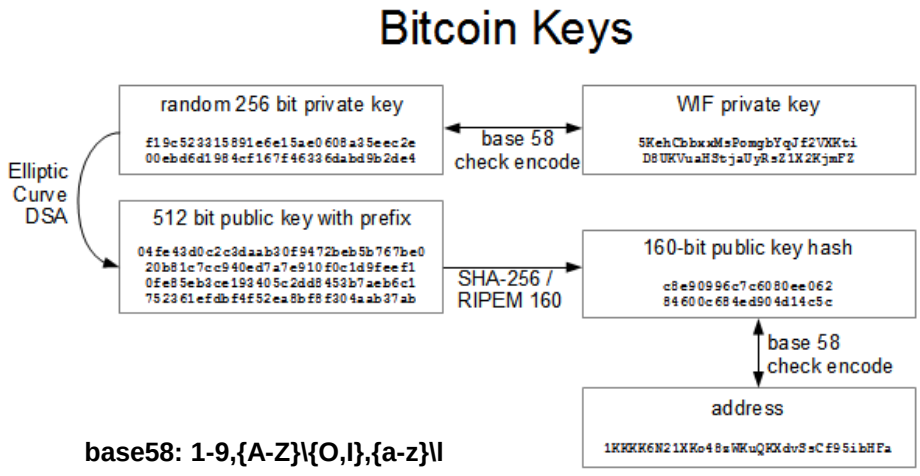
- Peer-to-peer
- Online payments
- Without financial institution
- Crypto-techniques
  - Digital signature
  - Hash chain
- Double-spending problem (copy data is easy)

- E-cash [David Chaum 1990s]
  - anonymous electronic cash
  - used blind signatures to achieve unlinkability between withdrawal and spend

Bitcoin-Ownership

- bitcoins consist of entries in a distributed database that keeps track of the ownership of bitcoins.
- Unlike a bank, bitcoins are not tied to users or accounts. Instead bitcoins are owned by a Bitcoin address, for example *1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa*.
- It is the hash-code of the owner's public-key, If the private key is lost, the user cannot prove ownership by other means. The coins are then lost and cannot be recovered

Owner: address and keys



base58: 1-9,{A-Z}\{O,I},{a-z}\l

Lost and found

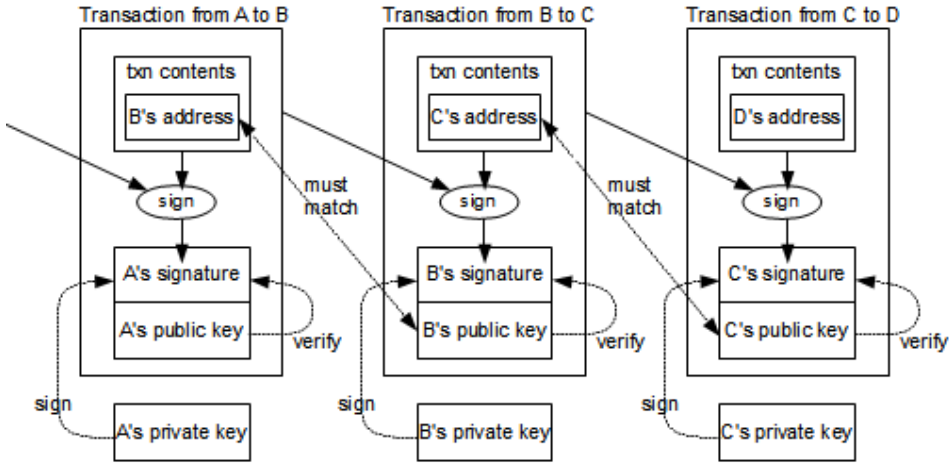
- Bitcoins can be lost. In 2013 one user said he lost 7,500 bitcoins, worth $7.5m at the time, when he discarded a hard drive containing his private key.
- Bitcoins can also be found. In March 2014, former bitcoin exchange Mt. Gox reported it found an "old wallet", which was used before June 2011 [that] held about 200,000 bitcoins".

11

Transactions

- Transactions of an electronic coin—a chain of digital signatures
- Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin.
- A payee can verify the signatures to verify the chain of ownership.

transactions



Double-spend problem

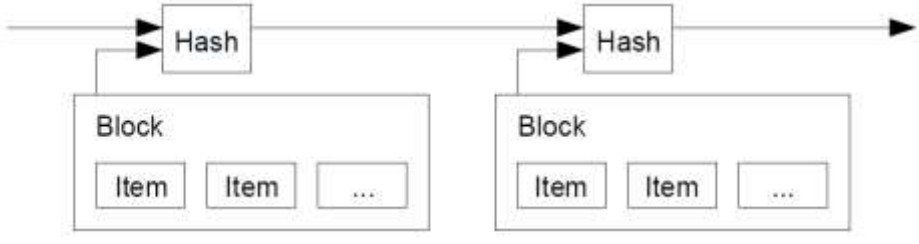
- Double-spending problem (copy data is easy)
- Common solution: introduce a trusted central authority, or mint, that checks every transaction for double spending.
- Problem: the fate of the entire money system depends on the company running the mint, with every transition having to go through them, just like a bank.

Double-spend solution

- The only way to confirm the absence of a transaction is to be aware of all transactions.
- To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received.

Timestamp server

- Taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post.
- Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before

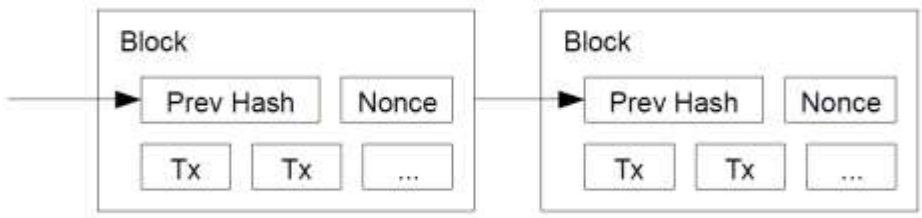


Proof-of-work (Mining) (1)

- Adam Back's Hashcash
  - Scan for a value that when hashed, such as SHA-256, the hash begins with a number of zero bits.
  - The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Mining (2)

- Implement by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits.
- Finding this solution generates a mined block, which becomes part of the official block chain.



Mining (3)

- Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work.
- As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

Mining (4)

- Mining is essentially one-CPU-one-vote.
- The majority decision is represented by the longest chain, which has the greatest mining effort invested in it.
- If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.

Mining (5)

- To compensate for increasing hardware speed and varying interest in running nodes over time, the mining difficulty is determined by a moving average targeting an average number of blocks per hour.
- If they're generated too fast, the difficulty increases.

Network-steps

1) New transactions are broadcast to all nodes.

2) Each node collects new transactions into a block.

3) Each node works on mining its block.

4) When a node finds a solution, it broadcasts the block to all nodes.

5) Nodes accept the block only if all transactions in it are valid and not already spent.

6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Network-details

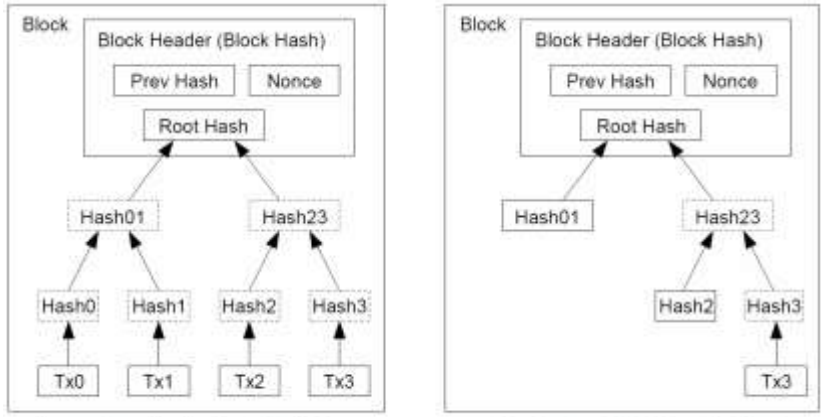
- Nodes always consider the longest chain to be the correct one and will keep working on extending it.
- New transaction broadcasts do not necessarily need to reach all nodes.
- Block broadcasts are also tolerant of dropped messages.

Incentive

- By convention, the first transaction in a block is a special transaction that starts new coins owned by the creator of the block. This mining bounty is large - currently 25 bitcoins per block (about $14,217, ￥88,358).
- The incentive can also be funded with transaction fees.
- Once a predetermined number (21million) of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

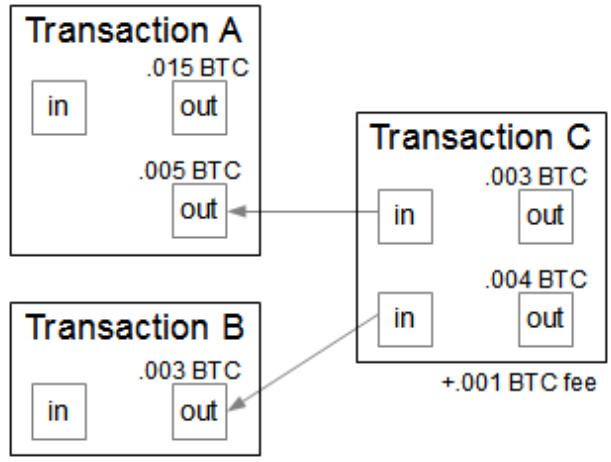
Reclaiming disk space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space.



Combining and splitting value

Transactions contain multiple inputs and outputs.



Security

- Unauthorized spending
  - Attack PKC and hash.
- Double-spend
  - Global public transaction log(blockchain)
- Race attack
  - Transaction may be removed by a fork.
  - In theory, users can never be completely sure. In practice, most bitcoin clients require 6 “confirmation” blocks before accepting that a transaction is published.

Security

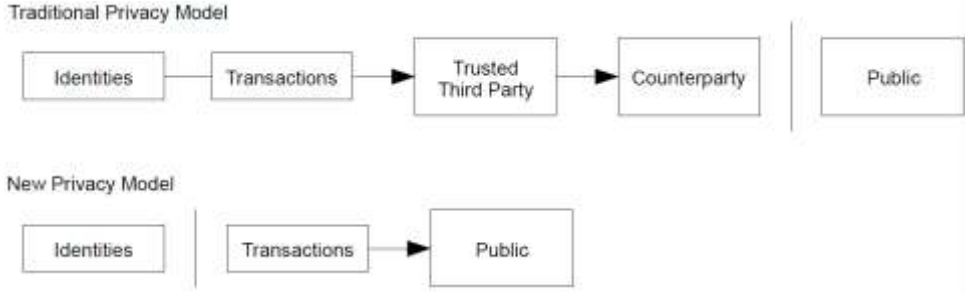
- Goldfinger attack[WEIS13]
  - Essentially a 51% cartel attack.
  - Goal: destroy Bitcoin’s stability and hence its utility as a currency.
  - have already been observed. CoiledCoin was destroyed by a Bitcoin mining pool.
- Selfish mining[FC14]
  - a miner initially keeps blocks secret after finding them, keeps mining, and publishes them later.
  - potentially leading to a 51% attack ?
  - no evidence of a selfish mining attack occurred.

Security

- Mining pools are vulnerable to participants submitting partial shares in exchange for compensation but withholding valid blocks to lower the pool's profitability.[arXiv14]
- Denial-of-service attack against pools.[FC14]
- Client security
  - the entire blockchain is large now, mobile devices need simplified payment verification(SPV): untrusted nodes prove to lightweight clients. This may lead to privacy leakage.[ACSAC14]

Privacy

Keep public keys anonymous, similar to the level od information released by stock exchanges.

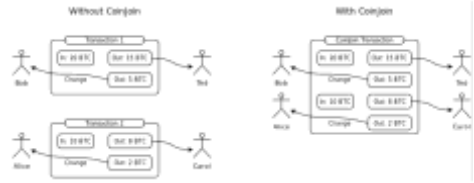


Privacy

- Bitcoin offers limited unlinkability. Transaction graph analysis yields clusters of addresses.
- Heuristic:[FC13]
  - Addresses contributing to a multiple input transaction belong to the same user.
  - If a transaction has two outputs exactly one of which is to a new address, the new address and the sender address belong to the same user.
    - Transfer of BTCs to single-use addresses before or after the payment.
- Broadcast leaks IP address.(SPV)

Privacy

- Enhancement:
  - Bitcoin + Tor ?
    - Not a good idea: by exploiting Bitcoin's DoS protection, the attacker can link together user's transactions regardless of pseudonyms used.[SnP15]
  - P2P mixing protocol:
    - CoinJoin: a set of Bitcoin holders jointly create a series of transactions which permute ownership of their coins.



Privacy

- Enhancement:
  - Distributed mix network
    - Mixcoin: users send standard-sized transactions to a third-party mix and receive back the same amount from coins submitted by other users of the same mix.[FC14]
    - Blindcoin: the input/output address mapping for any user is kept hidden from the mixing server.[FC15]
  - Bitcoin-like base currency + shadow currency
    - Example: PinnochioCoin[PETShop13]
  - SNARKs
    - Zerocash: the corresponding transaction hides the payment's origin, destination, and transferred amount. [SnP14]
  - Ring signatures
    - CryptoNote: based on the work "Traceable ring signature". better performance but weaker anonymity compared to Zerocoin or Zerocash.

Evolution

- Altcoins: hundreds of derivative systems.
  - New genesis block: start a new blockchain from scratch.
  - Forking Bitcoin: choose to fork Bitcoin at a certain point, accepting the prior transaction history and ownership of funds.
  - Proof-of-burn: transfer funds in Bitcoin to a special address whose private key cannot be found such as the key with a hash of all zeroes.
  - Pegged sidechains: bitcoins can be transferred and eventually redeemed.
- Altcoins must compete with Bitcoin for miners and avoid Goldfinger attacks by Bitcoin miners.

Evolution

- Alternative protocols
  - Inter-block time adjustment. Litecoin is four times faster.
  - Limits on block and transaction size.[bitcoinfoundation.org,2014]
    - may raise the cost of using Bitcoin
    - may lead users to rely on intermediaries
    - benefit bandwidth-limited participants
    - affection remains unknown.
  - Different monetary policy: Dogecoin and Freicoin are different from Bitcoin.

Evolution

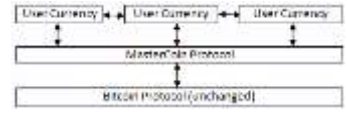
- Alternative computational puzzles
  - ASIC-resistant puzzles: nowadays mining is no longer “one-CPU-one-vote”. Require “memory-hard” puzzles. scrypt hash function is used in Litecoin and Dogecoin.
  - Useful puzzles:
    - Primecoin: find sequences of large prime numbers of mathematical interest.
    - Permacoin: distributed storage of archival data [SnP14]
  - Non-outsourceable puzzles:
    - Prevent miners to join coalitions.[CCS15]

Evolution

- From “proof-of-work” to “proof-of-stake”:
  - more difficult for an attacker to acquire a sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment;
  - No real-world resources are wasted.
- Proof-of-stake:
  - Proof-of-coin-age: PPCoin
  - Proof-of-deposit: Tendermint
  - Proof-of-burn: Slimcoin
  - Proof-of-activity: stakeholders’ lottery [ePrint14]

Bitcoin-inspired Applications

- As a naming service:[Schwartz, 2011]
  - square “Zooko’s triangle”. Namecoin implements the concept.
- As Secure timestamping:[FC12]
  - Blockchain is append-only
- As digital tokens: Colored Coins
  - use the history-tracking functionality of the blockchain as a feature.
- Omni(formerly Mastercoin)
  - use Bitcoin’s consensus mechanism but define completely different transaction syntax to be written as arbitrary data on the blockchain.



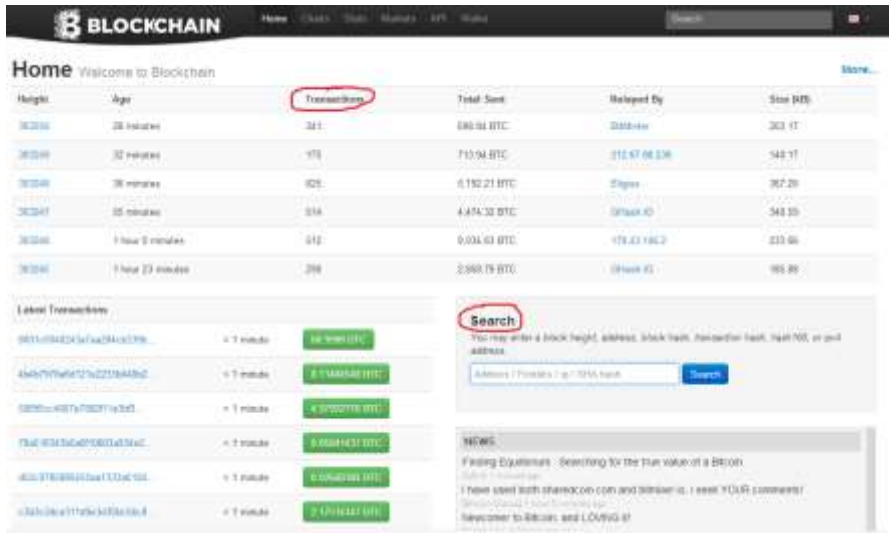
Conclusion

- Bitcoins are sent easily through the Internet, without needing to trust any third party.
- Transactions are irreversible by design.
- The supply of bitcoins is regulated by software and the agreement of users of the system and cannot be manipulated by any government, bank, organization or individual.
- The limited inflation of the Bitcoin system's money supply is distributed evenly (by CPU power) to miners who help secure the network.

Claims

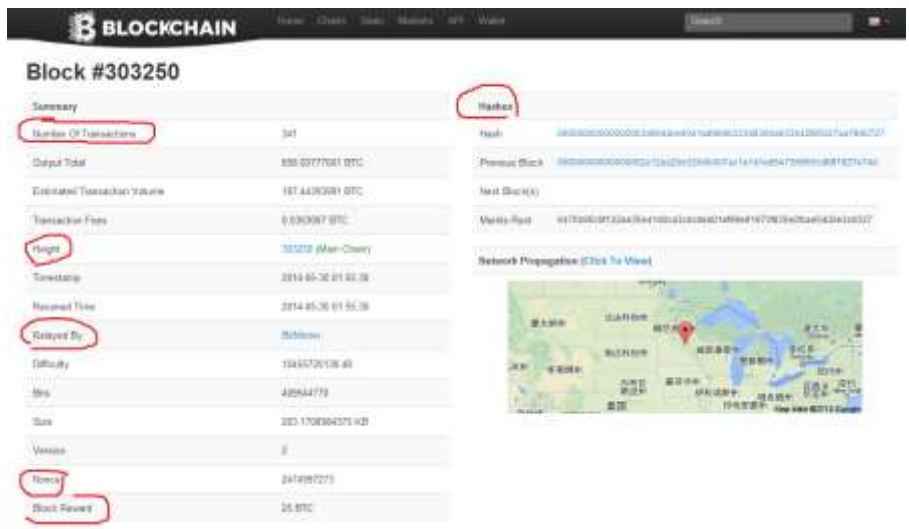
+ the first truly global currency which does not discriminate its users based on citizenship or location,
+ always running with no holidays, very low usage fees, no chargebacks, etc.
− it is widely misused to buy illegal items and to launder large sums of money,
− it is too easy to steal bitcoins from wallets via cyber attacks.

Block mining



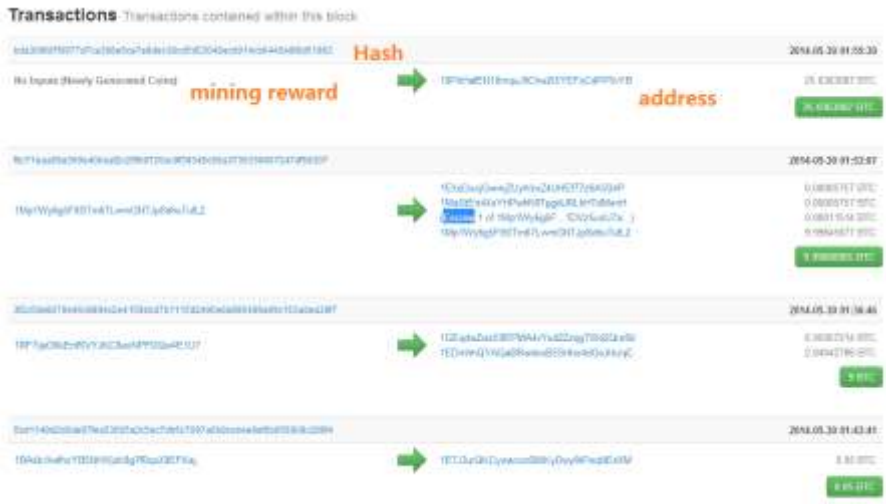
41

A new block



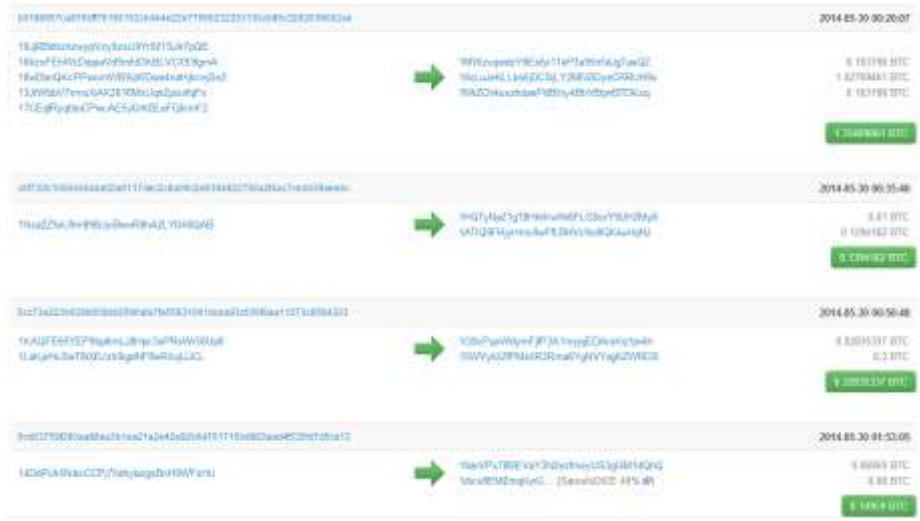
42

A transaction



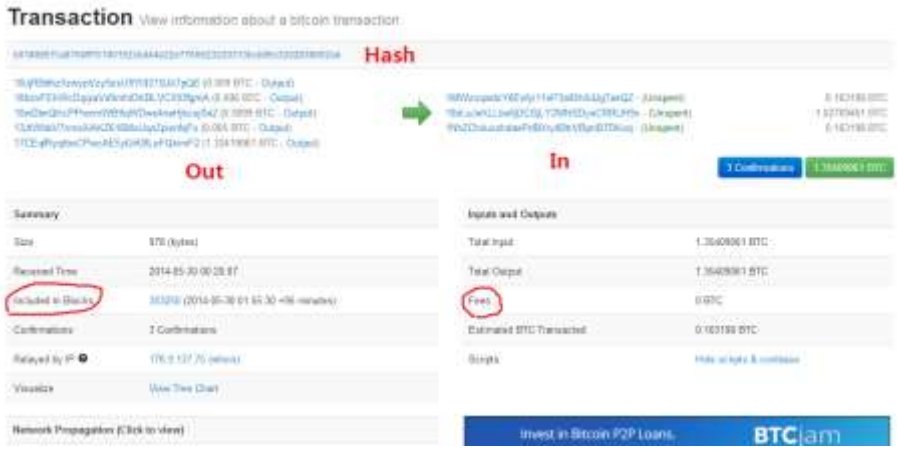
43

Multiple



44

Transaction fee



45

Bitcoin

A common logo from the bitcoin reference client

Date of introduction	3 January 2009; 5 years ago (2009-01-03)
User(s)	Worldwide
Production	**25 bitcoins per block (approximately every ten minutes) until mid 2016, and then afterwards 12.5 bitcoins per block for 4 years until next halving. This halving continues until 2110-2140**.
Source	Number of bitcoins in circulation
Method	Increase in the supply
Subunit	
10^{-8}	satoshi[2]
Symbol	BTC, XBT,[3]

46

Exercise 20

1. Is Bitcoin anonymous?

2. What is the purpose of mining?

- Deadline: before next lecture