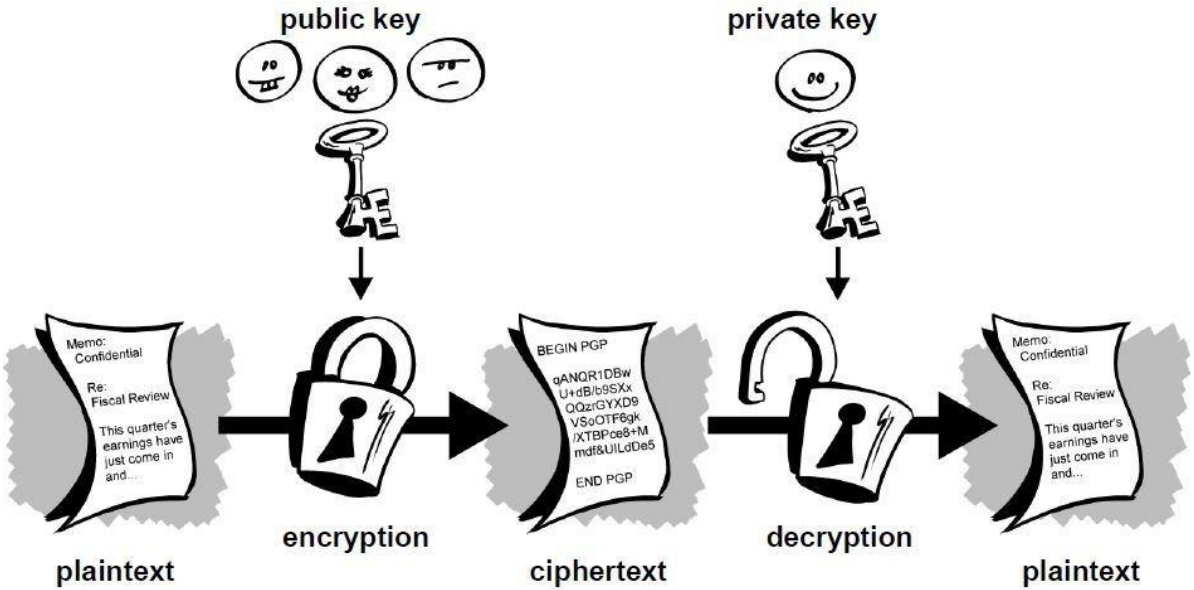
Introduction to Cryptography

By
Vipul Goyal



Digital vs Physical Money

- Bitcoin: purely digital currency

- But wait: don't we already have electronic banking?
  - Can transfer money online
  - Electronic payments using credit cards

- These systems are still tied to physical govt issued money
  - Can withdraw in physical format
  - If banks or govt wants, it can freeze your accounts

Bitcoin

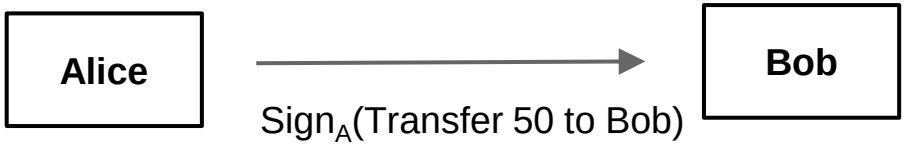
- Bitcoin: first truly decentralized currency
  - No trusted party, no government control
- Researchers had been trying since 1990s, however all attempts failed to take off
- In 2008: an unknown guy (or girl?) comes along: Satoshi Nakamoto
- Whitepaper and code posted on Cyberpunks mailing list in 2008

Bitcoin Beginning

- Mining started in Jan 2009
- First real world transaction made using Bitcoin: sometime in mid-2010
  - A guy paid 10,000 Bitcoins to his friend to order him a Pizza
  - Probably world's most expensive pizza: ~100 million dollars
- Started taking off mainly as a currency for hacker, online criminal and so on. Bad name.
  - Anonymity and lack of govt control
- Ransomware in 2014: CryptoLocker. Millions extorted.
- Today situation has changed entirely: major tech companies and banks are investing in cryptocurrencies

Creating Digital Currency using Digital Signatures

- Say Alice wants to transfer money to Bob (say everyone knows Alice has 50 coins)
- Alice and Bob will each have a public key (verification key of a digital signature scheme)
- Alice can send a digital signed statement “I, Alice, transfer 50 coins to Bob”

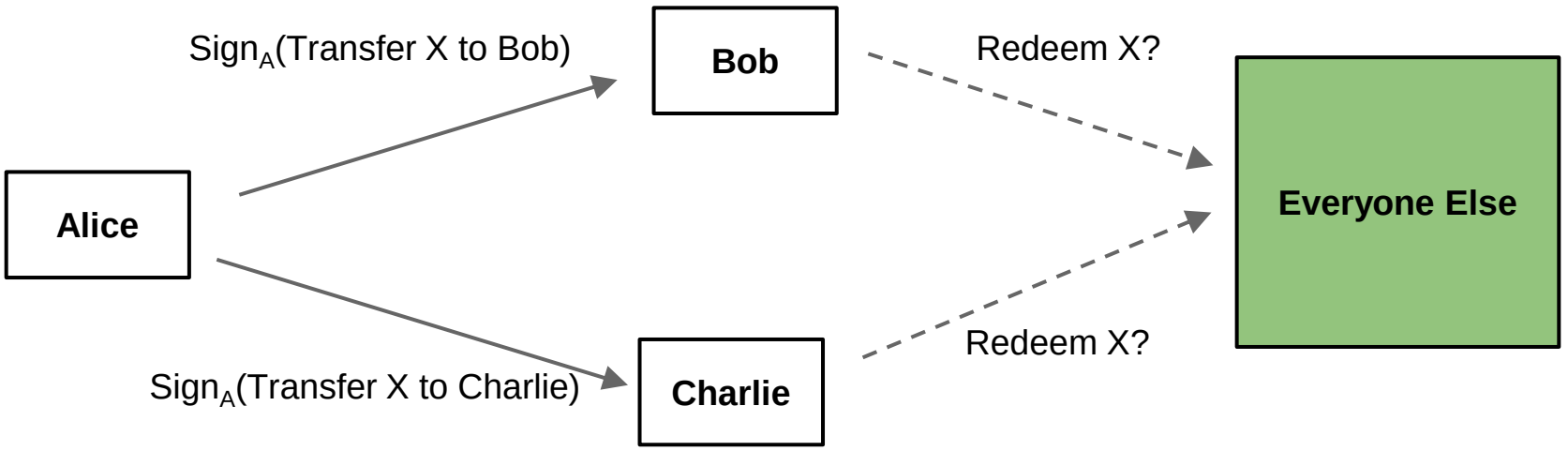


Creating Digital Currency contd..

- Bob can then take this signed statement to anyone as a proof that Alice's coin are now his
- Bob can spend these coins further using digital signatures again

- This process can continue

Double Spending Attacks



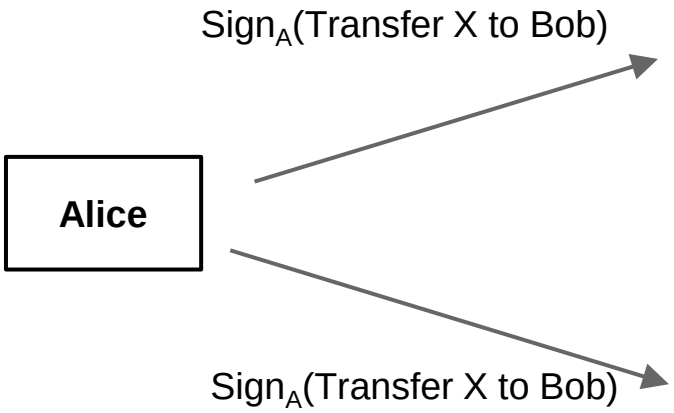
- Say Alice only has 50 dollars, but sends 50 to Bob and 50 to Charlie. What happens then?

Solution: Public Append only Public Ledger

- Public Ledger: public file which contains all transactions which ever took place
- Can only add entries, can never erase entries (append only)
- Anybody in the world can view this file (public) and check all records
- Say at any given point, Alice has 50 coins and Bob has 10.
  - Balance of each party can be computed from the transaction history

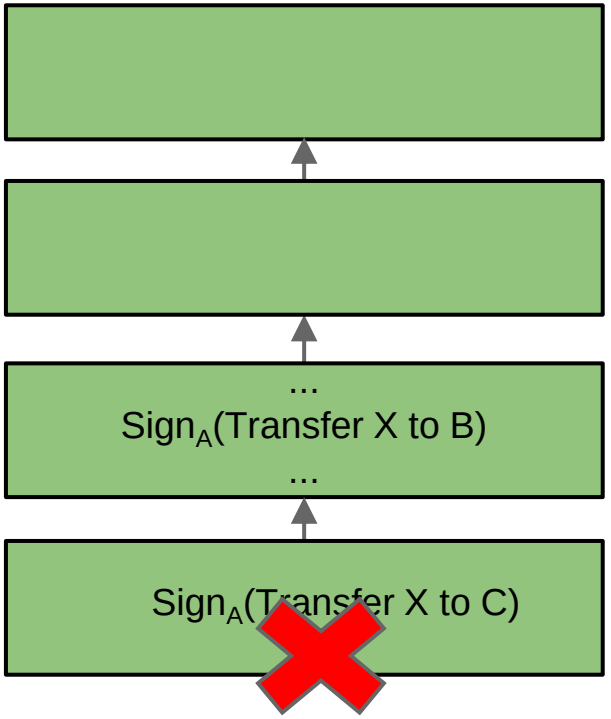
Money Transfer w/ Public Ledger

- Alice can publicly broadcast a digital signed statement “I, Alice, transfer 50 coins to Bob”



- This statement is added to the public ledger after verifying digital signature + verifying that Alice has 50 coins

Preventing Double Spending

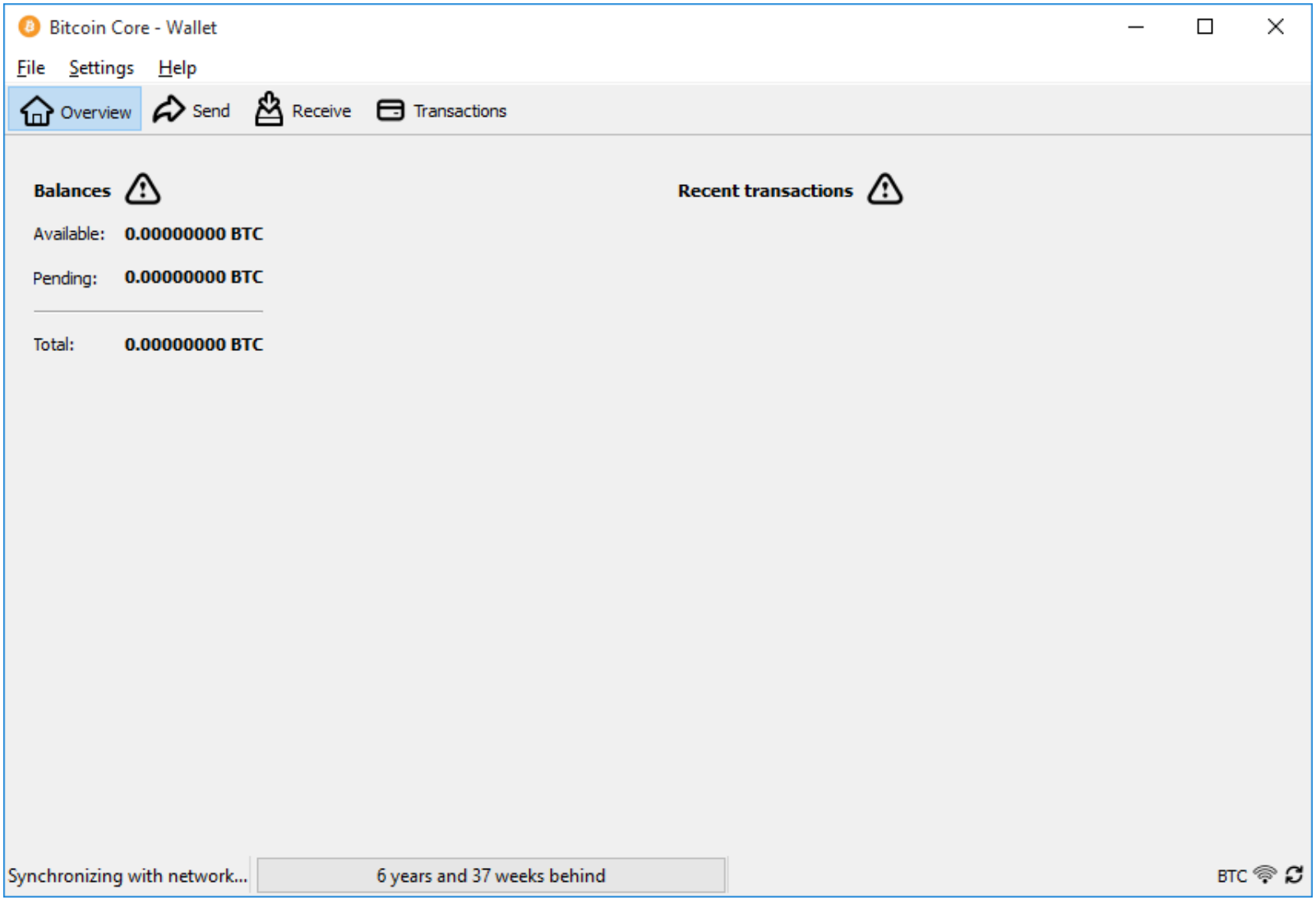


- One of the two transactions will be first. It will be added. For the 2nd one: Alice will not have sufficient balance

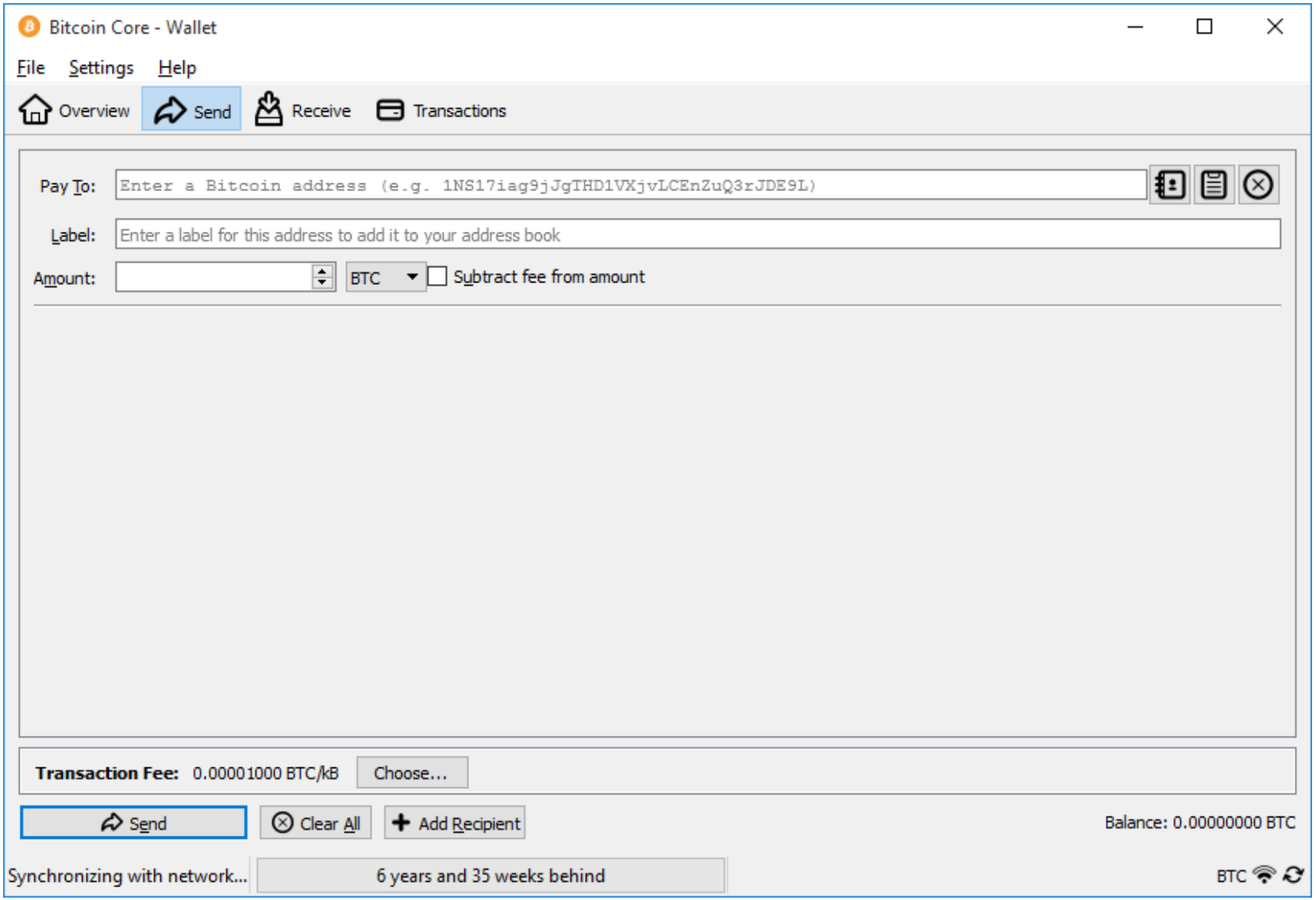
Getting Started with Bitcoin

- Download software to create a Bitcoin wallet (see https://bitcoin.org/en/choose-your-wallet)
- The software creates public/private key pairs for you as needed.
- The wallet holds the private keys you use for digital signatures. Your public key = your bitcoin address.
- The wallet also contains software that allows you to send and receive bitcoins. Again: by process of digital signing.

Bitcoin Core Wallet (on first setup)



Send Money


Bitcoin Core - Wallet
File
Settings
Help
Overview
Send
Receive
Transactions
Pay To:
Enter a Bitcoin address (e.g. 1NS17iag9jJgTHD1VXjvLCEnZuQ3rJDE9L)
Label:
Enter a label for this address to add it to your address book
Amount:
BTC
Subtract fee from amount
Transaction Fee: 0.00001000 BTC/kB
Choose...
Send
Clear All
Add Recipient
Balance: 0.00000000 BTC
Synchronizing with network...
6 years and 35 weeks behind
BTC

Some Key Questions

- Who maintains the public ledger?

- Answer: everyone maintains it? But what about disagreements?
  - For example: one party says “Alice to Bob” transaction was first and should go into ledger. “Alice to Charlie” should be rejected
  - Other party might say “Alice to Charlie” was first and should be added, other rejected.

- Answer: disagreements are resolved using a type of “voting” or consensus algorithms. Several types:
  - Proof of work based voting: number of votes you have is proportional to your computing power
  - Proof of stake based voting: number of votes you have is proportional to the number of coins you have

Some Key Questions

- Coin transfer is fine. But how are the coins created in the first place?
- Public ledger is written 1 “blocks” at a time (or 1 page at time)
- There is a competition to write to the public ledger
- Whoever wins the competition: writes next block. Some new coins are created and given to that miner as a reward
- These coins can then be transfer by this party to anyone else.

Cryptographic Hash Functions

- Similar to one-way functions we studied earlier
- Intuition: a hash function H, on any input, gives a "random" output

- Hard to find any pattern in the output
- If the output is random => output hides the input (one-way functions). Example: SHA-256.
  - Note that this is different from encryption: no keys, no decryption process

A Cryptographic Puzzle

- You are given some string a, you need to find b s.t.

- That is: find b such that Hash output has 20 0's (followed by other values). || denotes concatenation.

- Now H(a||b) = random. Hence, for any b, probability of this happening = 2^{-20}
  - Hence, to solve it, you need to hash many times with different values of b (approx. 2^{20} hash evaluations)

Bitcoin Mining

- For simplicity: assume a single miner with public key PK

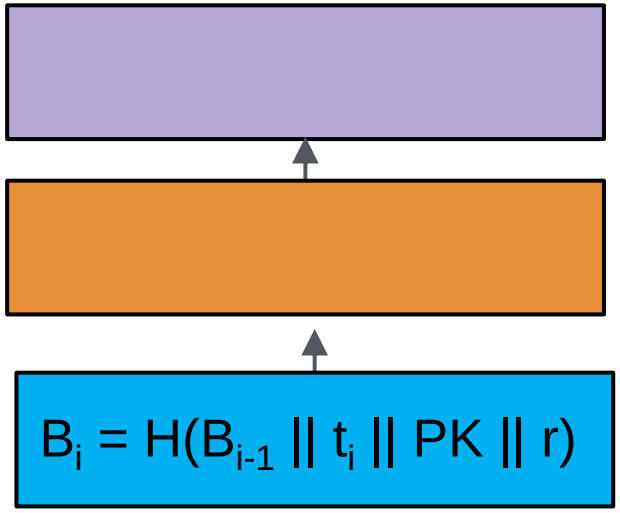
- Genesis Block B_0 = “The Times 03/Jan/2009. Chancellor on brink of second bailout for banks”

- For mining block i
  - First collect the list of transaction to be written: t_i
  - Let previous block be B_{i-1}
  - Compute any number (nonce) r

    $H(B_{i-1} \| t_i \| PK \| r) = 0000$ (k times) 0*********
  - Now $B_i = H(B_{i-1} \| t_i \| PK \| r)$

- New Bitcoins are created and given as reward to public key PK

Picture



- New block is created by hashing the previous block along with: transactions, public key and a nonce
- Hash output should have several 0's, hence computing it takes time

Multiple Miners

- Every miner tries to mine the new block: a race
- Think: many different miners trying many different values of r to get a hash output with several 0's
- Whoever succeeds first gets the reward
- Specialized mining hardware to do hashing quickly

300 GH Bitcoin Mining Card

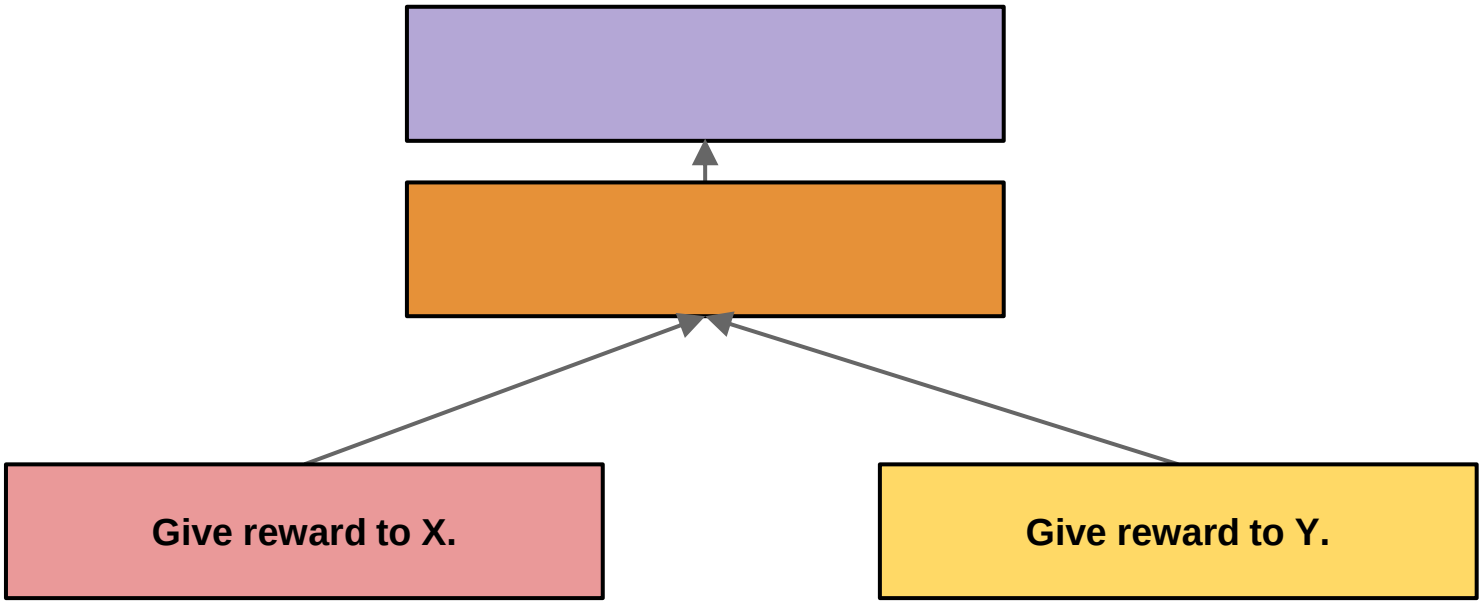
The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

Forking

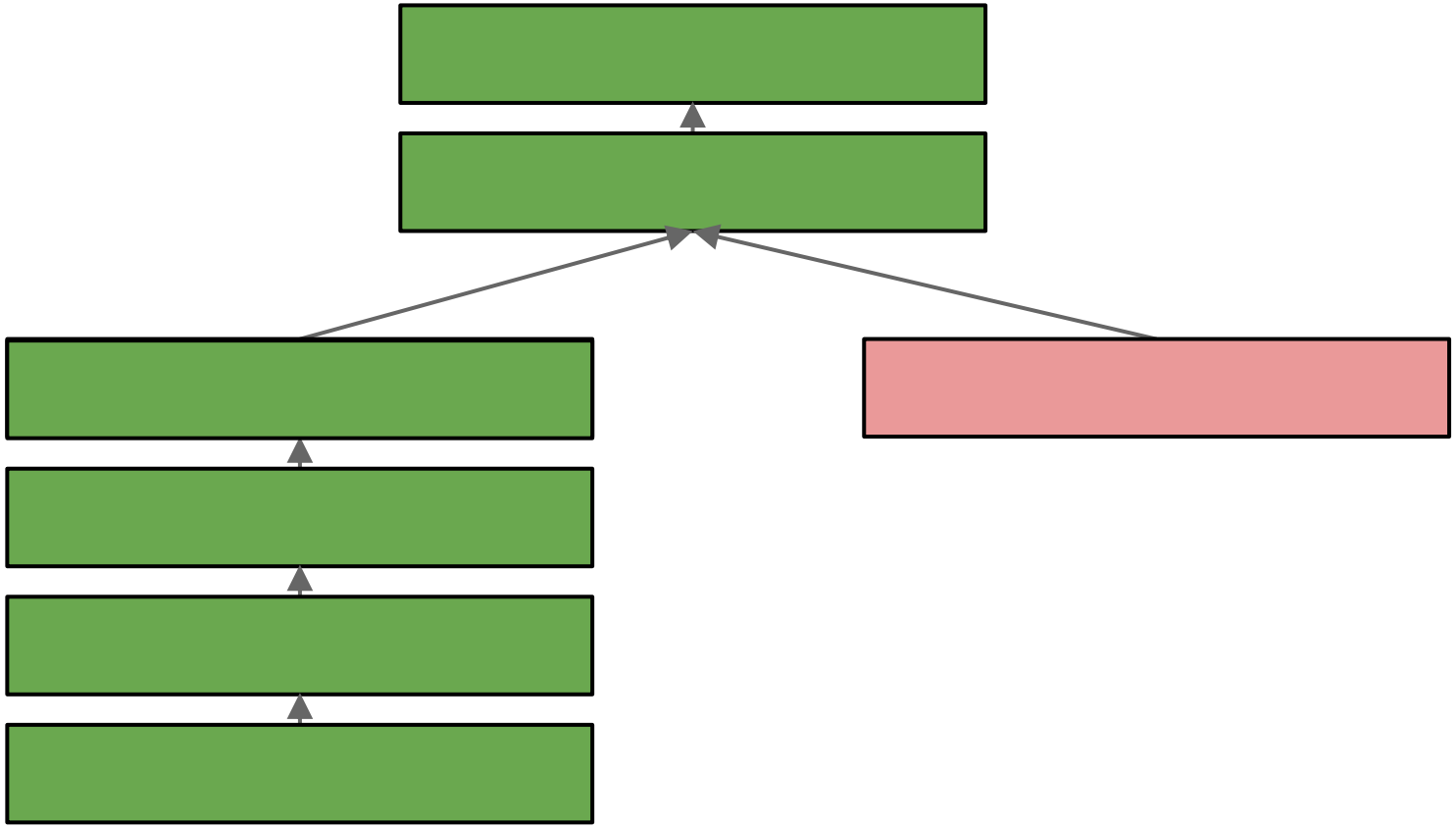
- A fork can occur when two miners publish blocks simultaneously. Such blocks are in conflict. (they may have different transactions, different nonce, etc)



- Problem: two different version of our public ledger

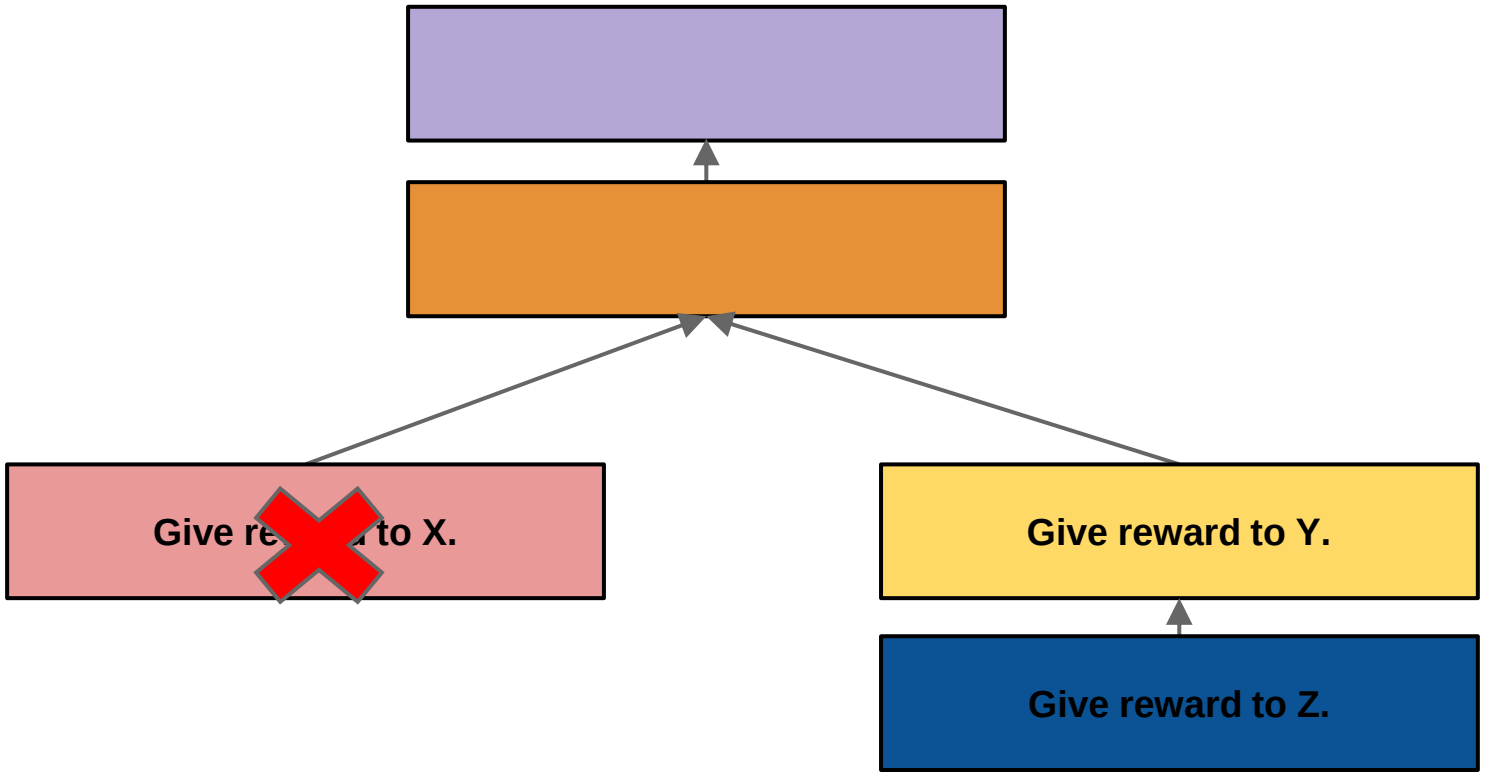
Forking Resolution

- Since it's a random process, one fork eventually becomes longer than the other one. The longer fork wins.



Forking Resolution

- It takes time to resolve conflicts. One of the forks is discarded with time.
- Effort spend on the smaller fork is wasted. All transaction in that fork are erased.



Transaction Confirmation

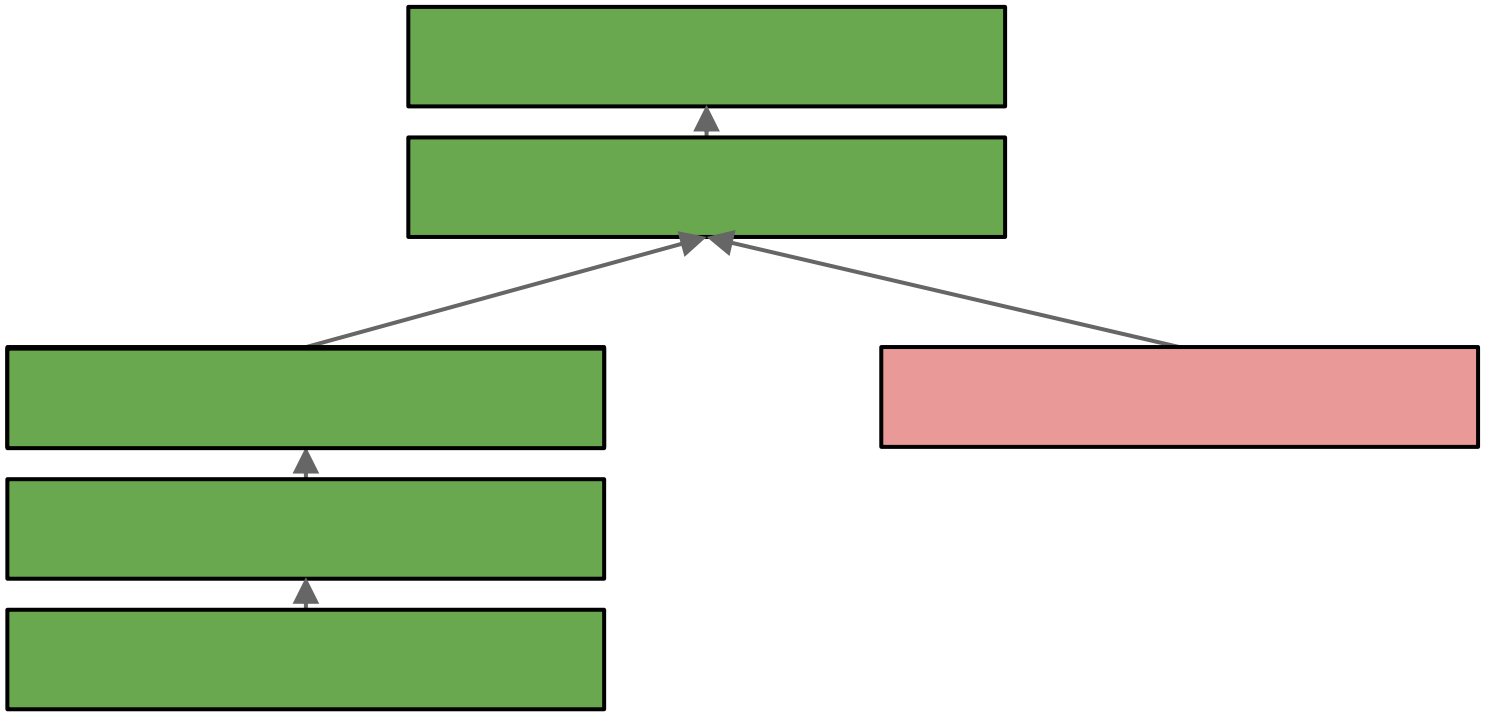
- A transaction is said to have received k confirmations if it has been published in a block that has been added to the blockchain, and k-1 more blocks have also been added.

- A transactions is typically considered “confirmed” once it has 6 confirmations.
  - This is to make sure its not erased because of some other fork becoming longer

- Newly minted Bitcoins are typically considered confirmed once they have received 100 confirmations. In practice: every merchant will accept them far sooner.

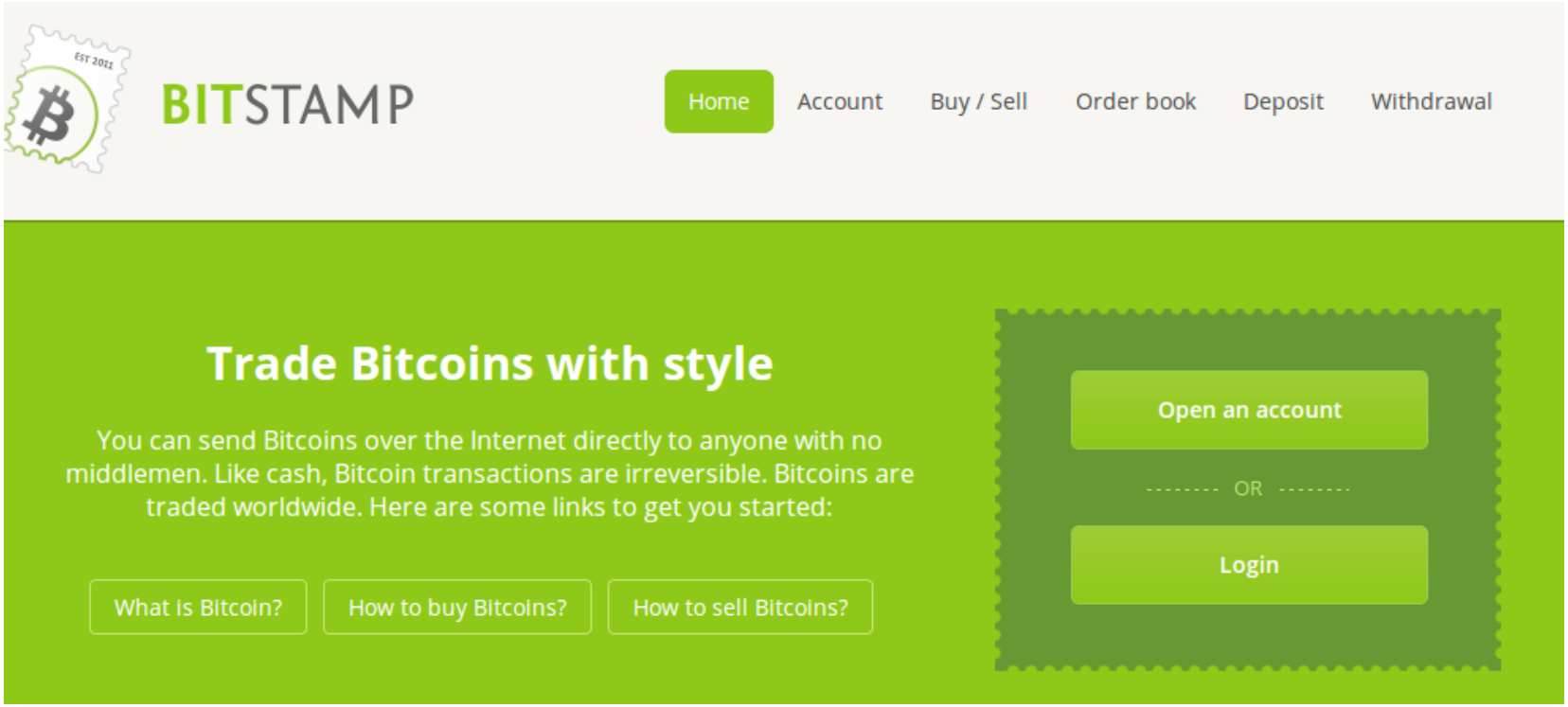
51 Percent Attack

- Say you have more computing power than all other miners combined.
- Take the discarded (pink) fork and keep extending it
- Since you can hash faster, it becomes the longest
- All transactions in green fork are erased!



Bitcoin Exchanges

- Use your US dollars or some other currency to buy Bitcoin from someone else
- Exchange is a trusted party which facilities this process
  - It will hold your dollars until the other party transfers their coin to you. Optional to use exchanges but simplifies the process.



Physical Bitcoin?

http://media.coindesk.com/2014/09/casascius-coins.jpg

- private key is embedded in coin and can be accessed (possibly electronically) only by physically breaking the coin
- trust creator to destroy any record of private key
- Having the physical coin = having the private key

Ongoing Research in Bitcoin/Blockchains

Some Burning Questions

- Scalability
- Usability
- Anonymity

...

Scalability / Speed

- Block size in Bitcoin = 1 MB. Can handle ~10 transactions per min
- Visa network: 5000 transactions per minute
- Further: transaction take up to 1 hour to “confirm”
- Can we do better? Many systems under development, many start-up companies.

Usability

Lost key?

Man accidentally threw away $127 million in bitcoin and officials won't allow a search

Shawn M. Carter | @shawncarterm | 12:30 PM ET Wed, 20 Dec 2017

Sam Hodgson | Bloomberg | Getty Images

https://www.cnbc.com/2017/12/20/man-lost-127-million-worth-of-bitcoins-and-city-wont-let-him-look.html# ia.

Usability

Stolen Key?

- Mt. Gox incident: $450 million stolen
- Coincheck: $530 million stolen
- DAO hack: $50 million stolen, Ethereum hard fork
- Parity Technologies: $421 million deleted
  - Earlier: $123 million

Anonymity

- While you are doing transactions, people only see your public key (address), not your real identity
- As such, nobody knows who you are: government, banks, or even the party who performs transactions with you
- However based on transactions patterns: one may derive information. For example,
  - Suppose everyone knows Alice and Bob are friends.
  - Suppose know Bob's public key
  - They say another public key running a lot of transactions with Bob => must be Alice
- System with near perfect anonymity: Zcash
  - Relies on zero-knowledge proofs

Questions and Discussion?