ELEC5616 COMPUTER & NETWORK SECURITY

Lecture B:

Bitcoin

DESIRABLE PROPERTIES OF CURRENCIES

Divisibility

The value of a kilogram of gold should be equal to two 500g blocks of gold

(counter: take an iPod and cut it in half)

Fungibility

Individual units should be capable of mutual substitution

(happy to exchange one $10 note for another, not one diamond for another)

Scarcity

There should be a reasonable restriction on the projected availability of the currency

Recognisability

It shouldn’t be difficult to verify an item of currency is genuine

LIMITATION OF TRADITIONAL CENTRALISED DIGITAL CURRENCY

Alice has $100 in her PayPal account and wants to buy X worth $25 from Bob

Bob asks for payment from Alice

Alice speaks to the PayPal server and asks to transfer $25 to Bob

Alice tells Bob the transaction has been processed

Bob checks with the PayPal server and confirms the transaction occurred

LIMITATION OF TRADITIONAL CENTRALISED DIGITAL CURRENCY

Advantages:

Transactions require minimal work for the clients

Transactions can be reversed in the case of fraudulent transactions

Transactions are secure and double spending / cheating can’t occur

Disadvantages:

The PayPal server is a valuable single point of failure

PayPal can shift or freeze money at their discretion

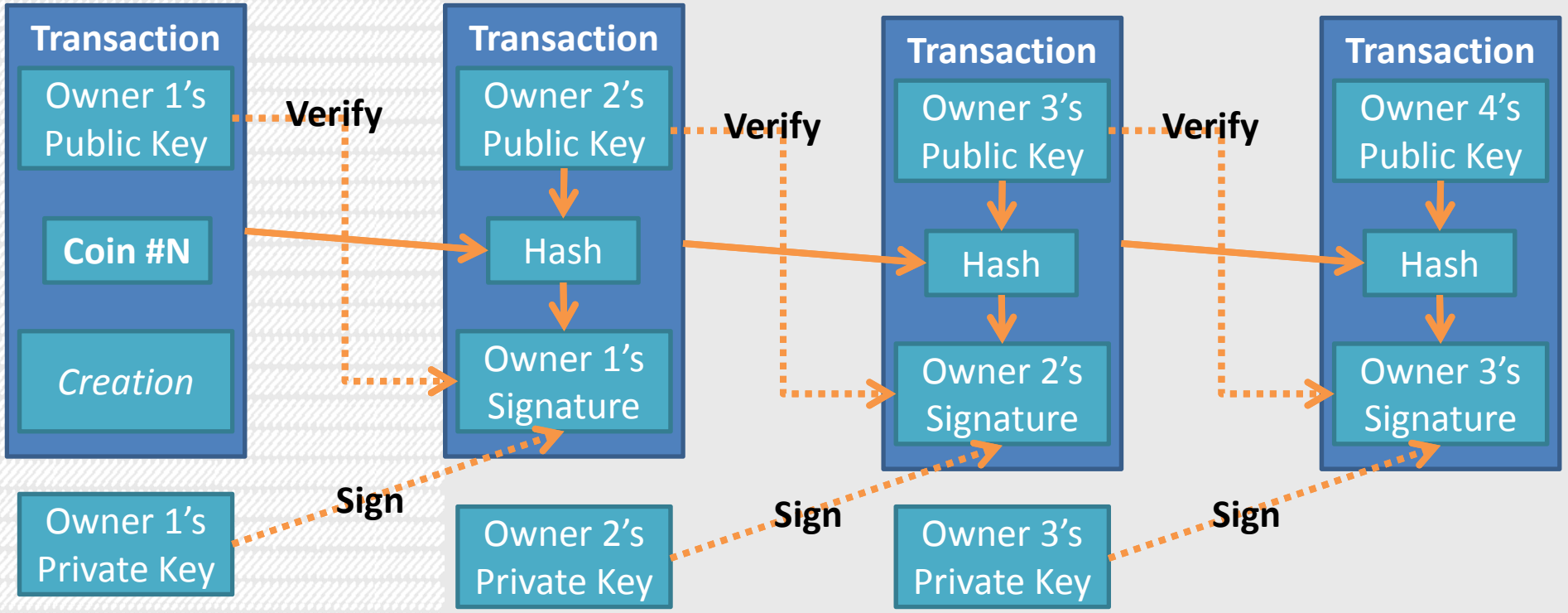
Alice and Bob can’t perform a transaction without the PayPal server

ELECTRONIC COIN AS A CHAIN OF DIGITAL SIGNATURES

Imagine we had a coin that we wanted to be able to transfer between others.

To transfer the coin,

1. The owner signs H(PrevTrans | $PublicKey_{NewOwner}$) with their private key
2. Adds the signature to the end of the chain
3. Gives the electronic coin (chain of digital signatures) to the new owner



ELECTRONIC COIN AS A CHAIN OF DIGITAL SIGNATURES

Advantages:

Transactions no longer require a third party (Trent / PayPal)

Assuming strong public key crypto, coins can’t be stolen

Disadvantages:

Nothing to prevent double spending

i.e. Mallory might “give” their coin to both Alice and Bob and then run off

ELECTRONIC COIN WITH A CENTRALISED MINT

Electronic coins now become similar to cheques: they're promises of cash that are only fulfilled when you confirm with the bank their account isn't empty

1. Mallory gives Alice a digital coin
   (this digital coin is composed of one or more digital signatures indicating change of ownership)
2. The mint (Trent/PayPal) verifies the signatures and most importantly **verifies this digital coin has not been "spent" already**
3. If this is all valid, the mint issues a new digital coin to Alice and marks the coin firmly as owned by Alice

If Mallory gives the digital coin to Bob after it has already been transferred to Alice, the mint can tell Bob that he has been cheated and the digital coin has already been transferred.

LIMITATION OF TRADITIONAL COIN-BASED DIGITAL CURRENCY

Alice has $100 in 100 $1 digital coins and wants to buy X worth $25 from Bob

These digital coins are backed by Trent at *CoinCompany*

Coin Acquisition

Coins are worth $1 and belong to whoever is the last in the owner chain

Alice's Coin = $[Alice]_{Trent}$ Alice's Coin to Bob = $[Bob \mid [Alice]_{Trent}]_{Alice}$

Alice pays Trent $100 in exchange for 100 digital coins

Trent signs each coin stating Alice is the owner

Alice creates a public key that Trent signs, allowing her to sign coins to others

Payment

Bob asks for payment from Alice

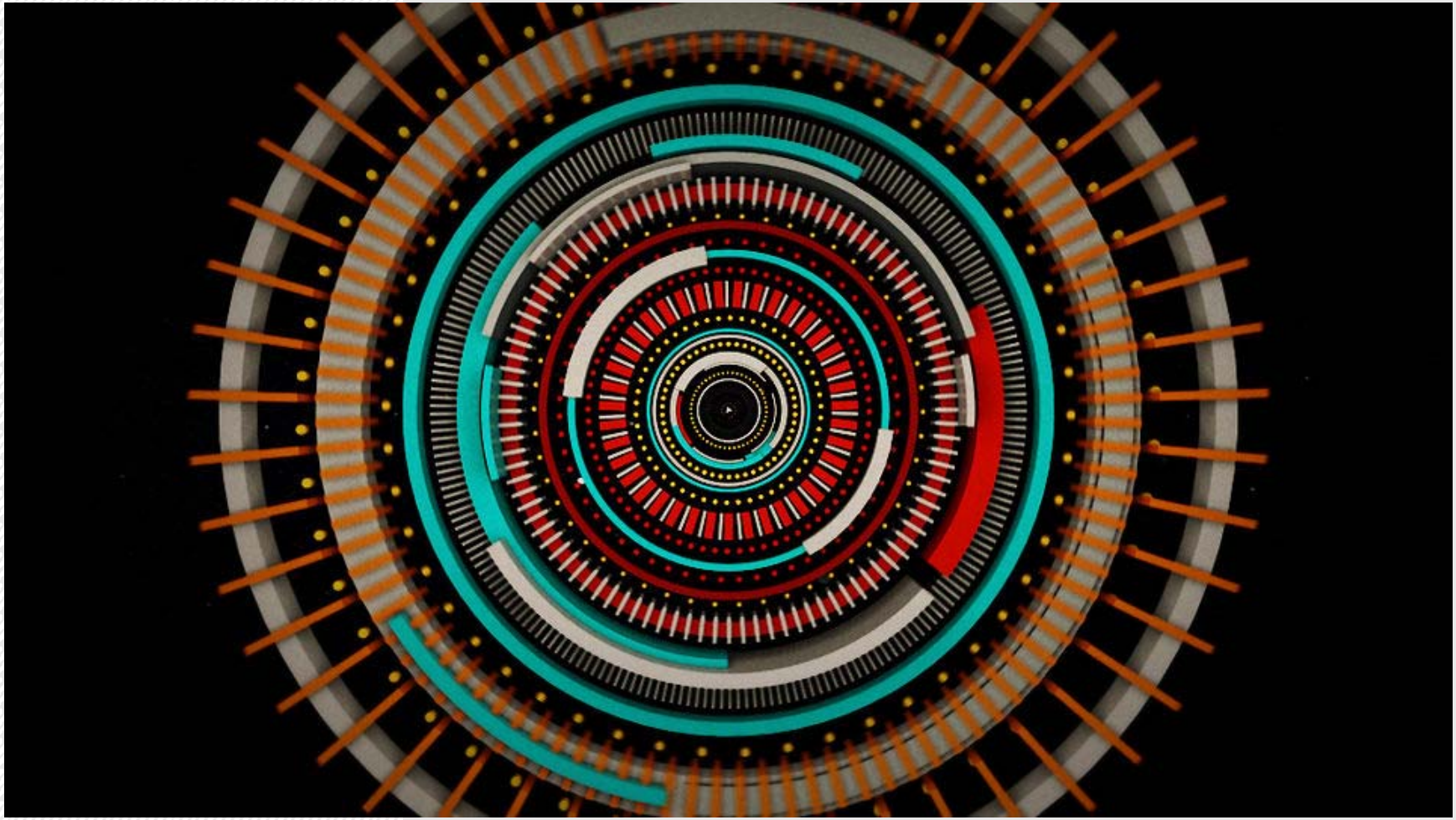
Alice takes 25 of her 100 digital coins and for each signs "Owned by Bob"

Alice sends Bob the coins and the new signature

Bob can cash the digital coins in at a later date with Trent at CoinCompany

BITCOIN OVERVIEW VIDEO

Bitcoin Video



OVERVIEW OF BITCOIN

Bitcoin uses public key encryption to secure transactions

– Public Key is like a bank account number

– Private Key is like your credit card / PIN / password

A “block chain” takes the place of a central server (Trent or PayPal server)

– Transactions are announced to the peer-to-peer network

– All transactions are visible to nodes in the peer-to-peer network

Bitcoin miners are rewarded for operating the block chain

– The creator of the next block is awarded the set of newly minted Bitcoins

– The creator of the next block is awarded the transaction fees

BEGINNINGS OF BITCOIN

Paper published in 2008 by pseudonymous developer Satoshi Nakamoto

(whilst only a short paper – 8 pages – this has had a greater impact than most researchers could ever dream to achieve)

No-one knows who Satoshi Nakamoto is... All we know is that he/they

1. created the open-source Bitcoin client
2. mined many of the first Bitcoins (millions of dollars minimum)
3. disappeared

Bitcoin has proven surprisingly strong, both the protocol and client

Immense incentive to break Bitcoin's security – millions of dollars on the line in a field where no-one has been prosecuted for stealing digital bits

ANATOMY OF A BITCOIN

Currency needs to be **scarce** and **divisible**

Scarcity

There will only ever be 21 million Bitcoins

They're be released in a predictable and slow fashion – mining

(specifics of mining will be discussed later)

Divisibility

Whilst there's only going to be 21 million Bitcoins, each Bitcoin is divisible

A *Bitcoin* can be divided into 100 million smaller units called *Satoshis*

1 **BTC** = 1,000,000 x 100 **Satoshis**

WHAT DOES YOUR WALLET LOOK LIKE?

Want a Bitcoin "bank account"?

Create a public and private key. The public key is your bank account number.

This is traditionally referred to as an "address".

The private key allows you to transfer Bitcoins away from that account

Whilst you can use a single address indefinitely, it's quite common for a new address to be created for *every single transaction*

Account Number (public key)	Bitcoin Balance
1CkH8epnCee2jSnoYKVf2no8564LygpZcr	1.5027
1Lm9AuUUcazH54qFFW1Rt3V35mNvUCVFb1	17.3723
1D8L2KPG2U8mUqu6seE1GrYCRw2tkCxBHR	0.2
1NbLhL5xGS1YF8LEcXo588EPWSswgsvizb	23.5643
...	...

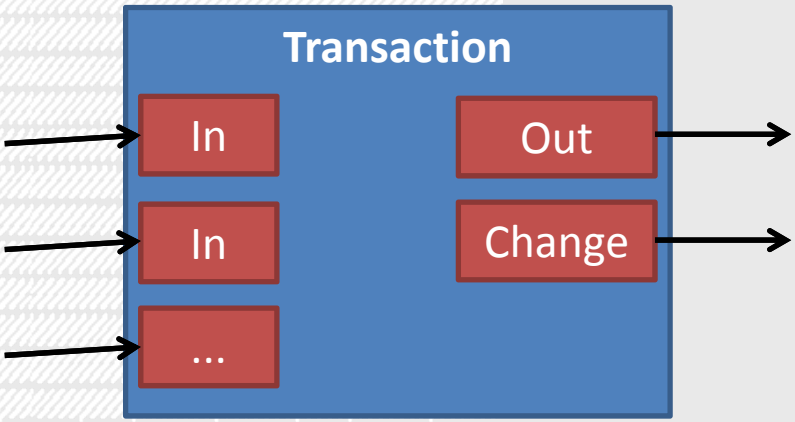
BITCOIN TRANSACTIONS

Transactions are based upon the chain of digital signatures seen earlier

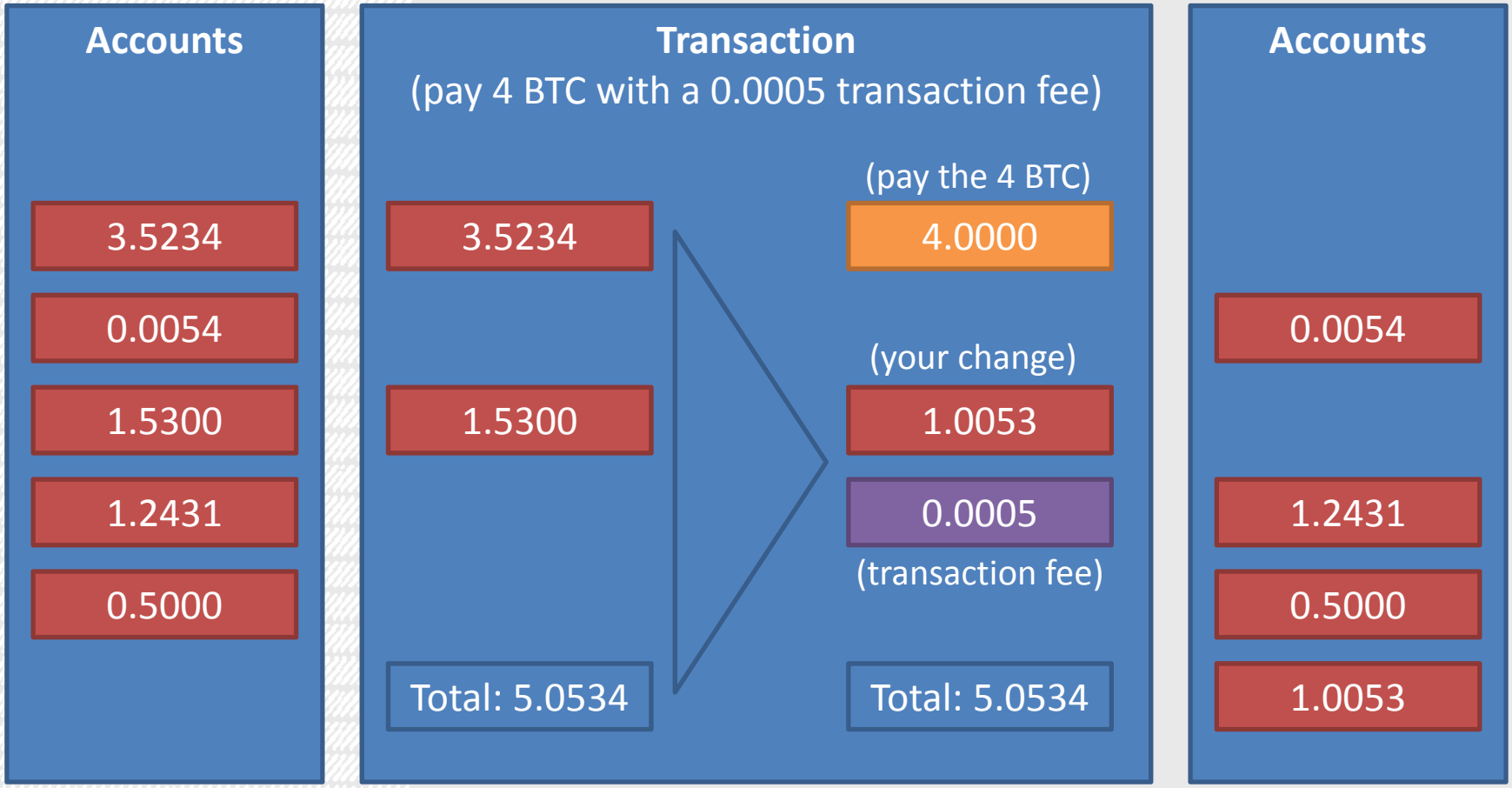
We could have a chain of digital signatures per coin but that means to transfer **N** Satoshis we'd need to perform **N** transactions

(imagine doing a large payment using 1 cent coins..!)

Bitcoin transactions: one or more inputs, one or two outputs, optional transaction fee (outputs = one for payment, one for returning change)



BITCOIN TRANSACTION EXAMPLE



HOW DO YOU PREVENT DOUBLE SPENDING?

The above is just a variation on the chain of signatures seen earlier

How do we ensure that Alice is only giving her coin / set of coins to Bob and not giving it to multiple people at the same time?
(i.e. how do we ensure no-one is double spending)

We don't want a single person (Trent) / group (PayPal) holding all the power

We don't want people to be able to unpredictably game the system

This is the ingenious part of Bitcoin: the block chain

THE BLOCK CHAIN

Payee must be able to “prove” the previous owners didn’t double spend (we’ll assume the earliest transaction is the one that counts)

How can we ensure that no previous fraudulent transaction has occurred?

We must be aware of all previous transactions

To accomplish this without a trusted third party:

1. Transactions must be publicly announced
2. All participants must agree on a single history for the order of transactions

THE BLOCK CHAIN PROPERTIES

The block chain must serve two core properties:

1. The block chain must definitively record all transactions and show the order in which these transactions occurred in the network
   (achieved using a *timestamp server*)
2. The block chain must be difficult to modify: specifically, it should be difficult to modify an existing block chain such that you can add, remove or modify previous transactions
   (achieved using a *proof-of-work*)

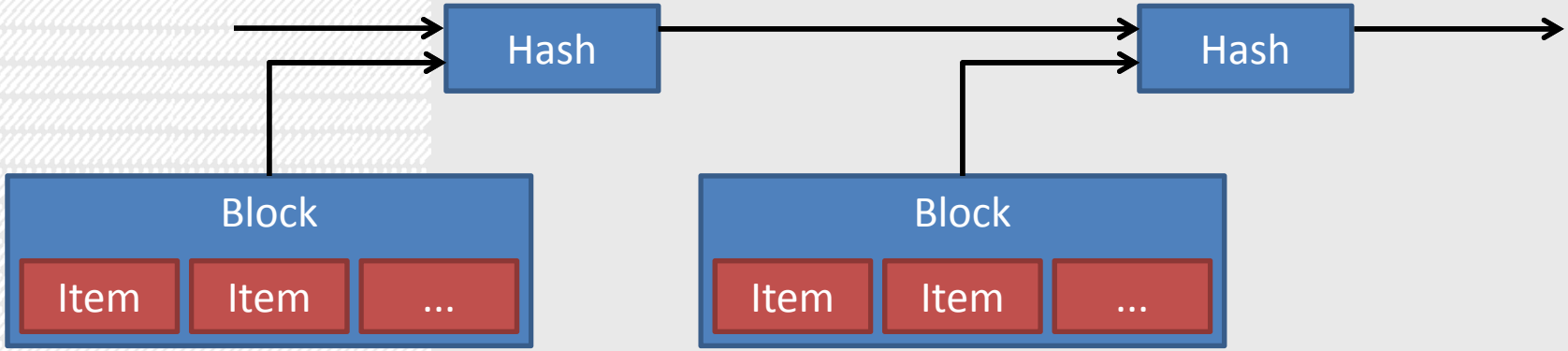
THE BLOCK CHAIN (TIMESTAMP SERVER)

Timestamp Server

Take a group of items from timestep **N** and combine them into a block $\mathbf{B_N}$

$$\mathbf{H_N = H(B_N + H_{N-1})}$$

Each hash is dependent on the previous hash
Thus, to add, remove or modify a previous item, you also need to recalculate all the hashes up to this point



THE BLOCK CHAIN (PROOF-OF-WORK)

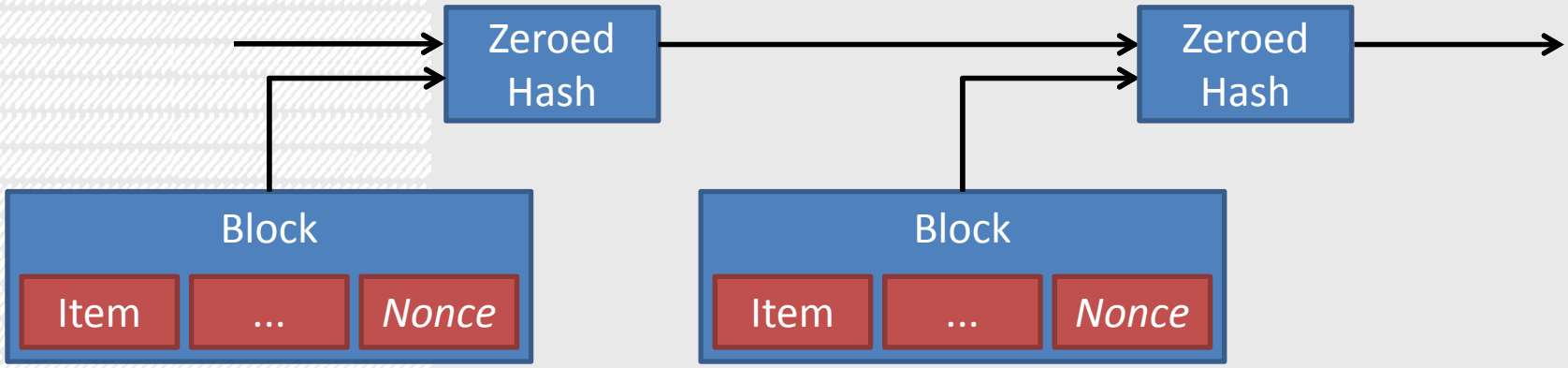
Proof-of-Work

Pure hashing isn't difficult, so modifying the timestamp server's chain is trivial

Make the task of hashing difficult:

modify a nonce until the hash starts with a set number of zero bits

Now to modify the timestamp server's chain, substantial work is required



THE PEER-TO-PEER NETWORK

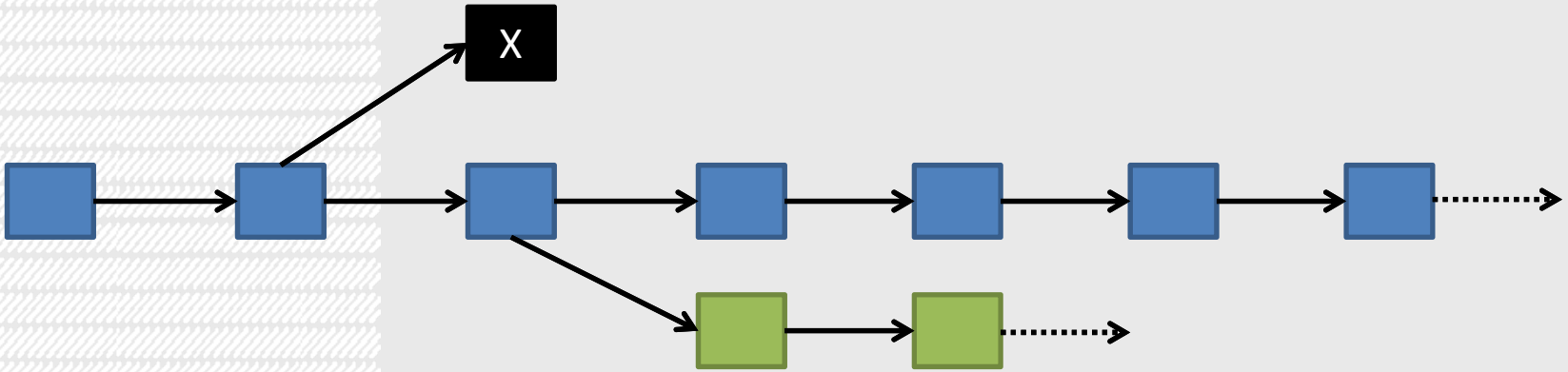
The peer-to-peer Bitcoin network runs as follows:

1. New transactions are broadcast to all nodes
2. Each node collections new transactions into a block
3. Each node works on finding proof-of-work (zeroed hash) for that block
4. When a node “solves the puzzle”, it broadcasts this to all other nodes
5. The other nodes verify the block by checking all transactions are valid and that the hash is a valid proof-of-work
6. Nodes express acceptance by working on creating the next block in the chain after this block, using the hash of the now accepted block

P2P AND THE BLOCK CHAIN

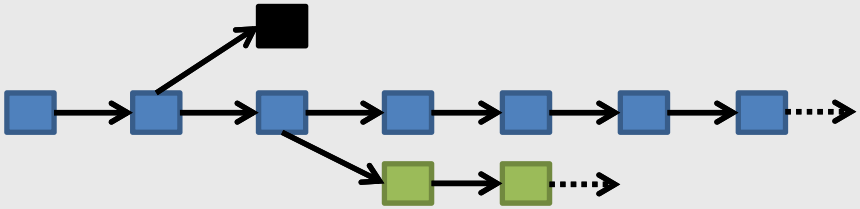
Ties are resolved when one of the competing heads solves the next block (remember: longest block chain is the most authoritative)

To fork the block chain, you need > 50% of the computing power in the network, otherwise your block chain will always be shorter
(i.e. if green and blue proceed at the same rate, or green is slower, the green block chain will never catch up)



TRANSACTION CONFIRMATION

If you're really unlucky, your transaction will end up in a dead branch



If your transaction ended up in the black or green branches, it's invalid as far as the majority of the network is concerned
This opens you up to double spending attacks

Transaction Confirmation
Wait a certain number of blocks – the more blocks you wait, the more certain you can be that your transaction will be permanent and irrefutable

Six confirmed blocks (around one hour) is generally considered entirely safe

INCENTIVES FOR MINING (CHINESE LOTTERY)

If your computer solves the proof-of-work in the next block chain, you receive two significant rewards

Mining Reward (early and declining reward until all 21 million BTC mined)

Only way to create and distribute new Bitcoins

Started at 50 Bitcoins per block, every approx 4 years drops in half

Eventually it will hits zero when the final Bitcoin is mined

Transaction Fees (permanent reward and increasing with heavier use)

Transaction fees are optional but encourage your transaction to be included early – if you have a low or zero transaction fee, you may need to wait several confirm blocks before your transaction is included (block creator's discretion)

Insight: creating blocks is still necessary for transactions even if mining no longer results in any Bitcoin reward – transaction fees give the incentive

PROOF-OF-WORK DIFFICULTY

Transactions rely on confirmed blocks before being valid (confirmation)

Bitcoin wants to produce a new block every approximately 10 minutes

Issue: what happens if the Bitcoin network's computing power rises or falls?

Solution: every 2016 blocks (approx two weeks), the difficulty of the proof-of-work is adjusted to try to make the next 2016 blocks take two weeks

Hash Format:	**XXXXXXXXXXXXXX**
Trivial:	00**XXXXXXXXXXXX**
Easy:	0000**XXXXXXXXXX**
Harder:	000000**XXXXXXXX**

MINING IN THE AGE OF ASICS

Bitcoin mining follows that of password cracking: CPU, GPU, FPGA, ASIC

Application-Specific Integrated Circuit (ASIC) is entirely custom hardware

Best multi-core CPU:	~35 Mhash/s	
Average GPU:	~200 Mhash/s	
Multi-card GPU setups:	1-2 Ghash/s	
FPGA:	10-25 Mhash/s	(far lower power usage)
$1k ASICs:	5-60 Ghash/s	
$30k ASIC:	1,500 Ghash/s	

Numerous Bitcoin mining botnets were discovered in the early days of Bitcoin when clusters of CPU and GPU systems could dominate mining

June 2011: an ABC employee was found to be mining on company servers without permission

THE STRENGTH OF BITCOIN

"Entire classes of bugs are just missing. Bitcoin has fixed almost all flaws that aren't forced by design." – Dan Kaminsky

The Bitcoin protocol is entirely open source and has been for years

Most importantly, breaking Bitcoin would be valuable and has had no legal precedents set against it yet

Bitcoin's security resides in three places:

– Strength of digital signatures (ECDSA) protects people's bank accounts

– Strength of SHA256 is basis of the proof-of-work

– General secure programming

Breaking any one of these would make you quite rich. Even if one of these were broken in the future, Bitcoin is made to be upgradeable

ATTACKS ON BITCOIN

Improper Verification

Verification wasn't properly done on transactions before they entered the block chain and less than a week after discovery a fraudulent transaction resulted in 184 billion fake Bitcoins being created
(reverted by the community)

Block Chain Forks

The block chain temporarily forked into two independent chains due to a major software bug. The new Bitcoin client produced a transaction that wasn't accepted by the older client, splitting the block chain and producing the first real world examples of "double spending".

Control of the Network

If an attacker had more than 50% of the computing power of the network, the attacker could perform double spending and also reject other people's transactions from receiving confirmations

ATTACKS ON BITCOIN EXCHANGES

Bitcoin exchanges are the weakest link in the Bitcoin security chain:
– Bitcoin exchanges are only required to buy or sell Bitcoins, yet many users decide to leave all their money in the hands of a third-party service

– Most secure method: transfer the Bitcoins from the exchange to accounts that only you have the private key for and keep a “wallet” locally

Numerous Bitcoin Exchange Hacks

200k (Bitcoin Savings and Trust) + 78k (MyBitcoin) + 47k (Linode hacks) + 40k (Bitcoinica) + 35k (InstaWallet) + 24k (Bitfloor) + ...

At peak valuation (1 BTC = $200), we’re talking hundreds of millions..!

Majority of hacks are due to poor developer practices, side attacks (Linode) and social engineering of supporting services (email, domain names, ...)

SCALABILITY OF BITCOIN

Assume Bitcoin did as many transactions per second as VISA (~2000 tps)

Bandwidth
60 GB every 60 seconds requires each P2P node 8 gigabits per second b/w

CPU
A network node capable of keeping up with VISA would require 50+ cores
(not counting any computing power required for mining)

Storage
Requires 3 terabytes of disk space for every 21 days of operation (1GB / block)

The future either improves this system or results in supernodes rather than fully decentralised system

BITCOIN SCRIPTING

Bitcoin uses a stack based scripting language to verify transactions

Scripting provides flexibility on spending transferred Bitcoins

– You could require two or more private keys

– You could require no private keys

– Give money to anyone who can solve a puzzle (i.e. Find any **x** s.t. H(**x**) = **y**)

A transaction is valid if nothing in the combined script triggers failure and the top stack item is true (non-zero).

See https://en.bitcoin.it/wiki/Script for an example

BITCOIN SCRIPTING AND INSERTING DATA

A transaction is valid if nothing in the combined script triggers failure and the top stack item is true (non-zero).

There's also explicitly OP_DROP (or drop the top item on the stack)

This means messages can be encoded in the transaction's verification code.
Including questionable and/or illegal contact.

– Pornography links (may or may not lead to child porn)
– 2.1 MB of Wikileaks
– Random news text fragment (Genesis block by Satoshi)
– Illegal primes (i.e. a number that represents an illegal number)
– Len Sassaman (http://pastebin.com/raw.php?i=BUB3dygQ)

BITCOIN, ANONYMITY AND PRIVACY

"Bitcoin transactions are more private than credit card or PayPal transactions, but are less private than physical world cash transactions. Unless you are very careful in the way you use Bitcoin, you should assume a persistent, motivated attacker will be able to associate your IP address with your Bitcoin transactions."

Gavin Anderson, lead developer on Bitcoin

All transactions are in the public domain meaning:

–numerous tools already exist to combat fraud or to trace money laundering that can be adapted to the Bitcoin network

– once your identity is linked to a single account your identity can propagate backwards or forwards through all your connected transactions

Does use of many random accounts equal anonymity? No. But it can help. (proposed extension to Bitcoin, Zerocoin, would improve this situation)

REFERENCES

Bitcoin: A Peer-to-Peer Electronic Cash System

– Satoshi Nakamoto

Bitter to Better – How to Make Bitcoin a Better Currency

– Simon Barber et al.

Frontiers of Finance: An Introduction to Bitcoins

Some Thoughts on Bitcoin / Black Ops of TCP/IP

– Dan Kaminsky