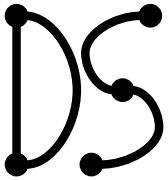


Research Group
Distributed Systems

Blockchain & Bitcoin

Olaf Landsiedel

Welcome

- The students from
  - Blockchain and Robotic Process Automation

Last time?

- Applications I
  - More on DHT: CAN
  - Bittorrent

Q1: What is a Bitcoin?

- Have you seen one? Do you own one?
- Bitcoin is a digital currency

Bitcoin Address

18a7fQxBBZUw4TPD98pXECn83yxGgvRC7o

Bitcoin Address Compressed

1LnxdWSxXcUwj1WTWQPEEMJ2wSM19gV5RQ

Public Key (130 characters [0-9A-F]):
0448694DF67E50D6805FBEC54CD9C833137F30C70062BBAF18F5213E9C471BC1C79
3F623B77E6108410C06057DDB4F8E7E48E268A9A782CEFFC27409AA3D7AF01F

Public Key (compressed, 66 characters [0-9A-F]):
0348694DF67E50D6805FBEC54CD9C833137F30C70062BBAF18F5213E9C471BC1C7

Q2: Who invented Bitcoin?

Bitcoin: A Peer-to-Peer Electronic Cash System

White paper:
Published by Satoshi Nakamoto
In 2008

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

GMX email address…

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Q3: Who is Satoshi Nakamoto?

- Person or persons who
  - wrote the bitcoin paper
  - wrote the bitcoin code in 2007 – 2010
- Speculation on who he/she/they are continues
  - Name is likely a pseudonym

Q4: First Transaction (First Block)?

- The transaction in the genesis block reads:
  - "The Times 3 January 2009 Chancellor on brink of second bailout for banks"
  - The title of The Times on that date
- Underlying Bitcoin is blockchain

THE TIMES

Saturday January 3 2009 timesonline.co.uk

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets". The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to reduce lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of intervention are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it
Body&Soul

Detox in style
The best spas on the planet
Travel

Salman Rushdie
I won't marry again
Pages 22, 23

Giant killing?
Guide to the FA Cup third round
Sport

Q5: First Money Transaction?

- When? And What?
- On 22 May 2010, Laszlo Hanyecz made the first real-world transaction
  - buying two pizzas in Jacksonville, Florida for 10,000 BTC.

- How much would this be worth today?
  - December 2018: 29.673.806,42 Euro
  - Very expensive Pizza

Q6: What is a Blockchain?

- Have you seen one?
- Have you used one?

- A blockchain is a distributed record of transactions (=distributed ledger)
- The “heart” of Bitcoin

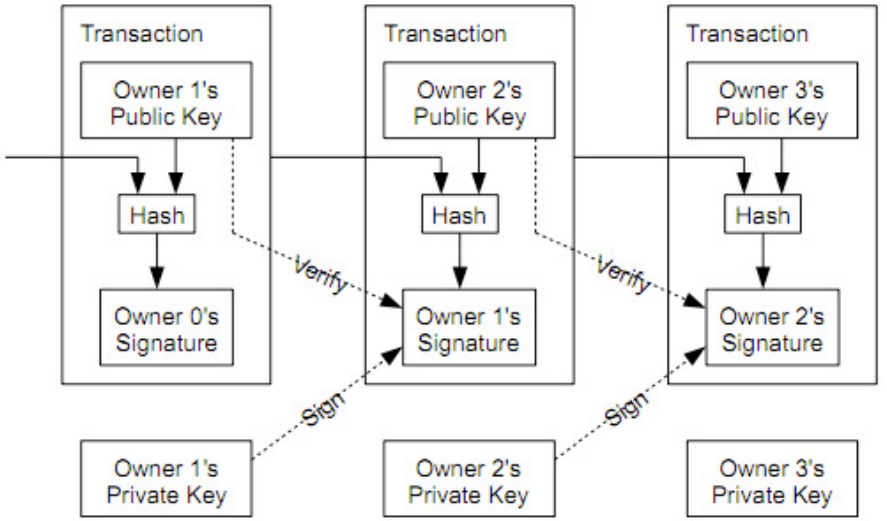


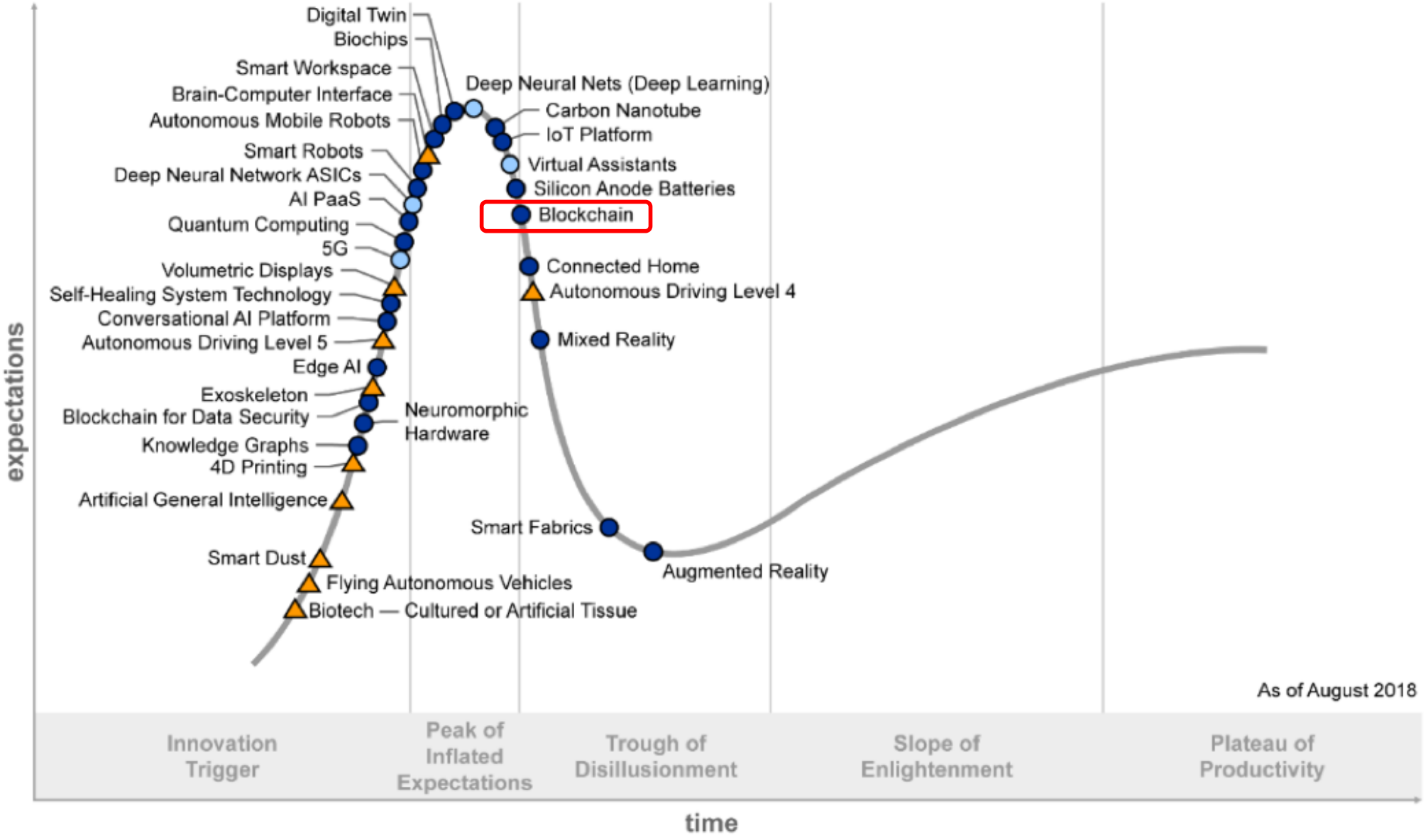
Image Credit: https://bitcoin.stackexchange.com/questions/10279/explainations-about-chaining-of-transactions

Today (and next two lectures)

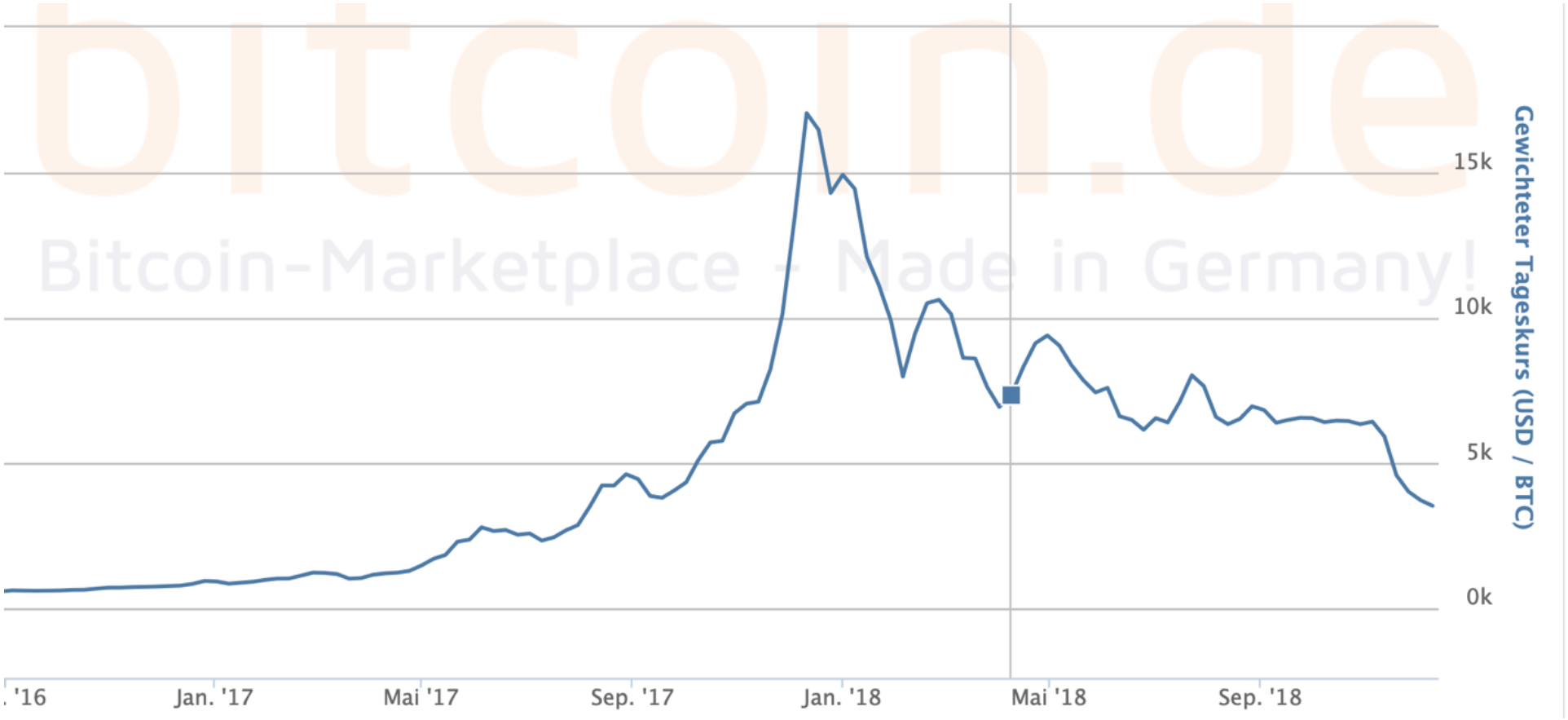
- Answers the questions from the previous slides
- Introduce you to
  - Bitcoin and other digital currencies
  - Blockchain
  - Smart Contracts
  - Focus on the concepts

  - We will see how far we get today…
- Bitcoin and blockchains are distributed systems
  - Built, in part, on the concepts introduced in the course

WHY DOES BITCOIN MATTER?

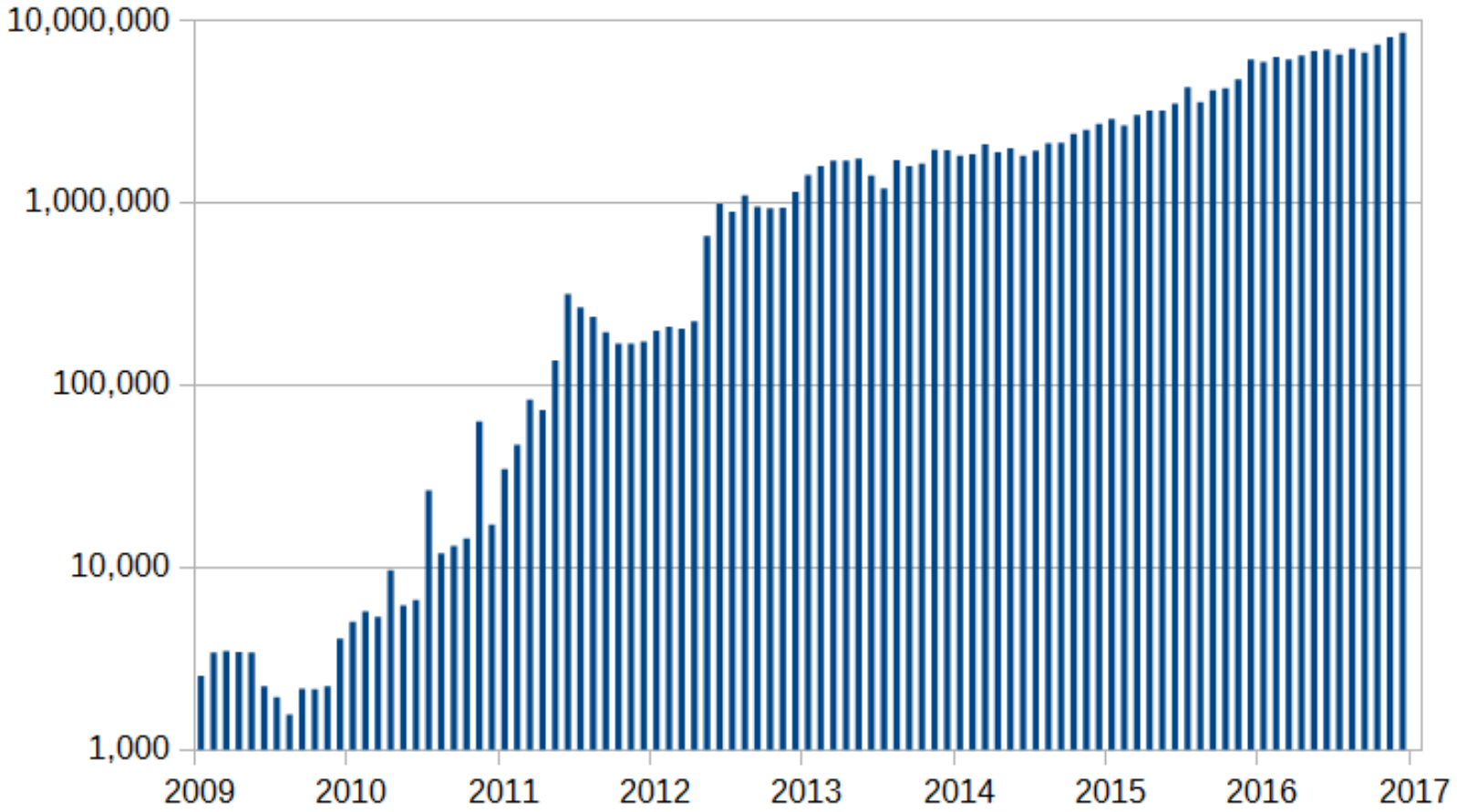


Reason I: Money



- Bitcoin to USD rate

Reason II: Transactions per Month



Note logarithmic scale on y-axis

Image credit https://upload.wikimedia.org/wikipedia/commons/c/c8/BTC_number_of_transactions_per_month.png

The dark side of Bitcoin?

BUT…

Bitcoin Prize

- “Uncontrolled” Currency
  - No governmental entity
- Can also be used for illegal activities
- Highly volatile
- Energy consumption

Bitcoin: Energy Consumption

Image Credit: https://digiconomist.net/bitcoin-electricity-consumption-surpasses-singapore-portugal

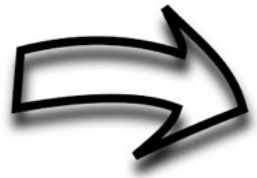
- Electrical Power Consumption
  - Germany: about 580 TWh (2016)
  - Nuclear Power Production: Germany (2016): 85 TWh
  - Singapore: 49.5 TWh per year
  - Portugal: 49.8 TWh per year
- Why?
  - Bitcoin Mining is energy intense!

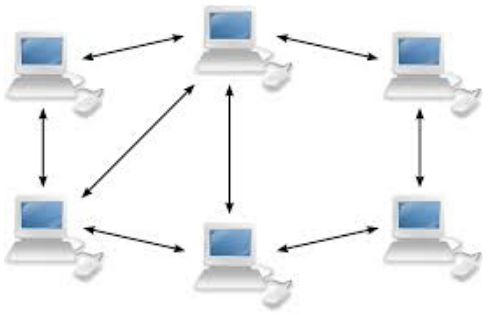
BUILDING BLOCKS

Building Block I: Blockchain

- Blockchain networks are peer-to-peer networks
  - Permissionless blockchains
    - any client can sync to the network and begin to participate
  - Note: permissioned blockchain also exist
- Uses:
  - Consensus mechanisms & cryptographic primitives
- to ensure consistency & agreement among all replicas
  - Make sure everyone follows the rules (Cmp. to Bank)

Bank





Blockchain

Building Block II: Crypto Currency

- Cryptographic tokens (cryptocurrency)
  - are a cryptographically secured digital unit of account (numeraire),
  - medium of exchange (currency), and
  - a store of value.
- Token balances are stored on the blockchain database.
  - An account address is identified by the public key of a user.

Smart Contracts

- A virtual machine:
  - Enables programmable blockchain transactions
- Smart contracts are
  - Code that runs inside the blockchain
  - Fully distributed
  - Triggered by external events

Example:

If Germany wins over the Netherlands ten times in a row, pay 10 Bitcoins from account A to account B

Before we go deeper

WARNINGS

Warning I

- Blockchain is more than Bitcoin
- Blockchain is more than digital currencies

- But, let's start with Bitcoin
  - As this is where is all started to go big

Warning II: Bitcoin is questioned

Eric Schmidt (Google)

„[bitcoin] is a remarkable cryptographic achievement and the ability to create something which is not duplicable in the digital world has enormous value“ (March 2014)

Jamie Dimon (JPMorgan)

„worse than tulip bulbs“,
„it's a fraud“

(Sept. 2017)

Peter Thiel (Clarium Capital, Palantir, Facebook)

„if bitcoin ends up being the cyber equivalent of gold it has a great potential left“

(Oct. 2017)

Warren Buffett (Berkshire Hathaway)

“with almost certainty [cryptocurrencies] will come to a bad ending”

(Jan. 2018)

Warning III: Bitcoin is questioned

- In this lecture we look at the technical concepts
  - Of Bitcoin, Ethereum etc.
  - Including blockchain and smart contracts
  - And their applictions beyond digial currencies

- This lecture is neutral on whether Bitcoin and other crypto currencies will be success
  - It does not encourage investments in this domain
    - Highly risky, see also previous slide

Today

- Motivation
- Bank transfers
- Cyrpto Primer
- …

Motivating Digital Currencies & Distributed Ledgers

BANK TRANSFERS

Banking Today

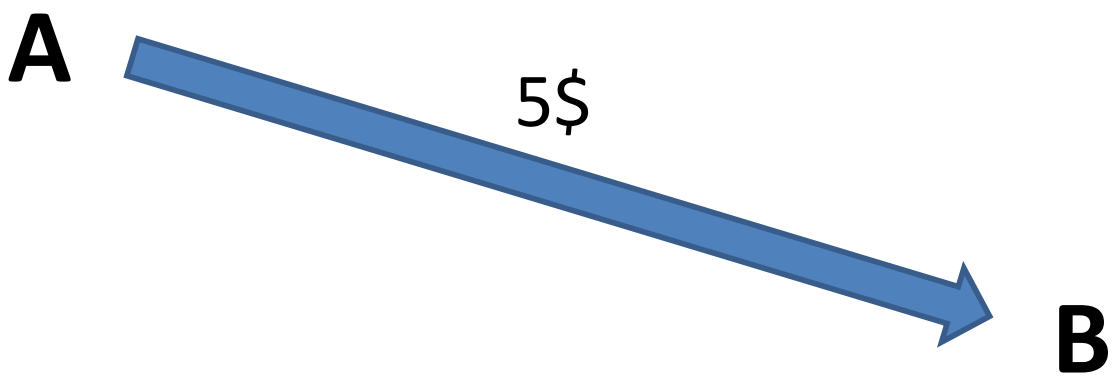
- How do we transfer money?
  - Via a trusted third party (=Bank)
- Where is the record of this stored?
  - Bank
  - Centralized ledger

Traditional Money Transfer

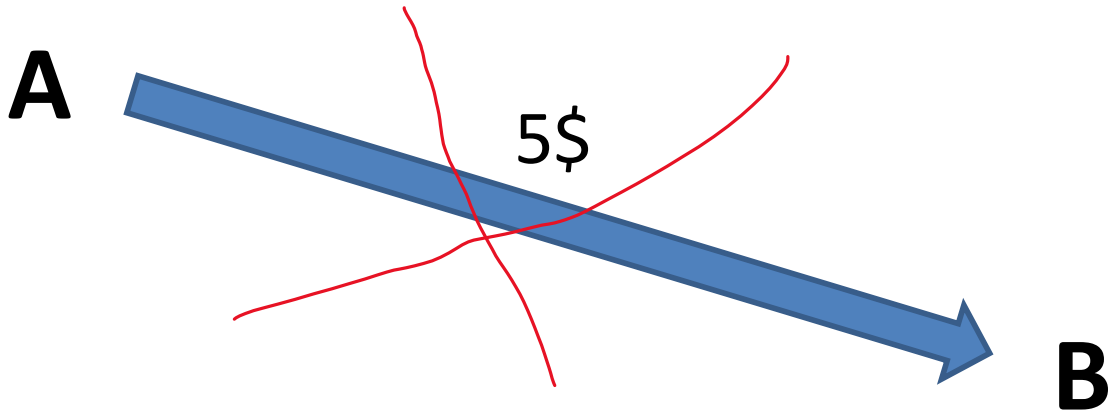
A

B

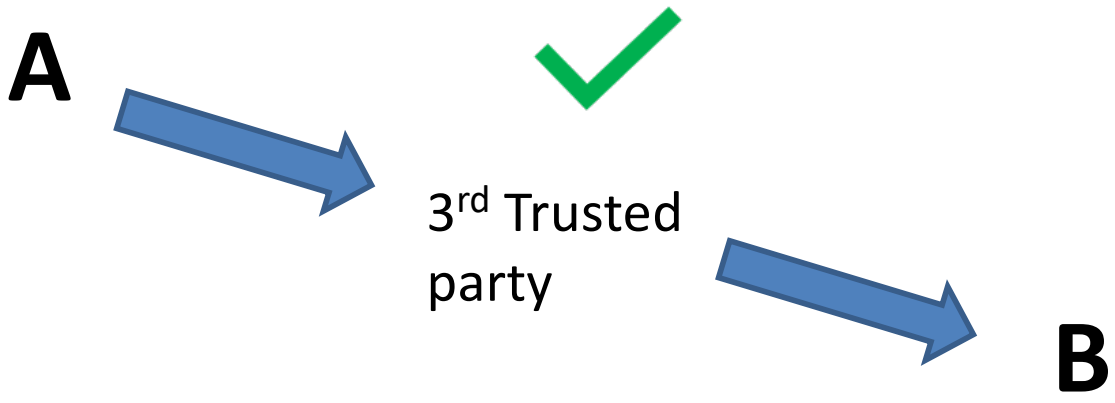
Traditional Money Transfer



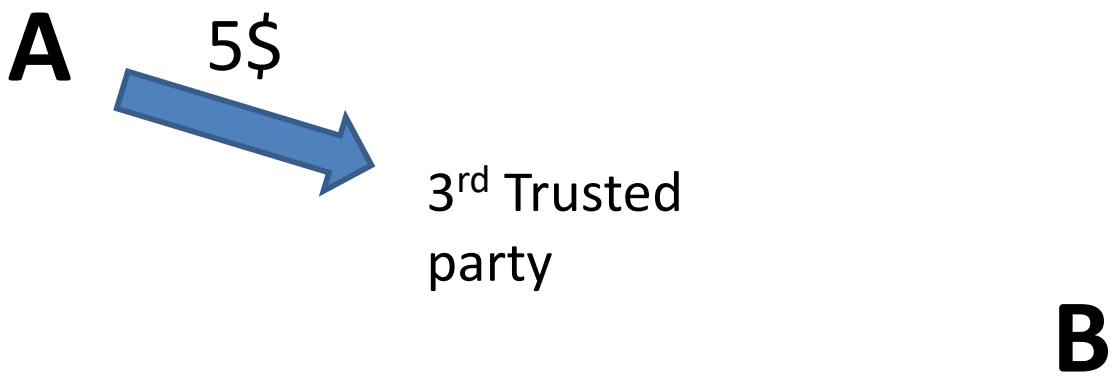
Traditional Money Transfer



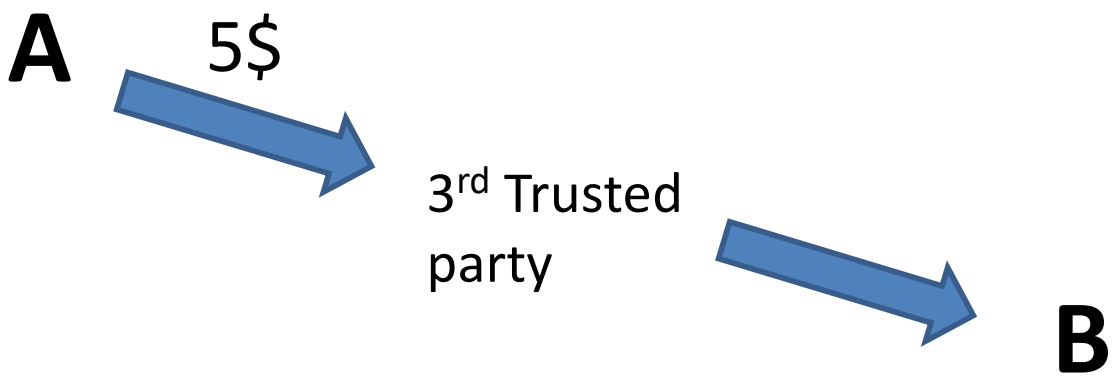
Traditional Money Transfer



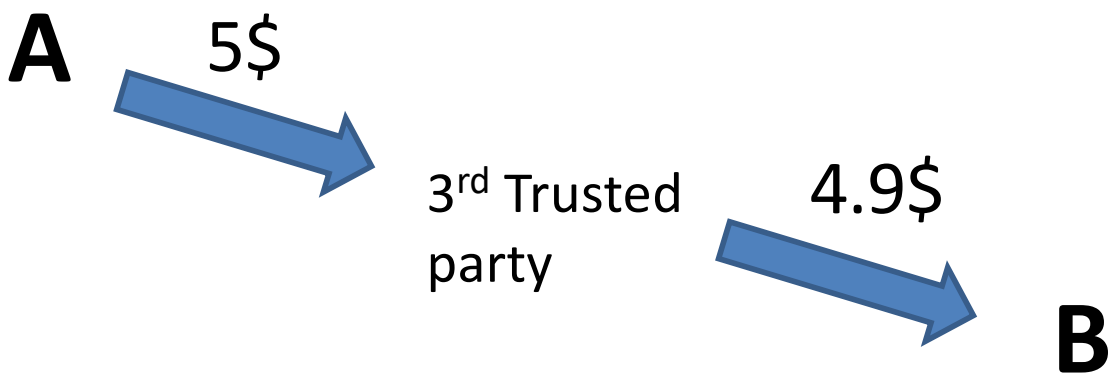
Traditional Money Transfer



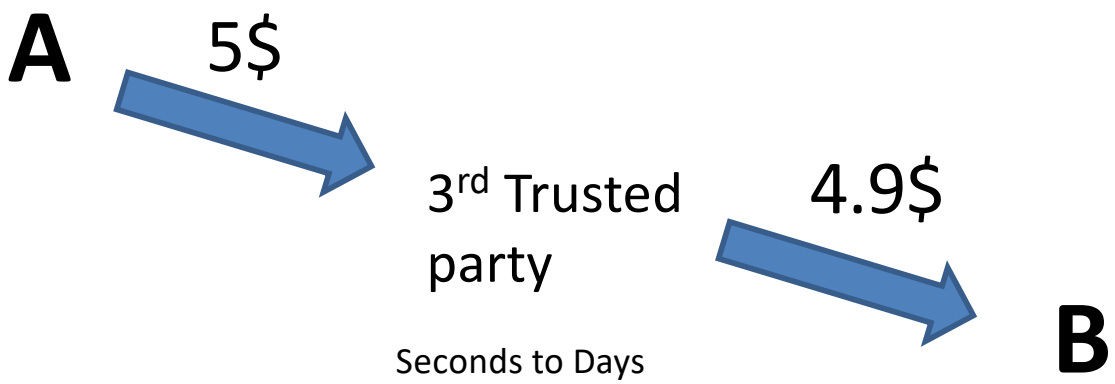
Traditional Money Transfer



Traditional Money Transfer



Traditional Money Transfer



Blockchain Aims to

- Eliminate the middleman
- Eliminate double spending
  - If there is no middleman: who makes sure that I spend each Dollar only once?
- Do it faster
- More Secure
- Traceable history

Ledger

A

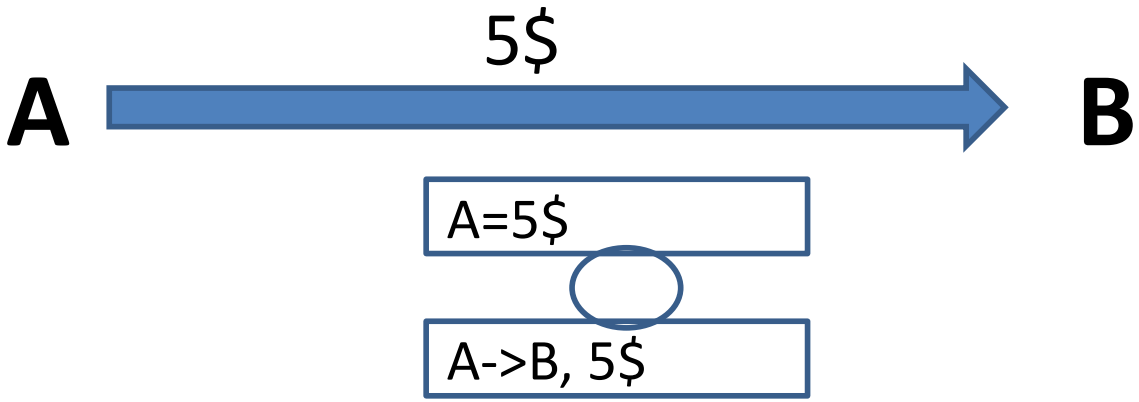
B

A=5$

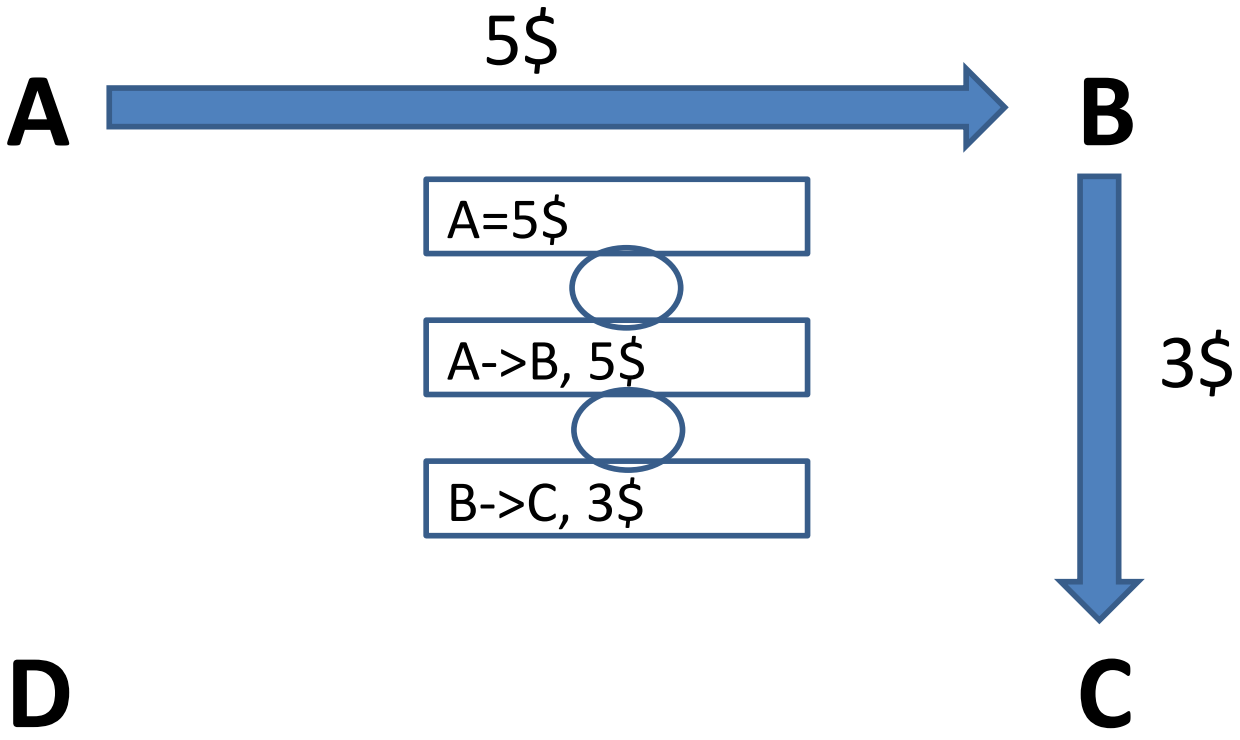
D

C

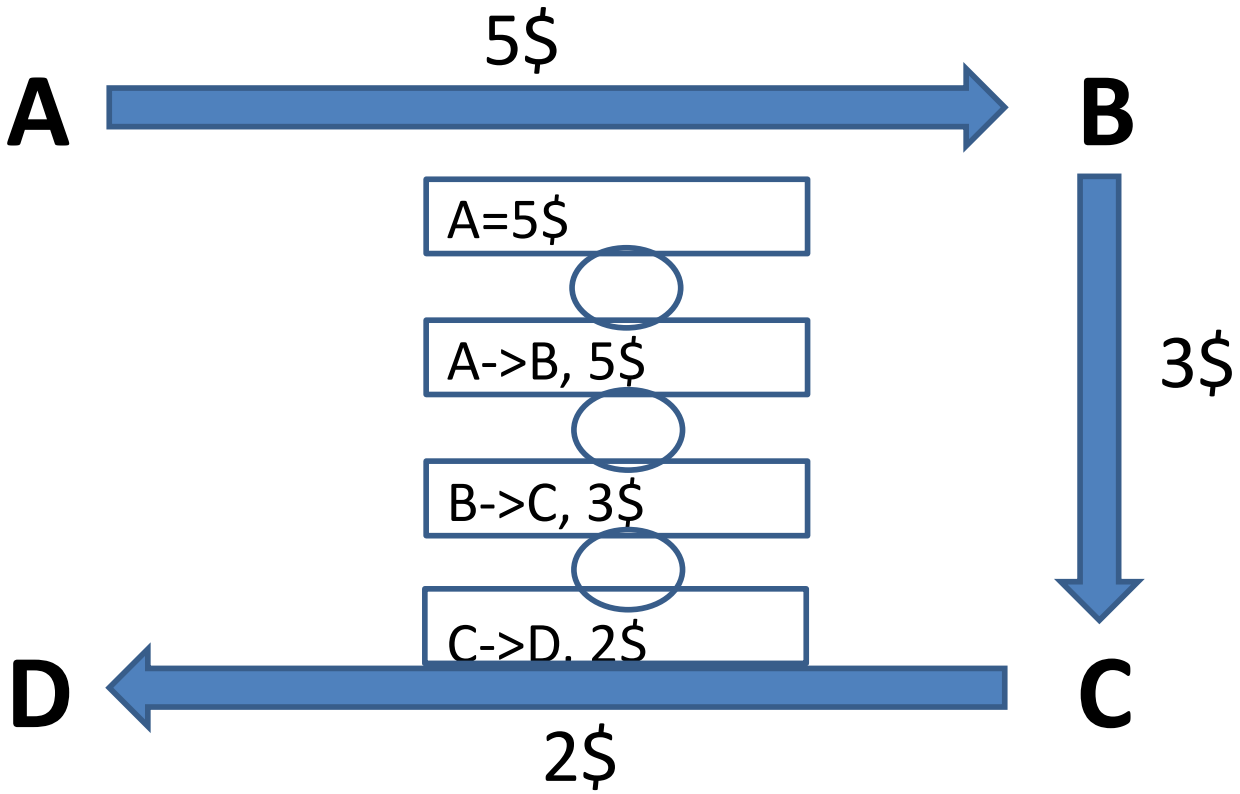
Ledger



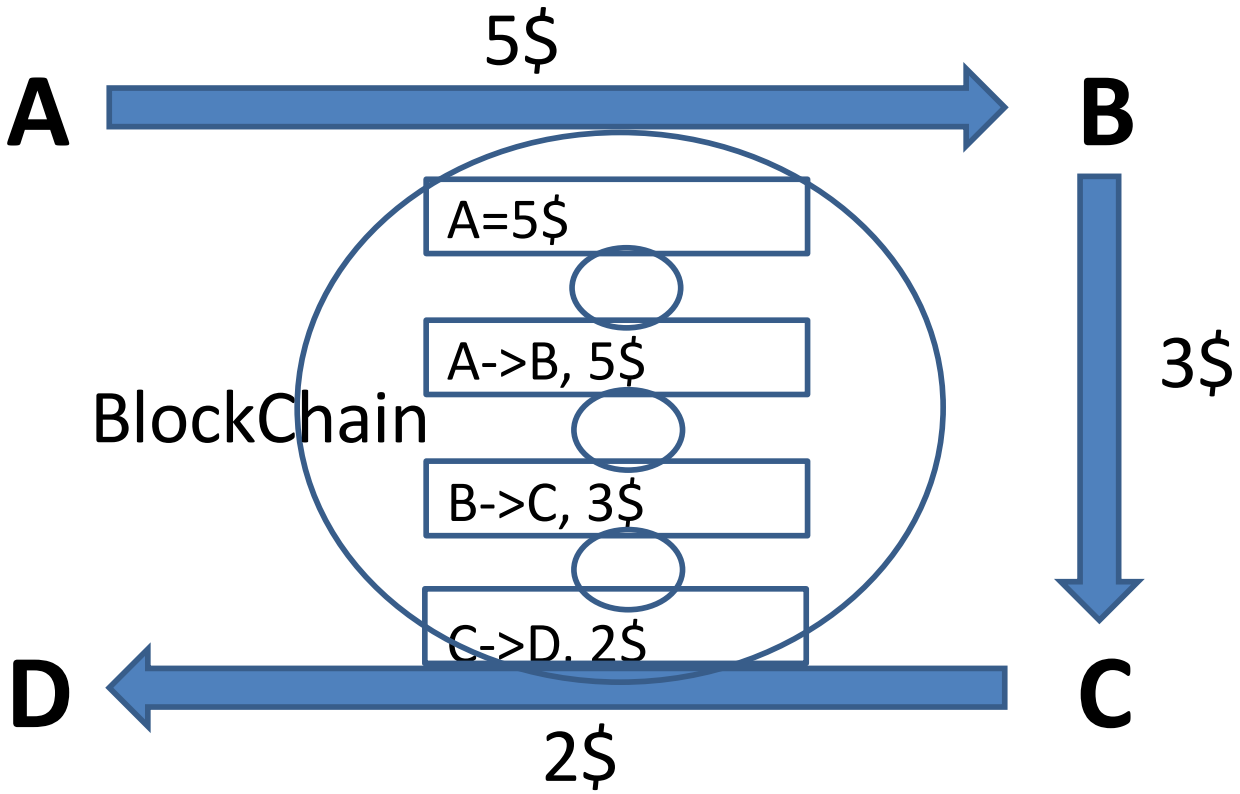
Ledger



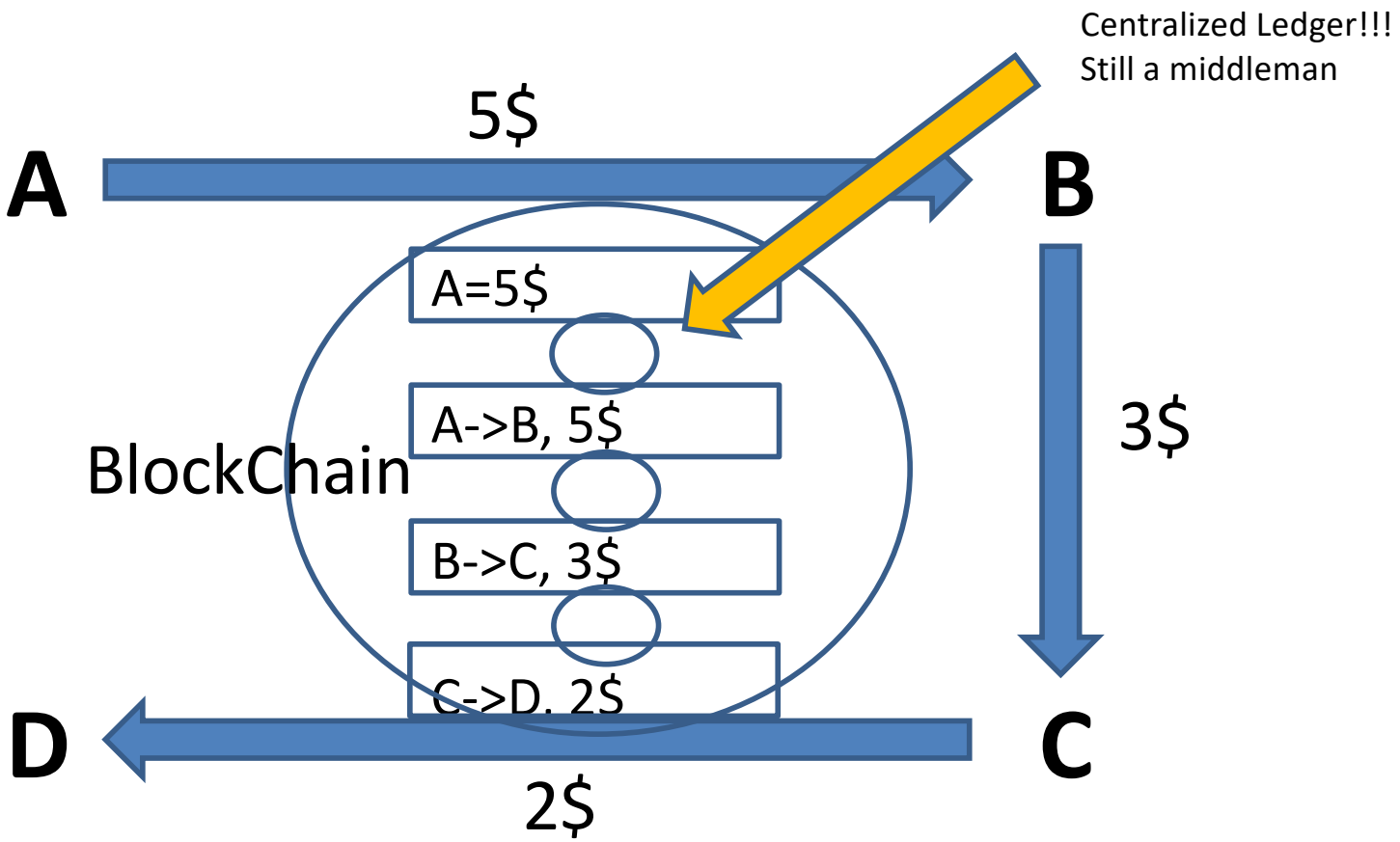
Ledger



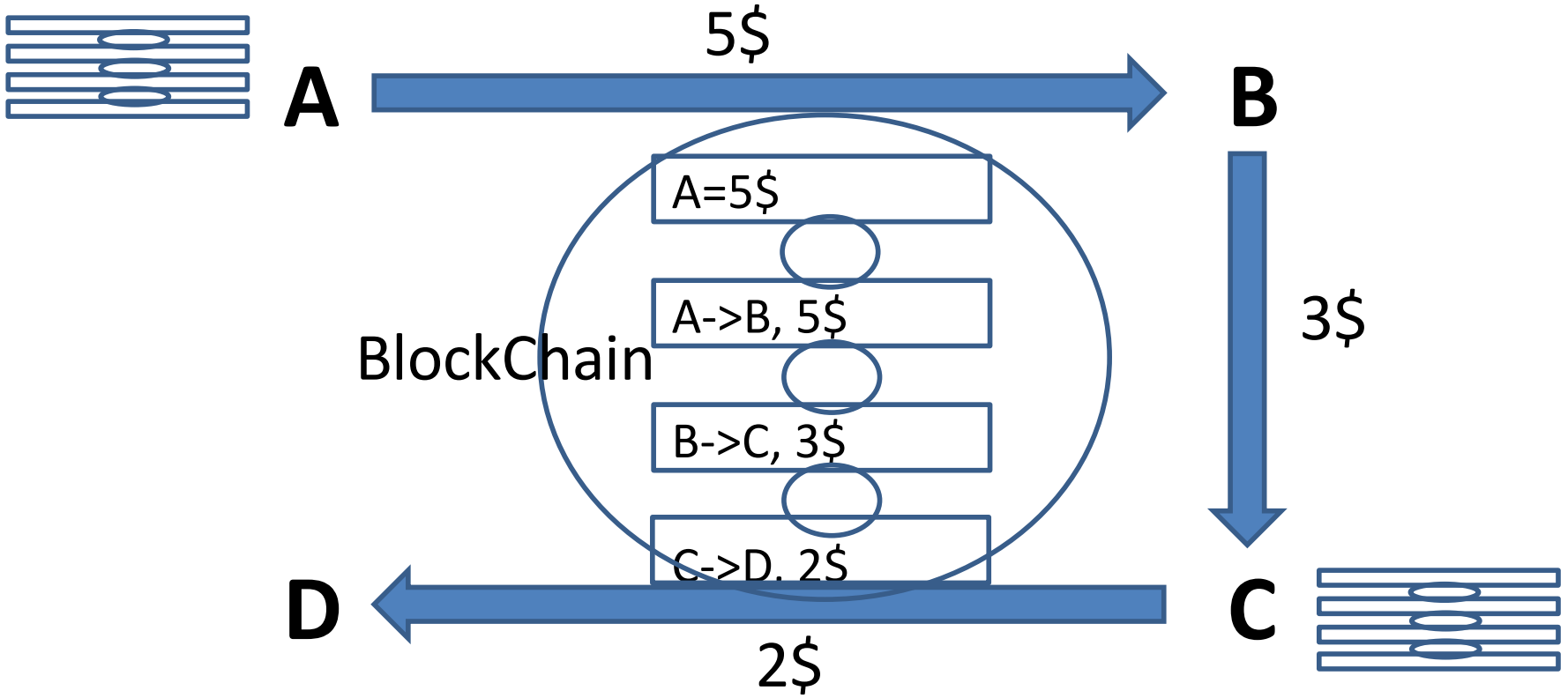
Ledger



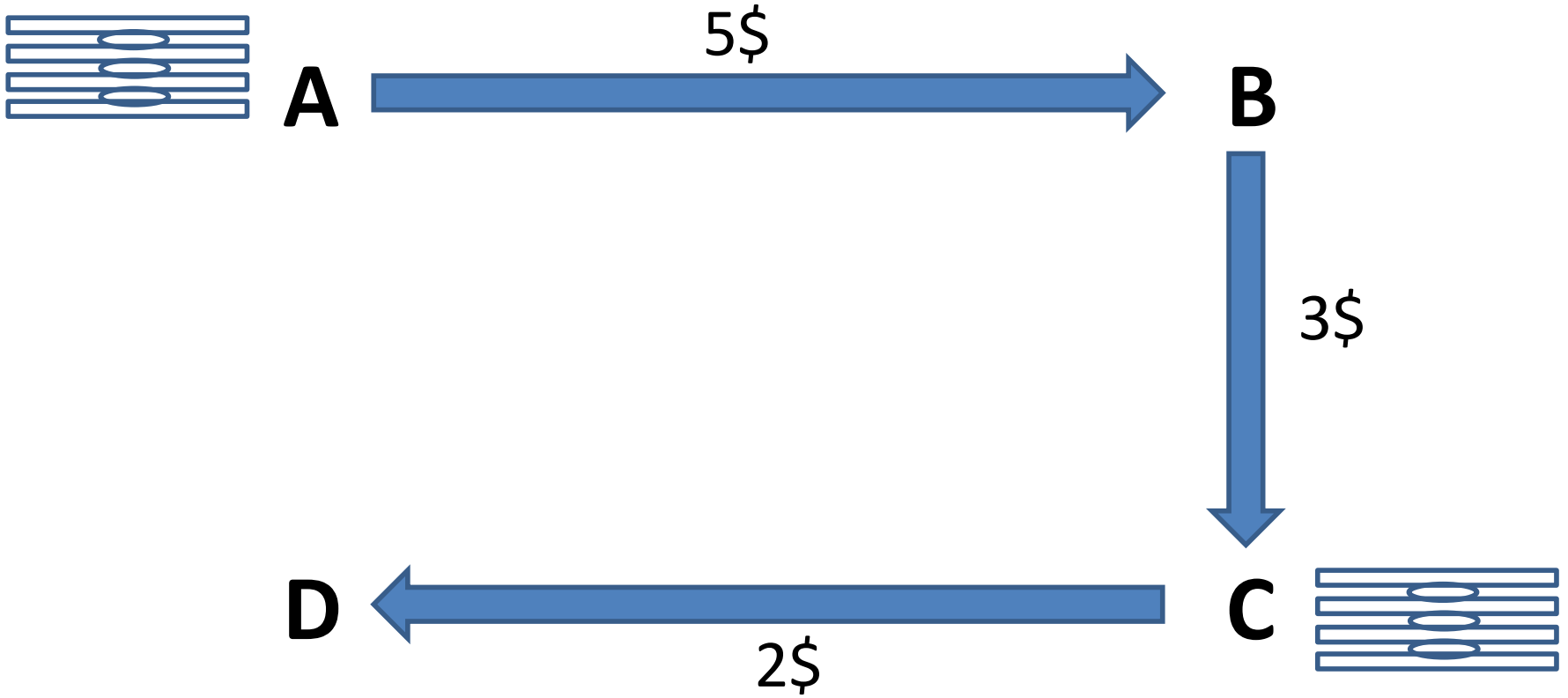
Ledger


Centralized Ledger!!!
Still a middleman
5$
A
B
A=5$
A->B, 5$
BlockChain
B->C, 3$
C->D, 2$
3$
D
C
2$

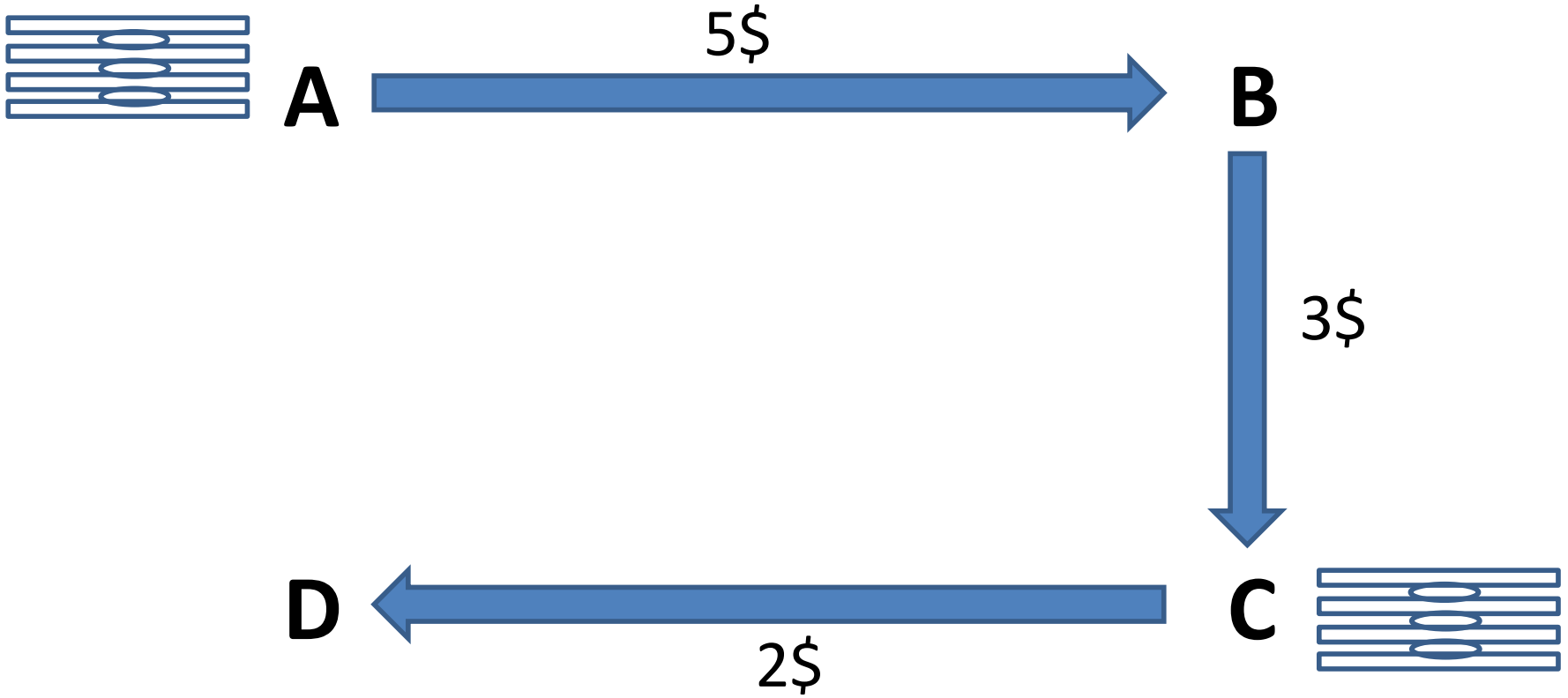
Ledger



Distributed Ledger



Distributed Ledger

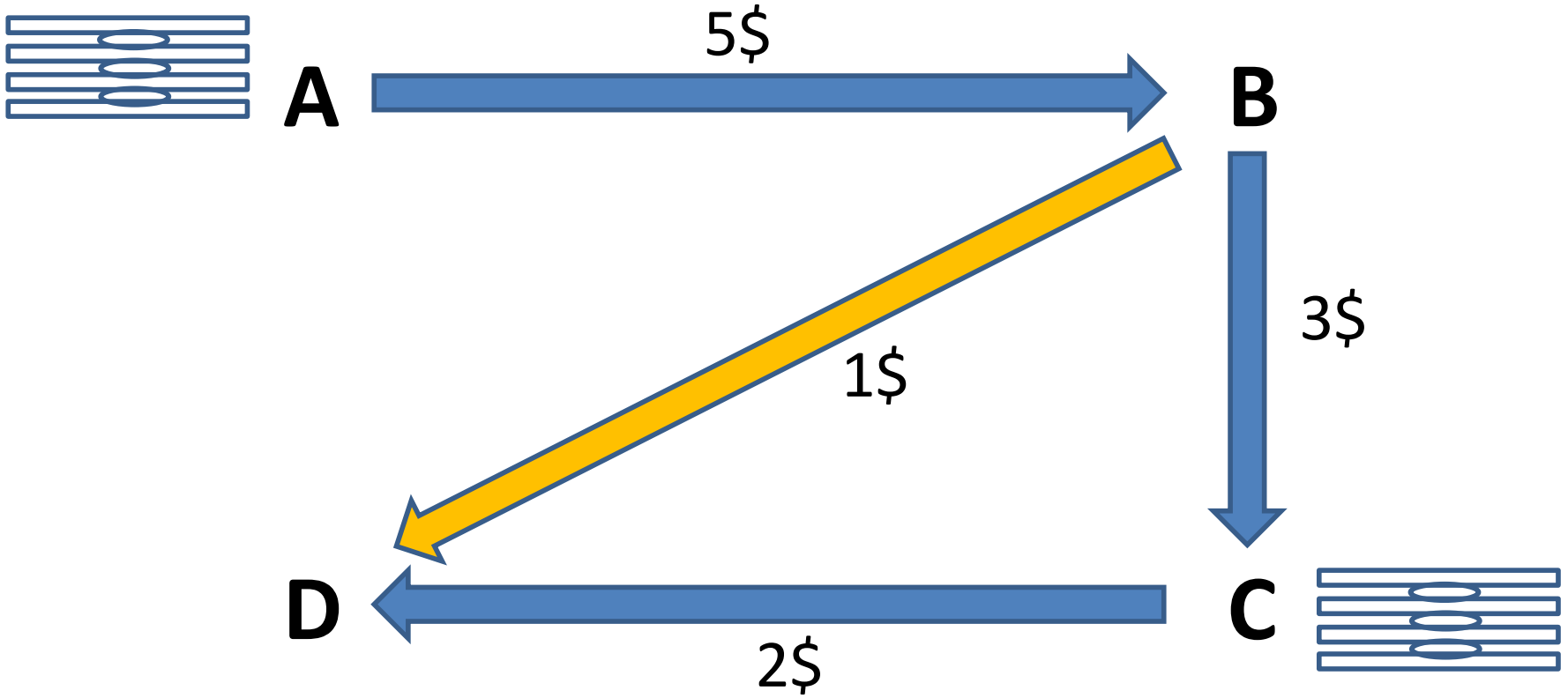


New Problems:

All copies in the network must be synchronized

All participants see the same copy of the chain

Distributed Ledger

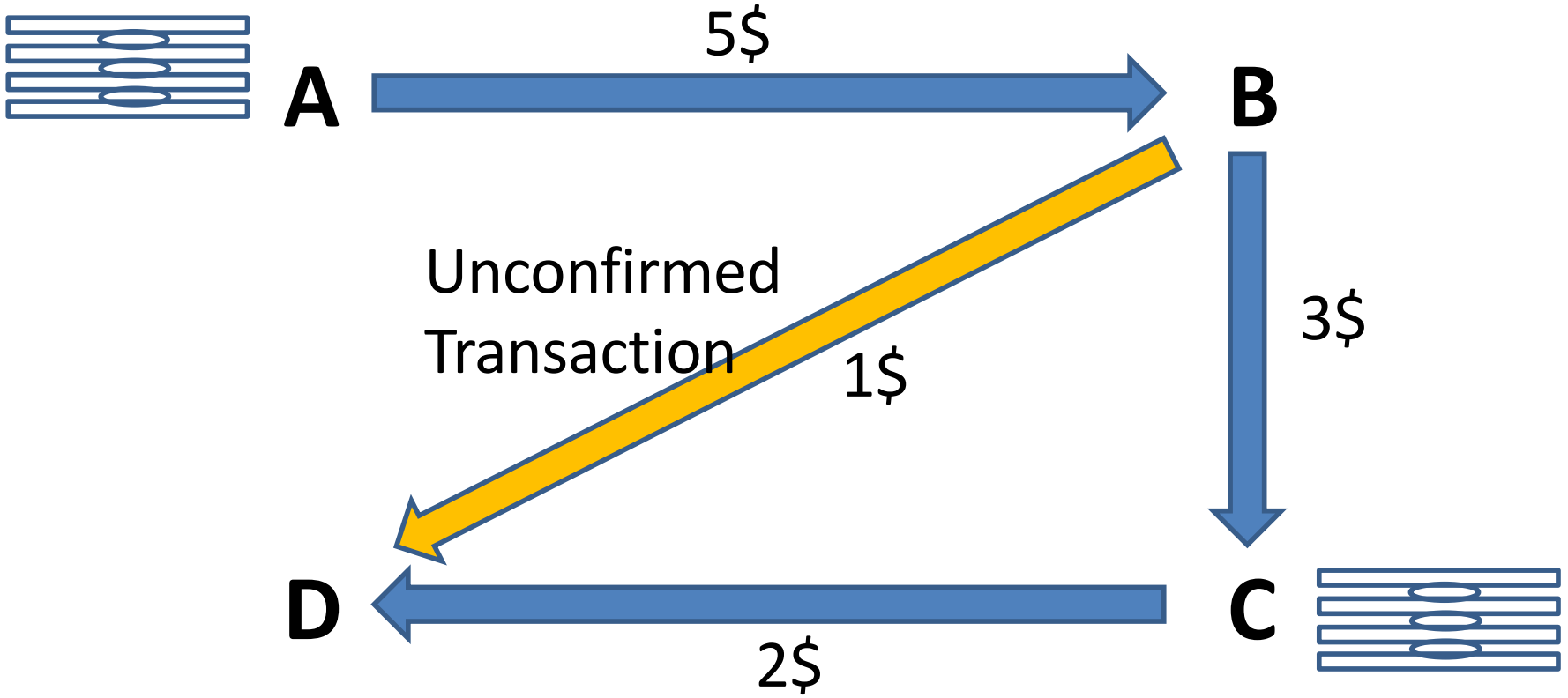


New Problems:

All copies in the network must be synchronized

All participants see the same copy of the chain

Distributed Ledger

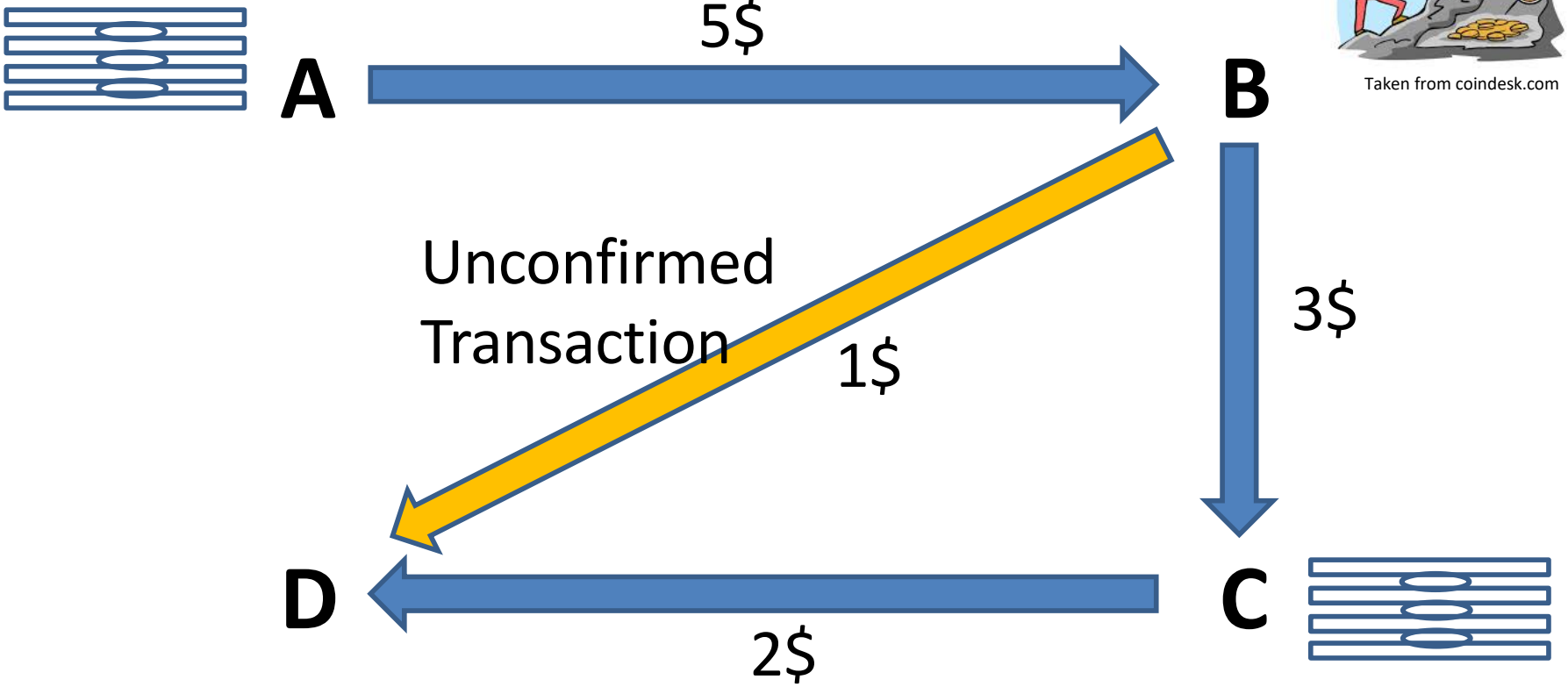


New Problems:

All copies in the network must be synchronized

All participants see the same copy of the chain

Distributed Ledger



Miners

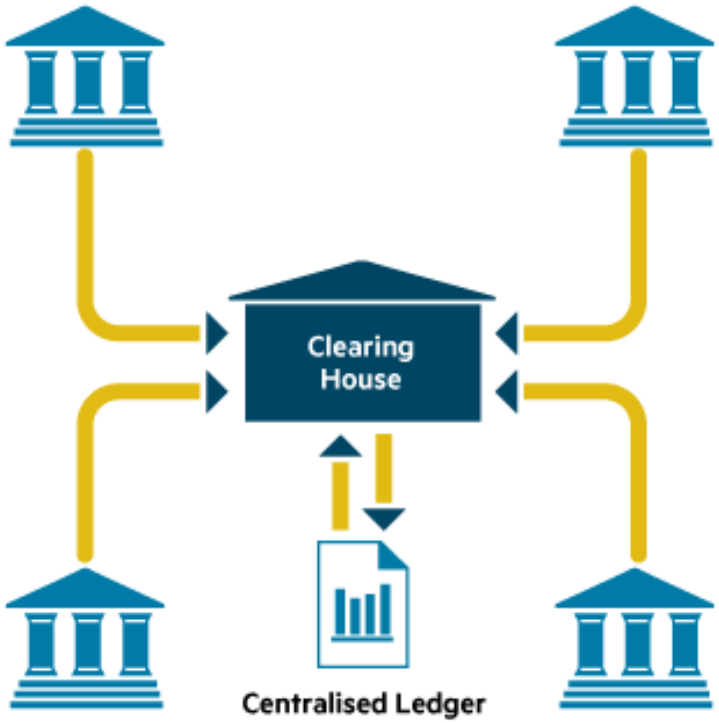
Taken from coindesk.com

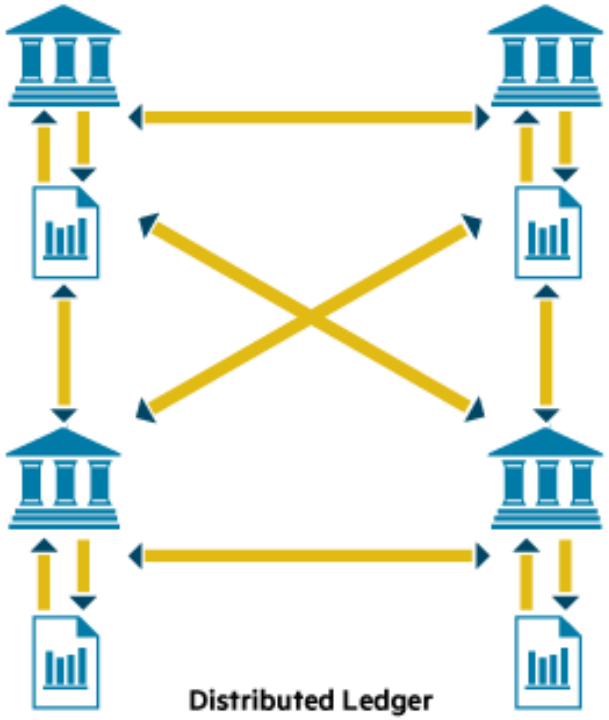
New Problems:

All copies in the network must be synchronized

All participants see the same copy of the chain

Centralized vs. Distributed Ledgers





Traditional, Centralized Ledger

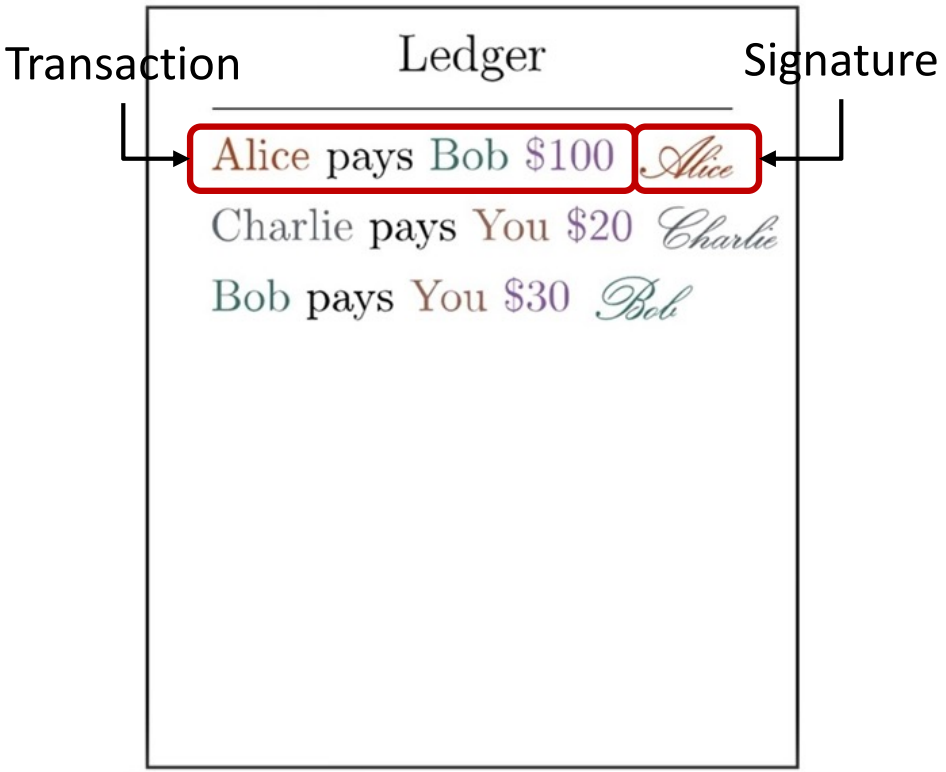
Trusted, central entity control the transactions

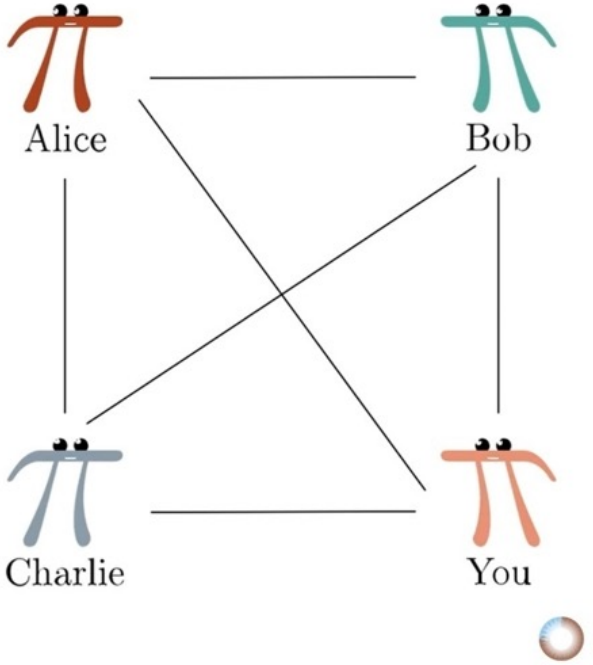
Blockchain

Every participant has its own copy of the transactions

Image Credit: Financial Times

Blockchain High Level



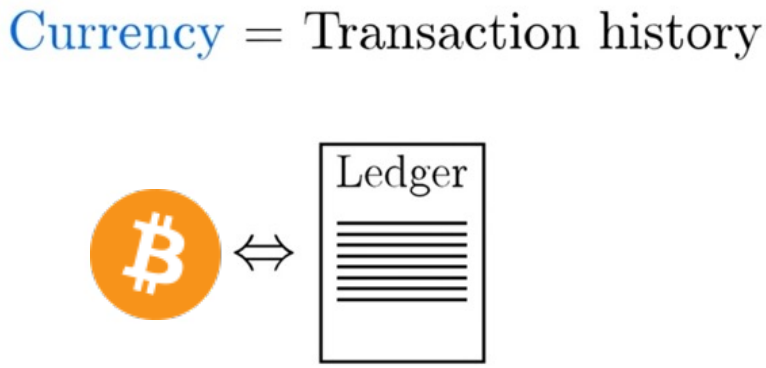


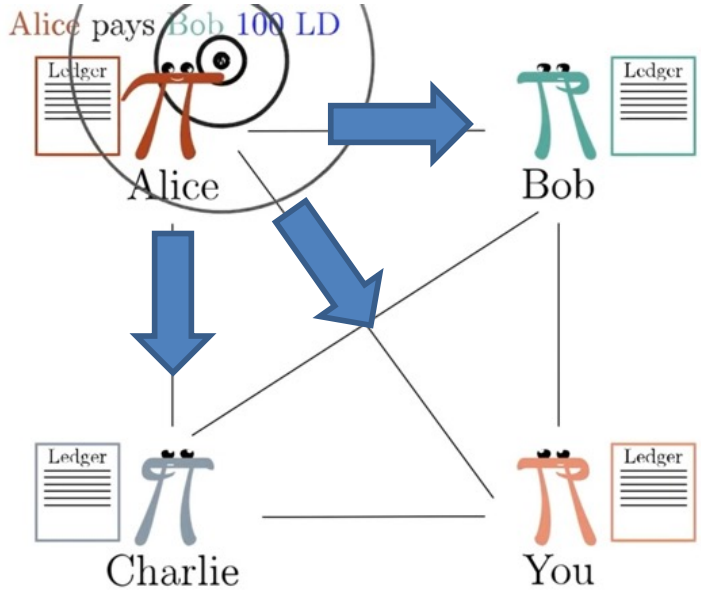
- Transactions recorded in ledger
- Signed with public/private keys

Image Credit (this slide and following): 3Blue1Brown

Blockchain High Level

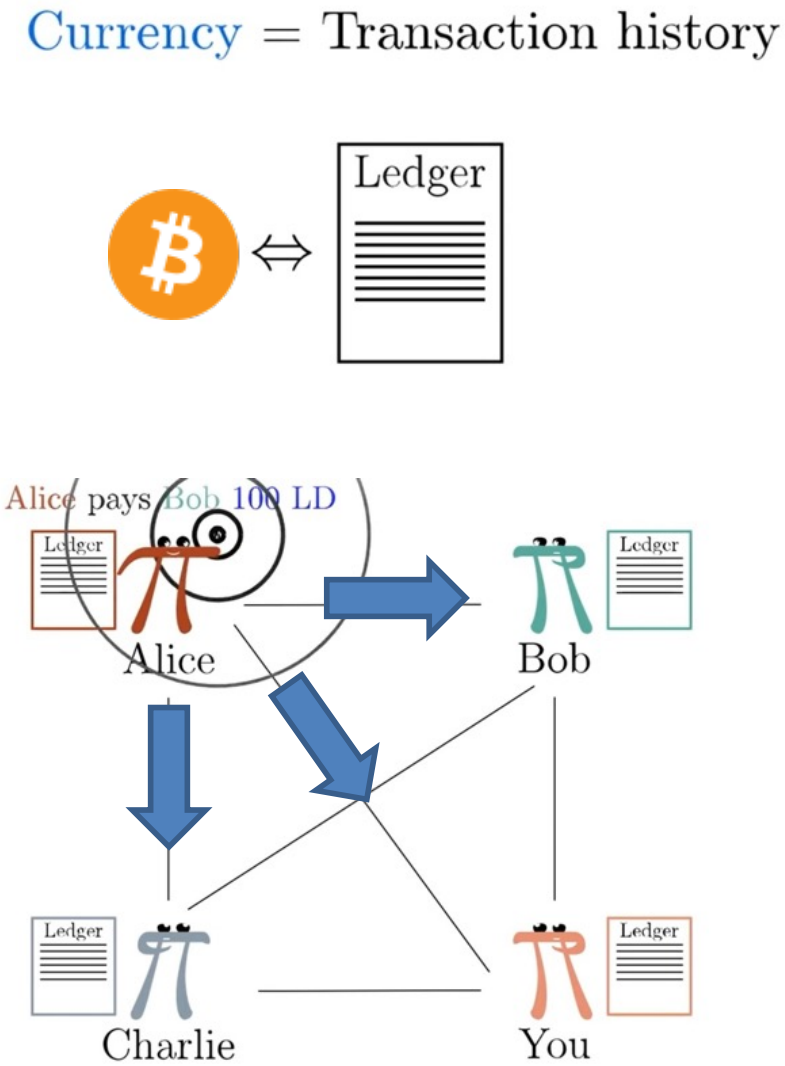
- Every node has its own copy of the ledger
- Transaction („Alice pays Bob 100 LD“)
  1. is signed by Alice,
  2. gets published by Alice
  3. is added by others to their ledgers
- Key challenges?





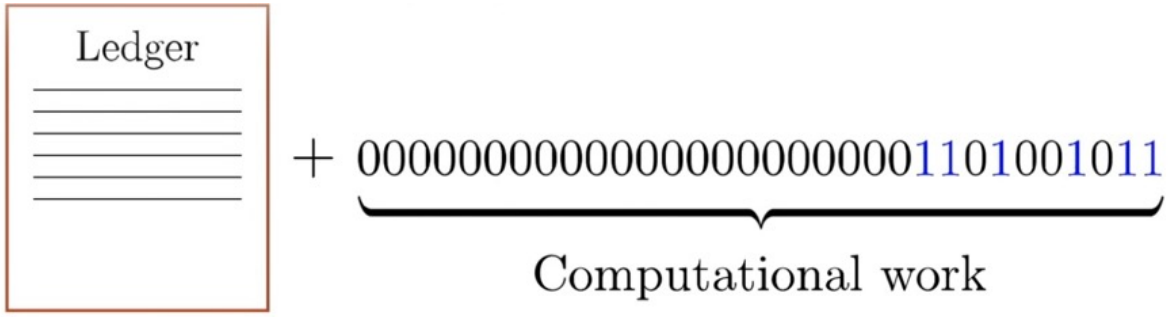
Blockchain High Level

- How can we ensure that
  1. the transactions from Alice is added by the others to their ledger (this is very important for Bob, as he received the money)?
  2. All ledgers become equal?
  3. And nobody removes / changes transactions afterwards?



Blockchain High Level

- Proof of Work
  - Ensure that ledgers are equal



- Hash chains
  - Avoid later modifications
- Main tool: Cryptographic Hash-Functions

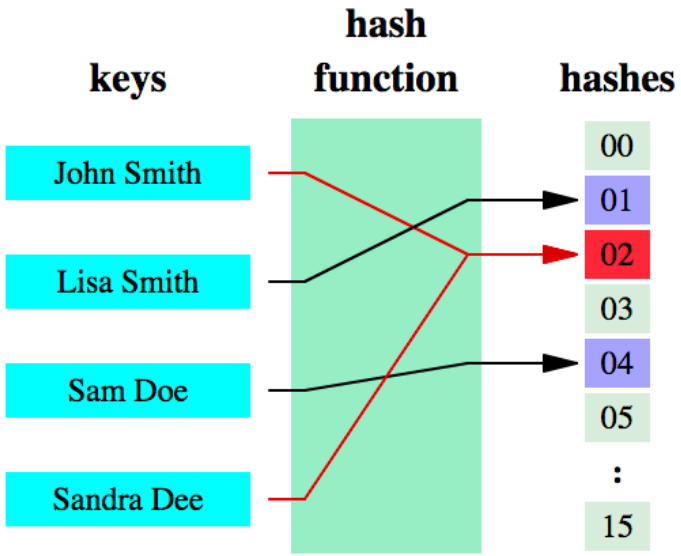
CRYPTO-PRIMER

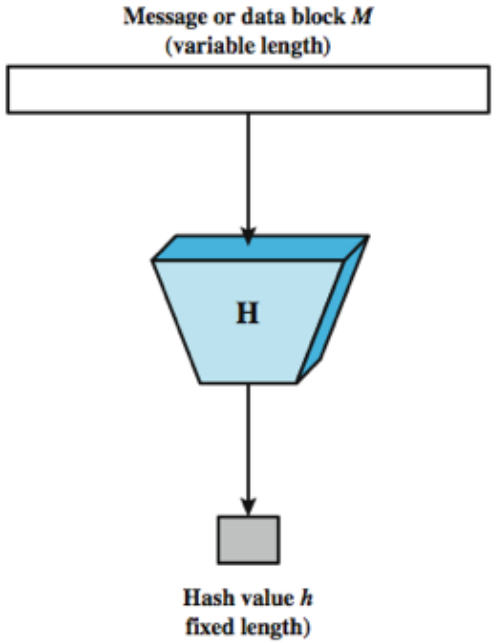
Topics

- Hash functions
- Cryptographic hash functions
- Asymmetric Cryptography

Hash functions

- What is a hash function?
  - Mapping: f(key) = hash
  - Key: variable length
  - Hash: fixed length
- What are hash functions used for?
  - Hash tables
- What is a hash table?
  - Efficient data structure





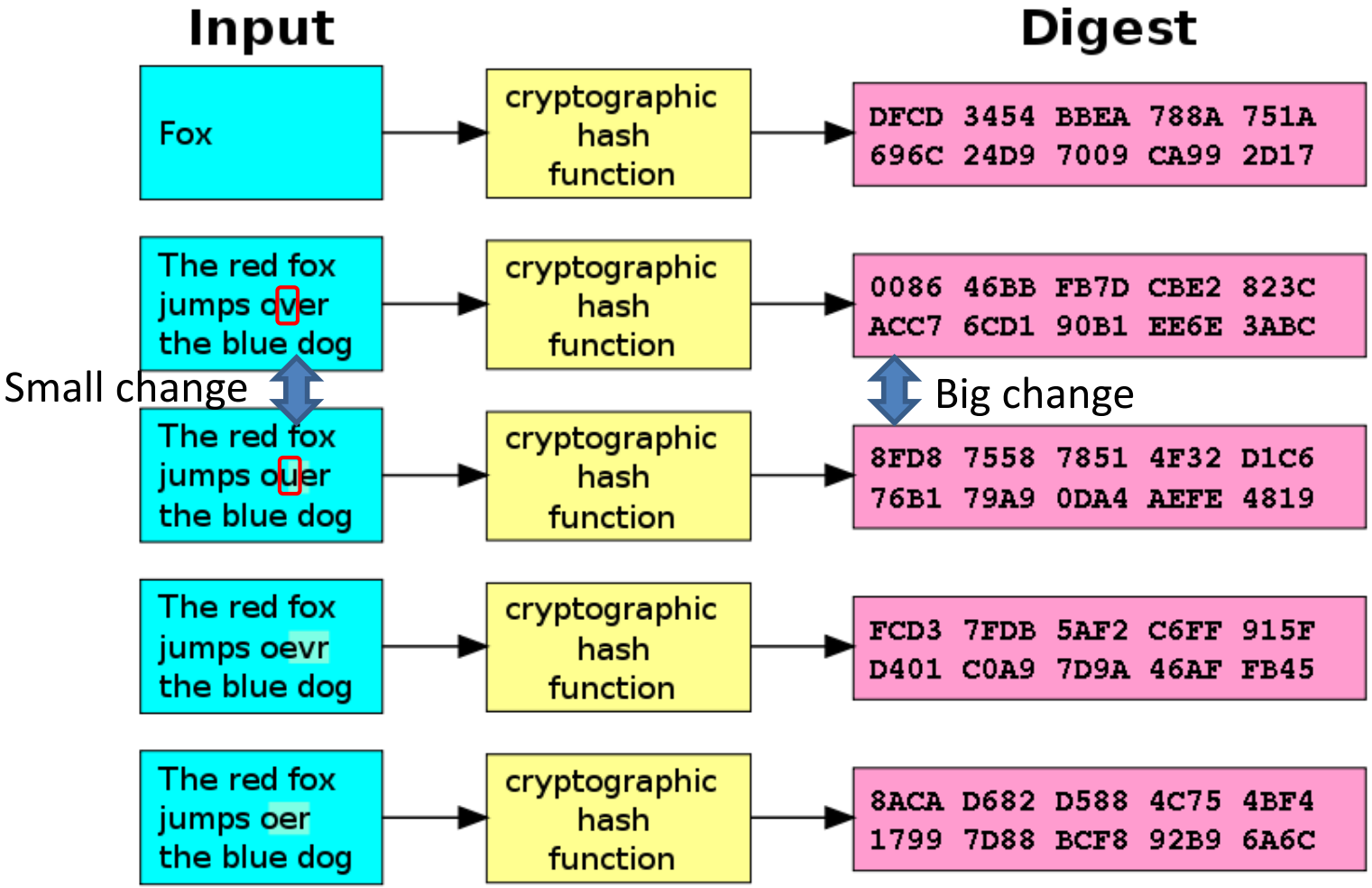
Topics

- Hash functions
- Cryptographic hash functions
- Asymmetric Cryptography

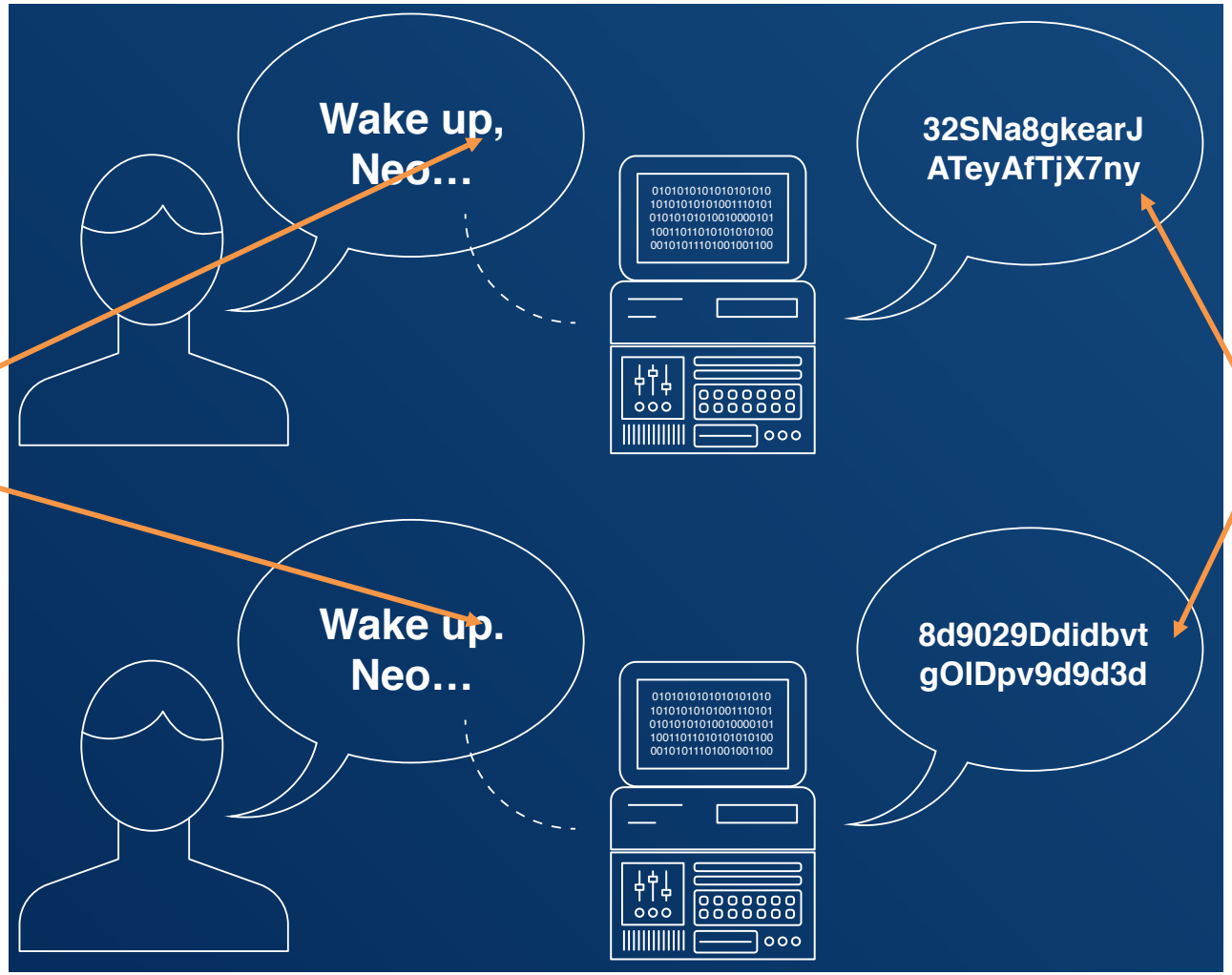
Cryptographic Hash Functions

- What are cryptographic hash functions?
  - Hash functions with specific properties
- Ideal cryptographic hash function:
  1. deterministic: same message -> same hash
  2. it is quick to compute
  3. it is infeasible to generate a message from a hash value
     - except by trying all possible messages
  4. a small change to a message
     - should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value
  5. it is infeasible to find two different messages with the same hash value (hash collisions)

Cryptographic Hash Functions



Cryptographic Hash Functions



Small change in input text

Large change in output

Cryptographic Hash Functions

- Most common cryptographic hash functions
  - MD 5 (1991): 128 bit (16 bytes) hash length
    - Today considered unsecure
  - SHA-1 (1993): 160 bits (20 bytes) hash length
    - Today considered unsecure
  - SHA-2 (2001)
    - SHA-256: 32 bytes,
    - SHA-384: 48 bytes
    - SHA-512: 64 bytes.
  - And many others including SHA-3 (2015)

Cryptographic Hash Functions

- Most common cryptographic hash functions
  - MD 5 (1991): Today considered unsecure
  - SHA-1 (1993): Today considered unsecure
  - SHA-2 (2001), many others including SHA-3 (2015)
- Why are all these „old“?
  - Give the crypto community time to try to break them
    - Use only afterwards

Topics

- Hash functions
- Cryptographic hash functions
- Asymmetric Cryptography

Asymmetric Encryption

- Encryption/Decryption
  - Encrypt with public key
  - Decrypt with private key
- Sign/Verify
  - Sign with private key
  - Verify with public key

Encryption/Decryption

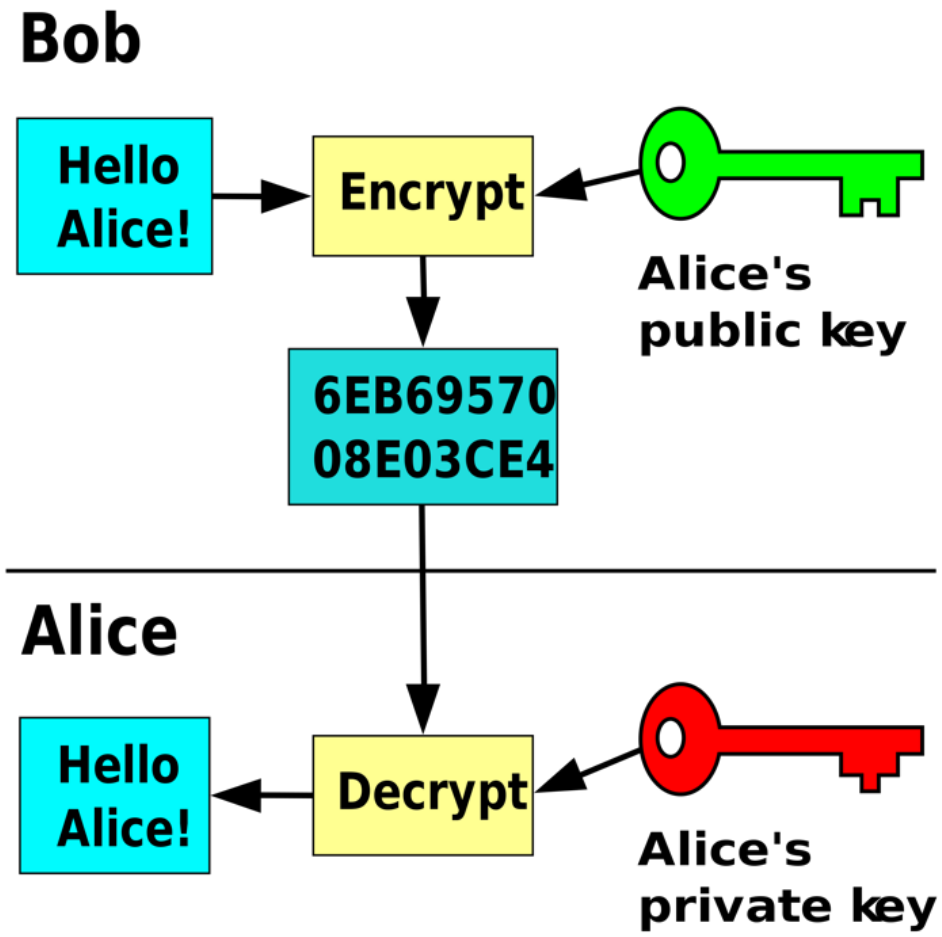


Image source: Wikipedia

Sign/Verify

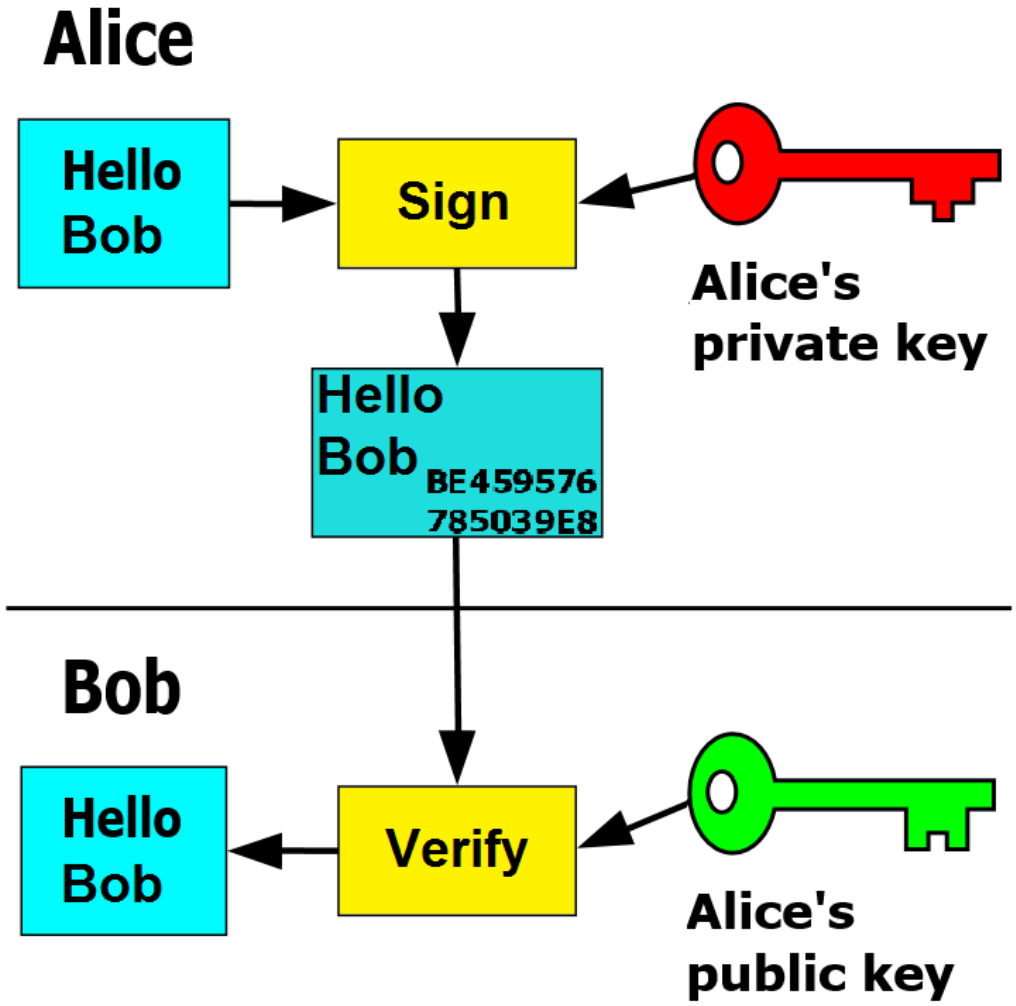


Image source: Wikipedia

Asymmetric Encryption

- Well-regarded asymmetric key techniques
  - Diffie–Hellman key exchange protocol
  - DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm
  - ElGamal
  - Various elliptic curve techniques
  - Various password-authenticated key agreement techniques
  - Paillier cryptosystem
  - RSA encryption algorithm (PKCS#1)
  - Cramer–Shoup cryptosystem
  - YAK authenticated key agreement protocol
  - …

BITCOIN

Central Principle

Give the good guys easy problems to solve…

(how should this sentence continue?)

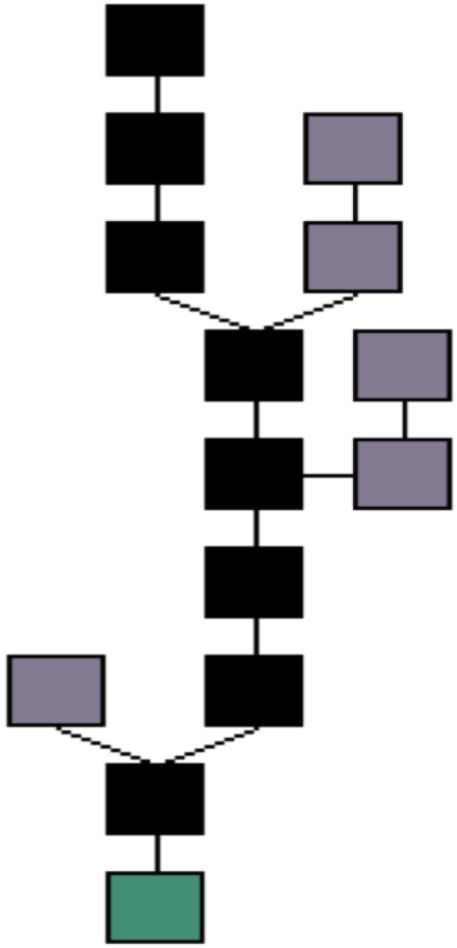
…and give the bad guys hard problems to solve.

Primitives

- SHA-256: hash
- Signatures: public / private key
- Tamper evident Merkle Trees
- Block chain
- Proof of Work

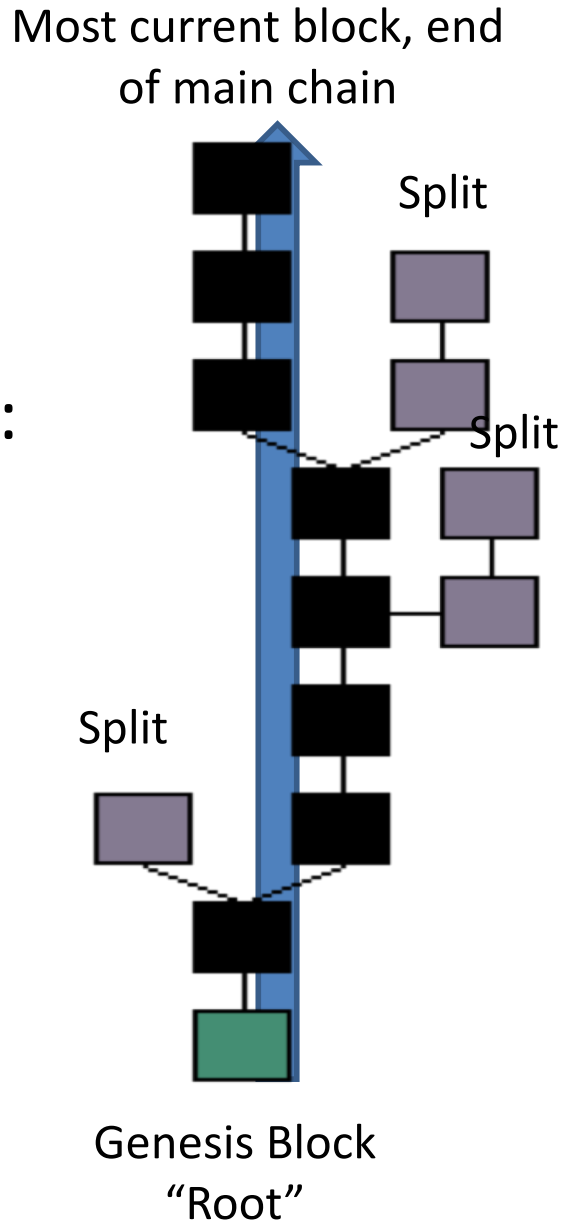
Blockchain: Concept I

- Blockchain: distributed ledger (=log)
  - time-stamped, non-repudiable (un-disputable) database
  - contains the entire history of transactions
  - Tamper proof via cryptographic primitives
- Each transaction processor
  - maintains own local copy of the blockchain
  - consensus algorithm:
    - every copy to stay in sync



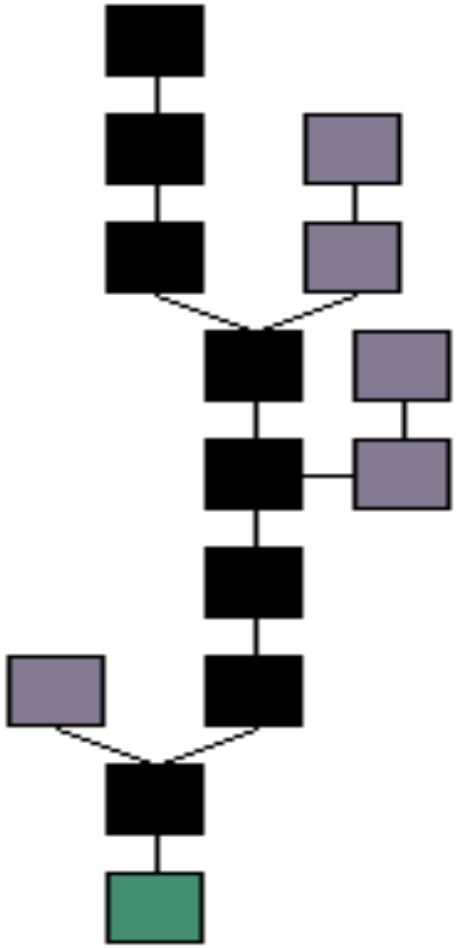
Blockchain: Concept II

- Each block
  - connected to previous one
- Each block has a hash of previous block:
  - -> blockchain
- Can/will get large
- Main chain (black)
  - Blocks from genesis block (green)
  - to the current block
- Can have splits
  - Dark grey blocks
  - Orphaned



Blockchain: Concept III

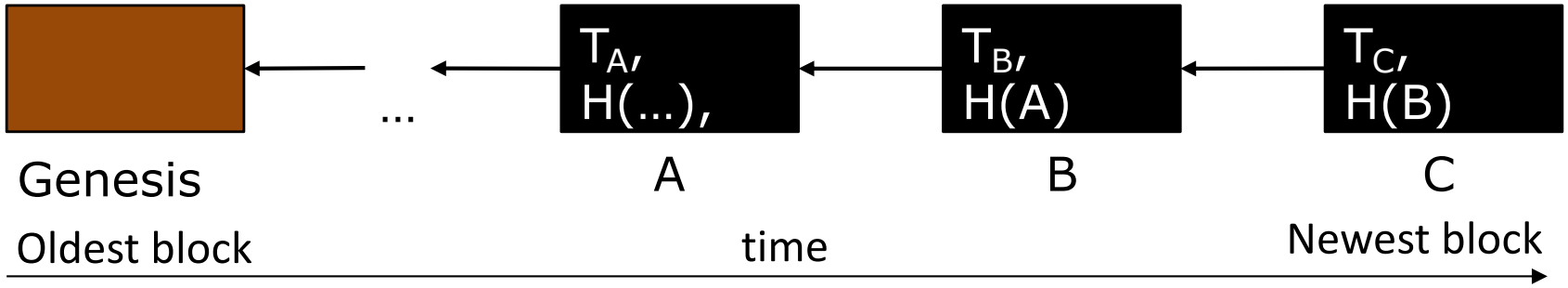
- Ensures complete transparency
  - Each transaction is visible to all
    - Participants use anonymous identifiers
- Prohibits double spending
  - No coin can be spend twice
    - As all transactions are known
    - Double spending can be detected
- Large data structure
  - Replicated on nodes in the network
  - Scaling: open research challenge



Block in the Blockchain

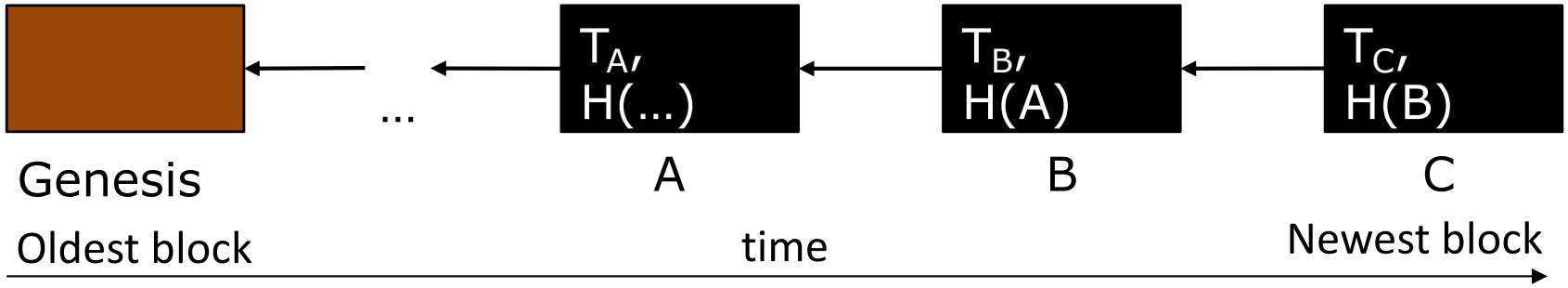
- A block is a container for a set of transactions
  - "A pays to B 10 crypto coins"$_{\text{signed by A}}$
  - "C pays to D 10 crypto coins"$_{\text{signed by C}}$
  - ….

Blockchain Details I



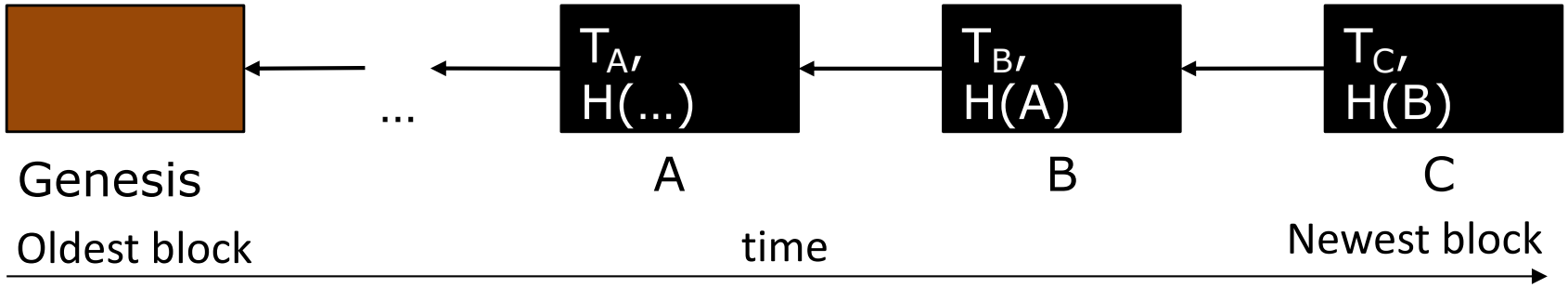
- Each block X contains
  - A set of transactions: T_X
  - Hash H_P of parent P (previous block => previous transactions)
  - And some meta data
- The genesis block has no parent
  - Bitcoin: It does have 50 bitcoins (initial money supply)
- Block identified by its hash or its height
  - Genesis has height 0

Blockchain Details II



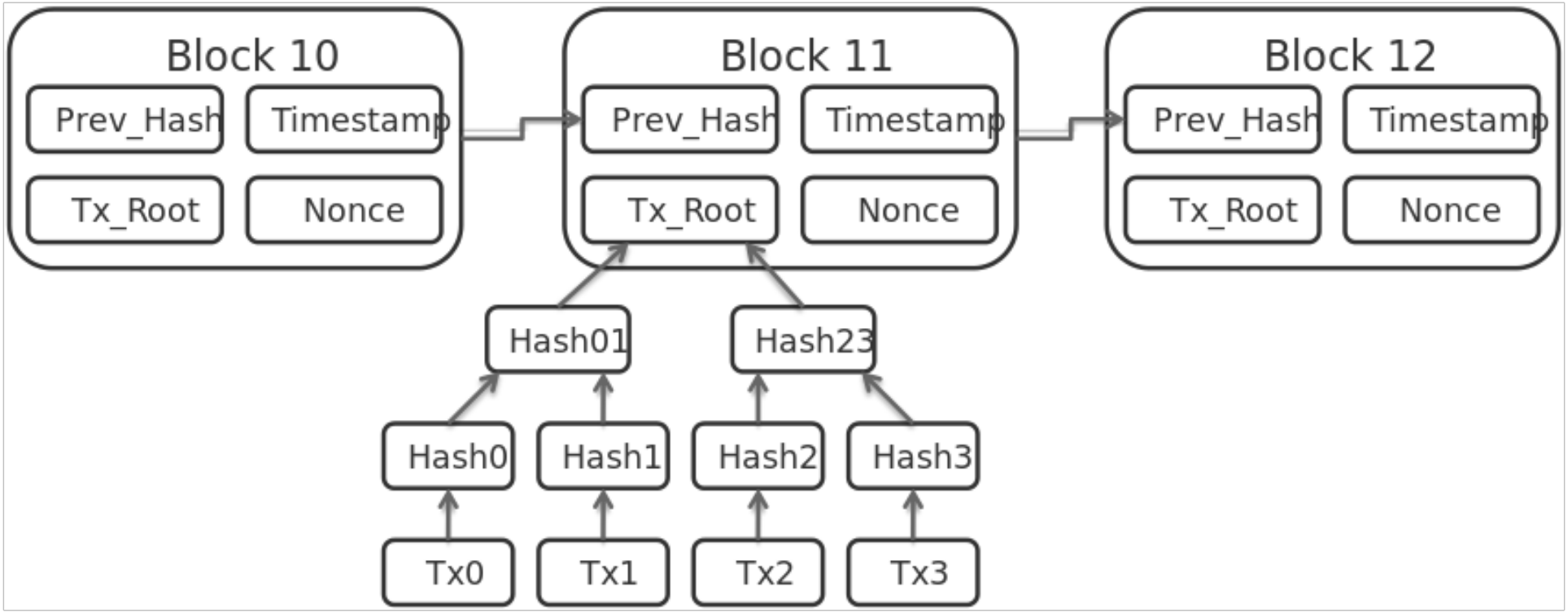
- Each block refers to its parent block:
  - Contains a hash H of the block's parent
  - The parent block is the previous block added to the chain
  - Example: B's parent is A
- Why is this tamper proof?
  - Change A forces a change to B and C
  - Proof of work needs to be recomputed too (later slides)
  - This makes later changes to transactions very hard

Blockchain Details III



- Transactions
  - A Merkle root summary of ~ 500 transactions

Blockchain Details IV



From Wikipedia

Anatomy of a Block

Block #404234

Summary	
Number Of Transactions	459
Output Total	3,812.78908631 BTC
Estimated Transaction Volume	815.7381711 BTC
Transaction Fees	0.1059914 BTC
Height	404234 (Main Chain)
Timestamp	2016-03-25 15:52:47
Received Time	2016-03-25 15:52:47
Relayed By	BitFury
Difficulty	165,496,835,118.23
Bits	403088579
Size	704.855 KB
Version	4
Nonce	311538175
Block Reward	25 BTC

Hashes	
Hash	000000000000000000221e92ec5f42f4ccf8ba7ad71020e9dcbeed3f5e484b2f8
Previous Block	000000000000000060e89871b8a2e9a769ec031ac3fc1da24d00886d5a8f256
Next Block(s)	000000000000000005687e47a1fa3936b3c7eca894920b30d4904f42faa1df75
Merkle Root	3bef11b868b850a27ca176d8c4a5fb465f71771f9b46ba272dbf6f53d4e1550b

Network Propagation (Click To View)

(from blockchain.info, a great resource for bitcoin info)

Transactions

- Many transactions live in the block's Merkle tree.
  - You do not spend from an account. You spend from previous transactions.
- Transaction
  - Input address
    - points to the output of an earlier transaction
  - Output address
  - Signed by owner of funds

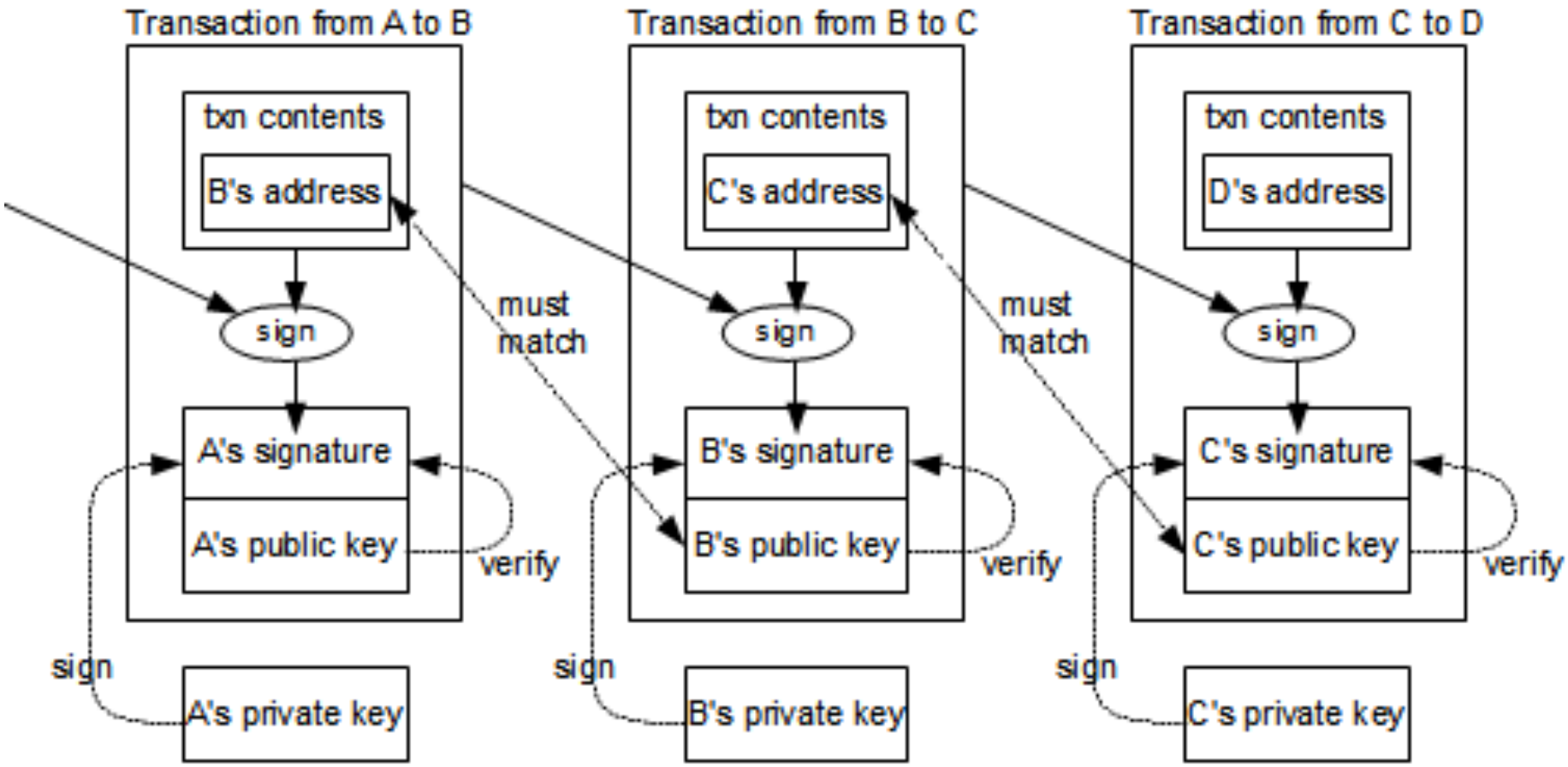
Transactions

- Transactions are between pseudonyms
  - hash of public keys
- Pseudonyms
  - Not anonymous
  - But also not connected to an identidy
  - You can reveal your public key to others
    - So that they can send money to you

Transactions

- Enough addresses
  - 2^160 possible addresses
  - 2^63 grains of sand on earth
  - 2^160 / 2^63 = 2^97
    - For each grain of sand, we have 2^97 addresses.
  - Compare: IPv6 128 bit addresses, here 160 bits

Transactions



Block Transactions

Transactions

4d0452c4fe98178875ede72319ca3162389edd43a22690ebcd49938bbcffd37c			2016-03-25 15:52:47
No Inputs (Newly Generated Coins)		1DrK44np3gMKuvc... (Bitfury)	25.1059914 BTC
			25.1059914 BTC
ed93695feee71a0d115d84e3bfbd759eebc03c3f707b9fdfec6fed3514d204ec			2016-03-25 15:51:26
1BJaAgMK9F31HpTB8yePe69zEqR6cTg9eS		1Lie2o1tAjKxHgRMkFVmJZUMgFbsjummks	1.1269325 BTC
			1.1269325 BTC
53cd4fbc48378eb686873f0f8b1d5cc34dfd0099bcc4cfb46069649fb18fe0e7			2016-03-25 15:51:55
17wLMV3wgDFCn4LQxQsDLrD6KvvVMZSuBi		15PUBY3omSex2kkBNBfEwextZvhRWYevNA 17zLoiL1EEdHkgdpNuagG1vq7Fa6UMyK2h	8.7 BTC 3.37028336 BTC
			12.07028336 BTC

Until now

- Motivation
- Crypto Primitives
- Block chain
- Transactions

- Next
  - Consensus
  - Proof of Work

Questions

- Blockchain is the same as Bitcoin.
- Each block of a Blockchain consists of which of the following?
- In blockchain, blocks are linked…
- A block in the blockchain can never have more than one parent block?
- Blockchain forks can result in which of the following
- Blockchain forks can result in which of the following
- Where is the central server located that is required to store all bitcoin transaction?

https://olafland.survey.fm/blockchain-i

CONSENSUS

Transactions Version 1

- Alice signs a message and sends it to Bob
  - `A -> B {A gives B 1 BC}`K_{APriv}
  - Private key of Alice: K_{APriv}
- Positive:
  - Alice shows intent
  - Alice cannot send a payment signed by Carol. Alice does not know Carol's private key K_{CPriv}
- Problem:
  - Not safe against replays from Alice: Does Bob now have several coins or 1?
  - Bob could make 5 copies. How many coins does he have now?

Transactions Version 2

- Alice signs a message and a unique serial number
  - Alice sends it to Bob
  - A -> B {A gives B 1 BC, 123990245}K_{APriv}
- Positive:
  - Alice shows intent
  - Replay not of concern with Bob
- Problem:
  - How does he know she has the money to spend?
  - She can double spend with Charlie
    - A -> C {A gives C 1 BC, 123990245}K_{APriv}
  - Where do we get all these unique serial numbers?

Transactions V2 With a Bank

- Alice gets a unique serial number from the bank
  - Alice signs a message and the serial number and sends it to Bob
  - `A -> B  {A gives B 1 BC, 123990245}K`$_{\text{APriv}}$
- The bank maintains a ledger of who owns what
  - Bob checks with the bank before providing service to Alice
  - Does Alice have this to spend?
- Positive:
  - No replays – everyone checks with the bank before accepting
  - No double spending: Transaction to C would fail verification with bank
    - `A -> C  {A gives C 1 BC, 123990245}K`$_{\text{APriv}}$
- Problem:
  - Centralized model

Transaction Version 3 No bank – the community keeps track

- Alice signs a message with a unique serial number
  - and sends it to Bob
  - A -> B {A gives B 1 BC, 123990245}K_{APriv}
- Bob verifies – he checks his copy of the ledger
  - Does Alice own the bitcoin?
  - Bob accepts and Bob tells everyone about the transaction
  - Everyone updates their own copy of the ledger
- Positive
  - Decentralized model
- Problem
  - Alice may double spend with Charlie
  - How do the others fix and keep up-to-date their ledgers?

Version 4 Everyone Verifies

- Alice signs a message with a unique serial number
  - and sends it to Bob
  - `A -> B  {A gives B 1 BC, 123990245}`K_{APriv}
- Bob asks everyone to verify
  - If enough verifications
    - Bob provides service
    - and asks everyone to update their copy of the ledger
- Positive
  - Double spending will normally be detected
  - Decentralized model
- Problem
  - Sybil Attack possible and allows the double spend.
  - How: Alice starts many entities, each can cast one vote
    - Alice votes: sure, money has not been spend
      - But already spent it

Detour Sybil attacks

- Scenario
  - Collect votes from all participants
  - As in Bitcoin
- Sybil attacks
  - What if one entities pretends to be thousands of entities
    - And thereby gets thousands of votes?
- Problem
  - Sybil Attack possible and allows the double spend.
  - How: Alice starts many entities, each can cast one vote
    - Alice votes: sure, money has not been spend
      - But already spent it

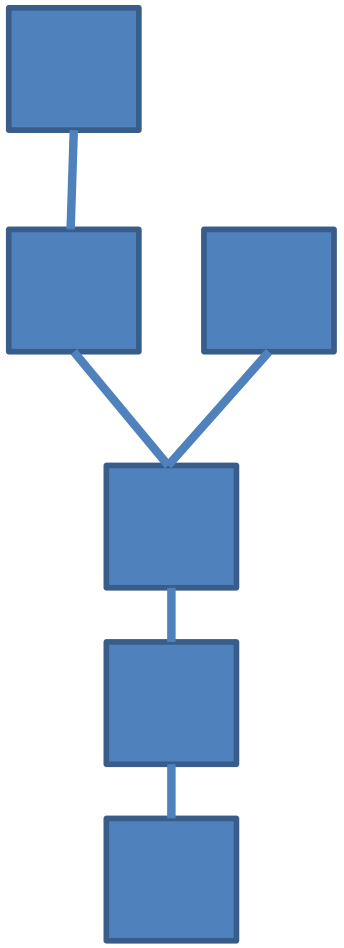
PROOF OF WORK

Proof of Work

- Goal:
  - Avoid Sybil attacks
  - Verify transactions of others
  - Identify double spending
  - Make changes to blockchain (practically) infeasible

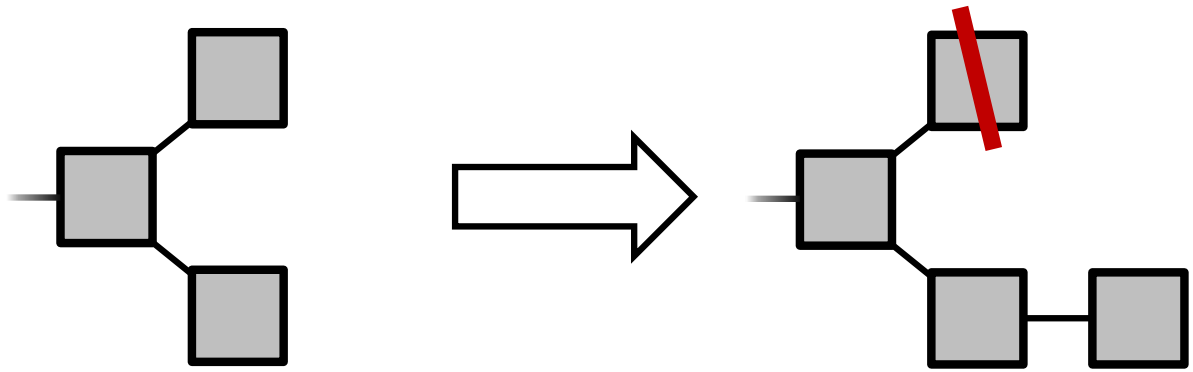
Consensus

- Do some transactions
  - Make a block, link to previous block
  - Share in the network
- Others do the same
  - Also link to previous block
- -> “Competing” blocks
  - Can only continue on one chain
    - Majority wins (and the larger one wins)



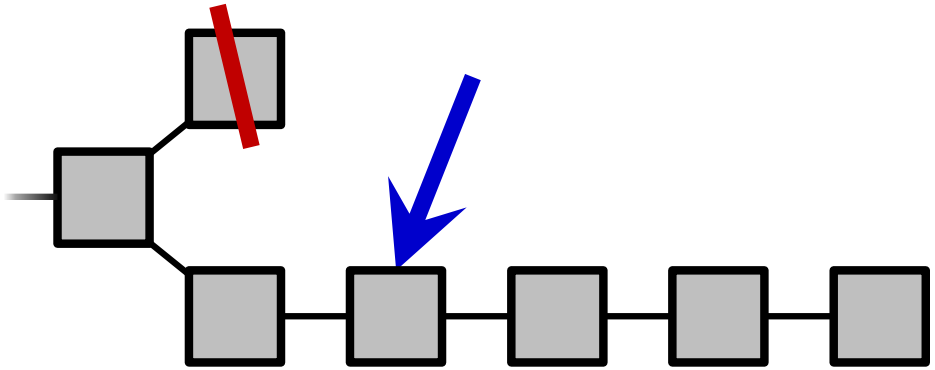
Root

Fork Resolution



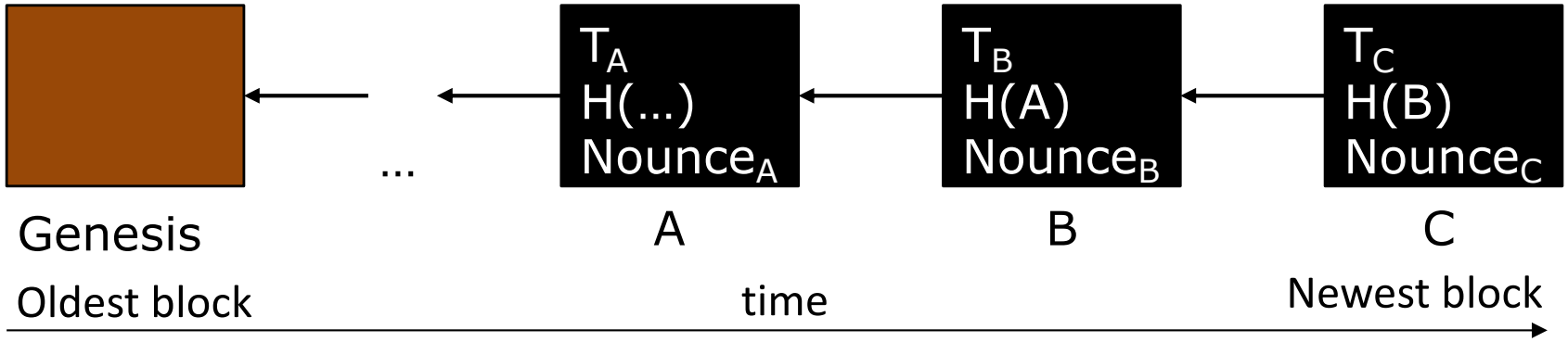
- **Longest** chain wins
- Transactions are reverted
- Double-spending a threat

Fork Resolution



A transaction is **confirmed** when
it is **buried** deep enough

Proof of Work



- Select Random Nounces until
  - Hash of block is less than target
  - Target: value known to all participants
  - Example:
    - Find Hash less 9999999 (easier)
    - Find Hash less 99 (harder)

Proof Of Work: Idea

- Consider a difficulty of 2:

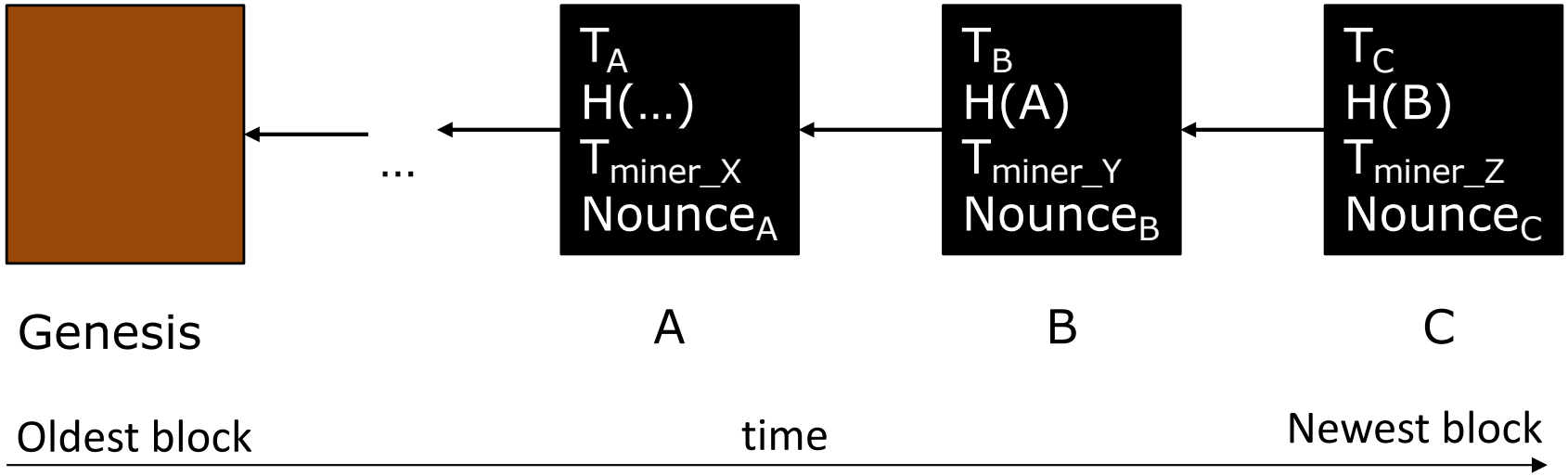
```
int i = 0;
h = SHA-256(someData + i);
while(two leftmost hex digits of h are not 00) {
    i = i + 1;
    h = SHA-256(someData + i);
}
```

- How any times will this loop execute?
  - Prob(”00”) = 1/16 * 1/16 = 1/256. 256 trials expected.
  - Hard to compute prooof of work but easy to verify.
- The difficulty can change. We can force this to take 2 weeks on average.
  - If computers become faster we can increase the difficulty

Version 5 Everyone Verifies with POW

- Introduce verifiers
- Alice signs a message and a serial number and sends it to everyone
  - `A -> All {A gives B 1 BC, 123990245}`K_{APriv}
  - The transactions are collected by each verifier
  - Verifiers maintain a queue of pending transactions.
- To verify:
  - (1) Check ledger for double spend
  - (2) Perform POW (solve a puzzle)
  - (3) Announce block is verified
- The first to do so, gets a share in the transaction
  - It is easy for others to check this result against the blockchain and check the POW.
  - Alice will likely not be the first to verify.
  - POW makes a Sybil attack very expensive.

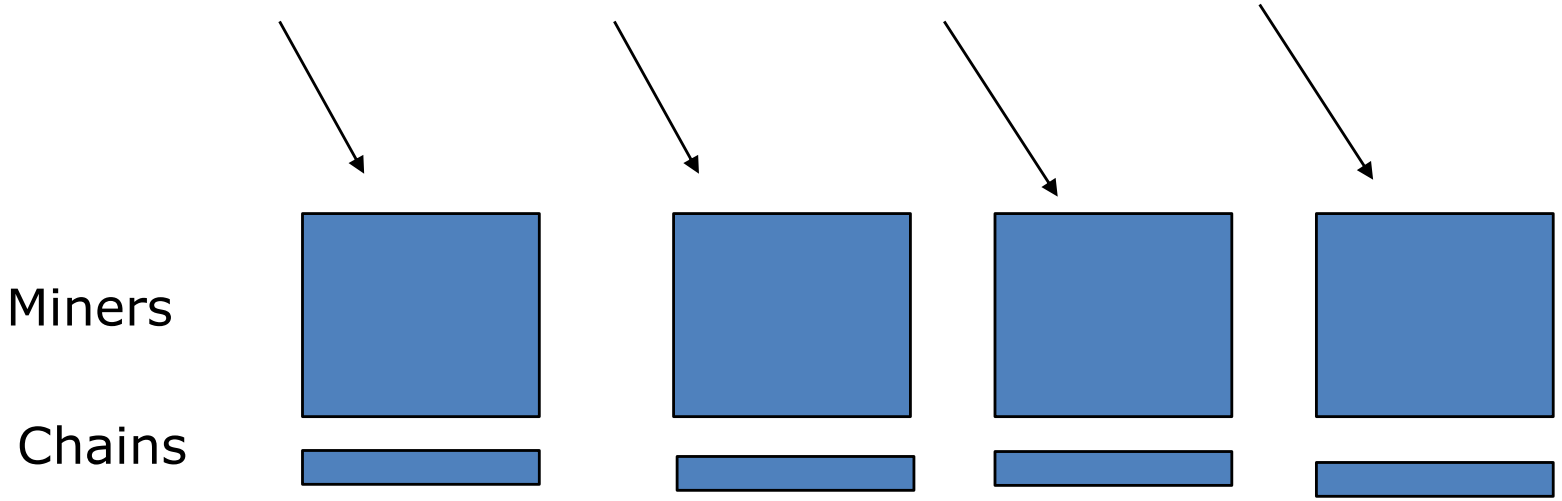
How are the miners paid?



- Transaction fee
- Stored in the block
  - Transaction to the miner itself

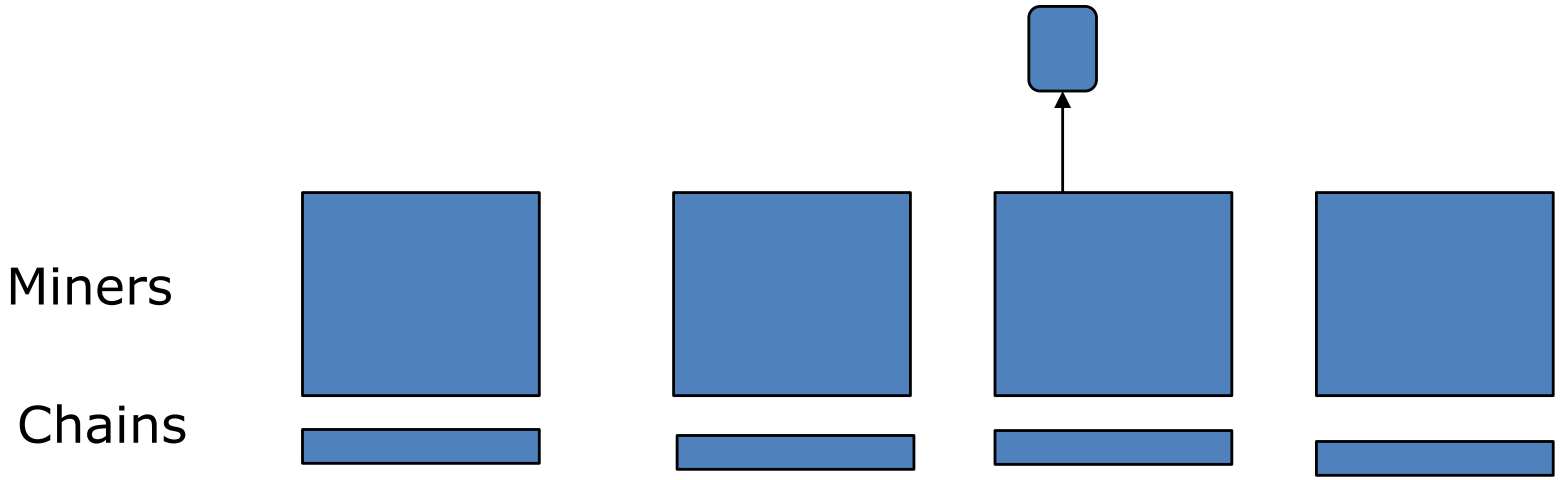
Try to double spend

- A -> All {A gives B 1 BC, 123990245}K_{APriv}
- A -> All {A gives C 1 BC, 123990245}K_{APriv}



Suppose both transactions are placed on the peer to peer network.
Miners verify each transaction and then collect the pending transactions into blocks.
An honest miner will not include inconsistent payments in their block.
-> One of these double spend transactions will be rejected.

Try to double spend



After about 10 minutes, some miner produces a block. This miner won the race.
Other miners receive the new block and verify transactions and the proof of work.
It is easy to verify the proof of work and all transactions in the block.
If the block passes all checks, it is added to the blockchain.
Unless she controls a lot of nodes, Alice cannot predict the winner
of the race to solve POW.

Fraud prevention

- Users can trust the block chain that was most difficult to produce
  - longest chain wins
- If there was a "fake" blockchain competing with the real ones the fraudster would have to do as much work as the rest of the network to make their block chain look as trustworthy
  - intense work that goes into finding blocks through hashing secures the network against fraud

Proof of Work

- Problems
  - Energy intensive
  - Sensitive threshold
    - One participant with more than 50% of the computer power
  - Only probabilistic protection
    - With sufficient resources a participant could buy sufficient computer power to cross 50% threshold

Bitcoin Security

- An attacker with > 50% of hash power can
  - Double spend: Reverse transactions that he sends while he's in control
  - Prevent some or all transactions from gaining any confirmations
  - Prevent some or all other generators from getting any generations

Task of Bitcoin Miners(1)

- Listen for transactions
- Validate transactions – signature is correct and no double spending
- Maintain blockchain and listen for new blocks
- Validate each block that you receive by validating each transaction in the block and checking that the block has a valid nonce.

Task of Bitcoin Miners(2)

- Assemble a candidate block from validated transactions.
- The candidate block will extend the longest known valid chain.
- Find a nonce for your block that makes it valid.
- Publish your block and hope it gets accepted
- Profit if accepted

Task of Bitcoin Miners(3)

- If two different blocks are mined and announced at around the same time, it results in a two block fork.
- So, which to build on?
- The default is to build on the block you heard about first.

Block Chain

- Bitcoin makes sure there is only one block chain by making blocks really hard to produce.
- miners have to compute a cryptographic hash of the block that meets certain criteria
  - difficulty of the criteria for the hash is adjusted based on how frequently blocks are appearing
  - also carefully validate all the transactions that go into their blocks
- Successful miners are rewarded some bitcoins according to a preset schedule

Bitcoin

- Governance - an open source community of developers backed by the Bitcoin Foundation.
- Democratic - if you don't like one of the changes, you are more than welcome to fork the chain and implement your own rules
- Money Creation - is given to the people, not to the central bankers.
- Deflationary by design - money supply cannot be manipulated and is fixed at 21 million coins, each divisible up to 8 decimal

Bitcoin Mining

- Dedicated HW: ASICS etc.
- Serious energy consumption

Bitcoin Mining

Bitcoin Mining

Where do people Bitcoin Mining

- Where energy is cheap
  - Mining one Bitcoin:
    - $3,000 in China,
    - $500 in Venezuela,
    - $4,700 in USA (2018)
    - https://www.trustnodes.com/2018/04/26/bitcoin-mining-costs-just-3000-china-500-venezuela-4700-usa
- But cheap energy is not always clean energy
- Ethical considerations?

Next Time

- Smart Contracts

- Questions?

- Inspired from / based on slides from
  - Jason Madden, Mehmet H. Gunes
  - Johannes Kofler
  - Terence Spies
  - And many others