Bitcoin Basics

Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

1. Introduction to Bitcoin & Blockchain

2. Setup of the Bitcoin blockchain
- Blockchain & blocks
- Block header & contents
- Genesis block

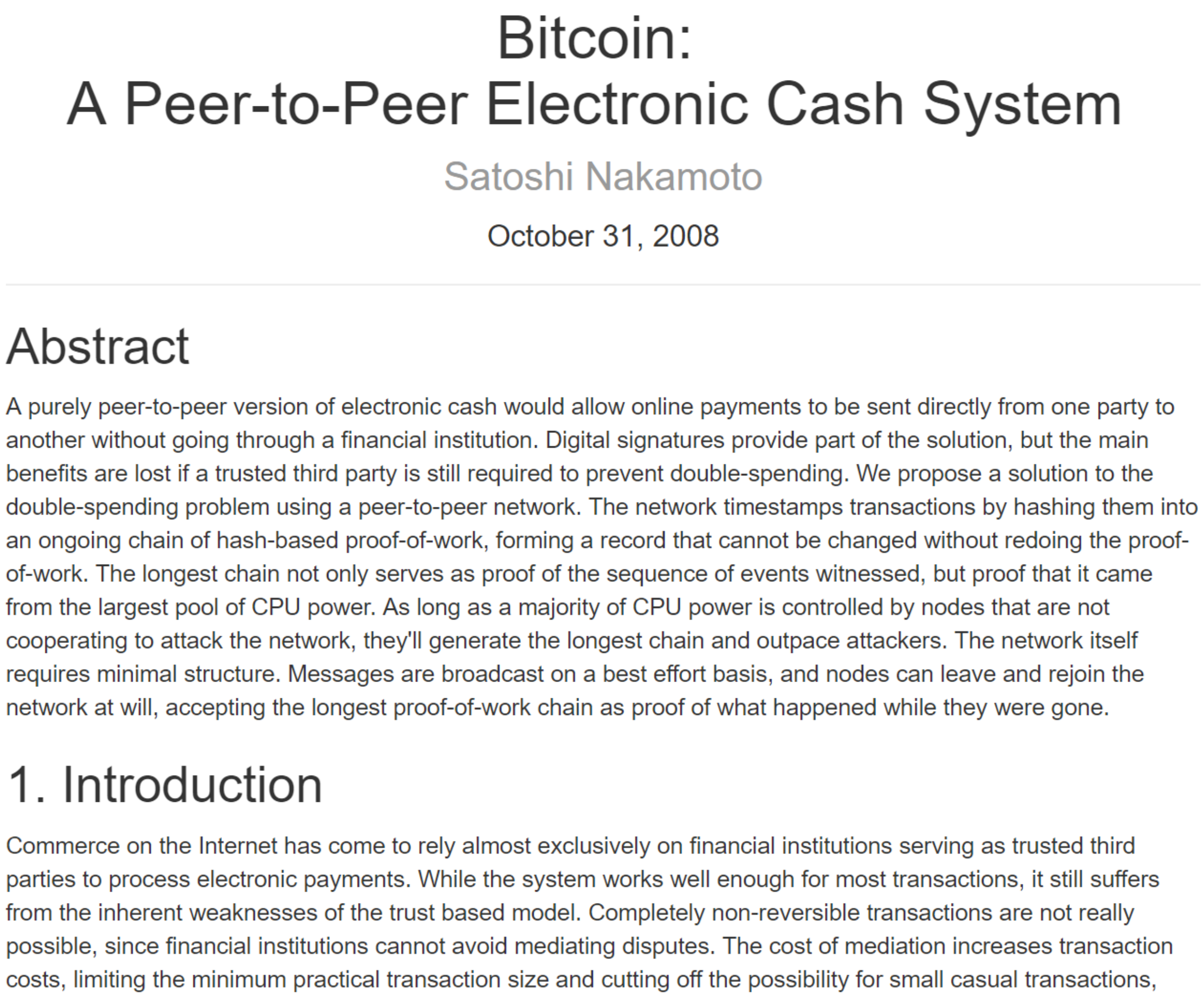
3. Transactions in Bitcoin
- Account-based vs. transaction-based ledger

4. Bitcoin network
- P2P network
- Types of nodes

5. Storing Bitcoins

This chapter is heavily inspired by and uses examples from „Bitcoin and Cryptocurrency Technologies“ by Arvind Narayanan

A technical paper published online in the year of the financial crisis



Bitcoin:
A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

October 31, 2008

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.

1. Introduction

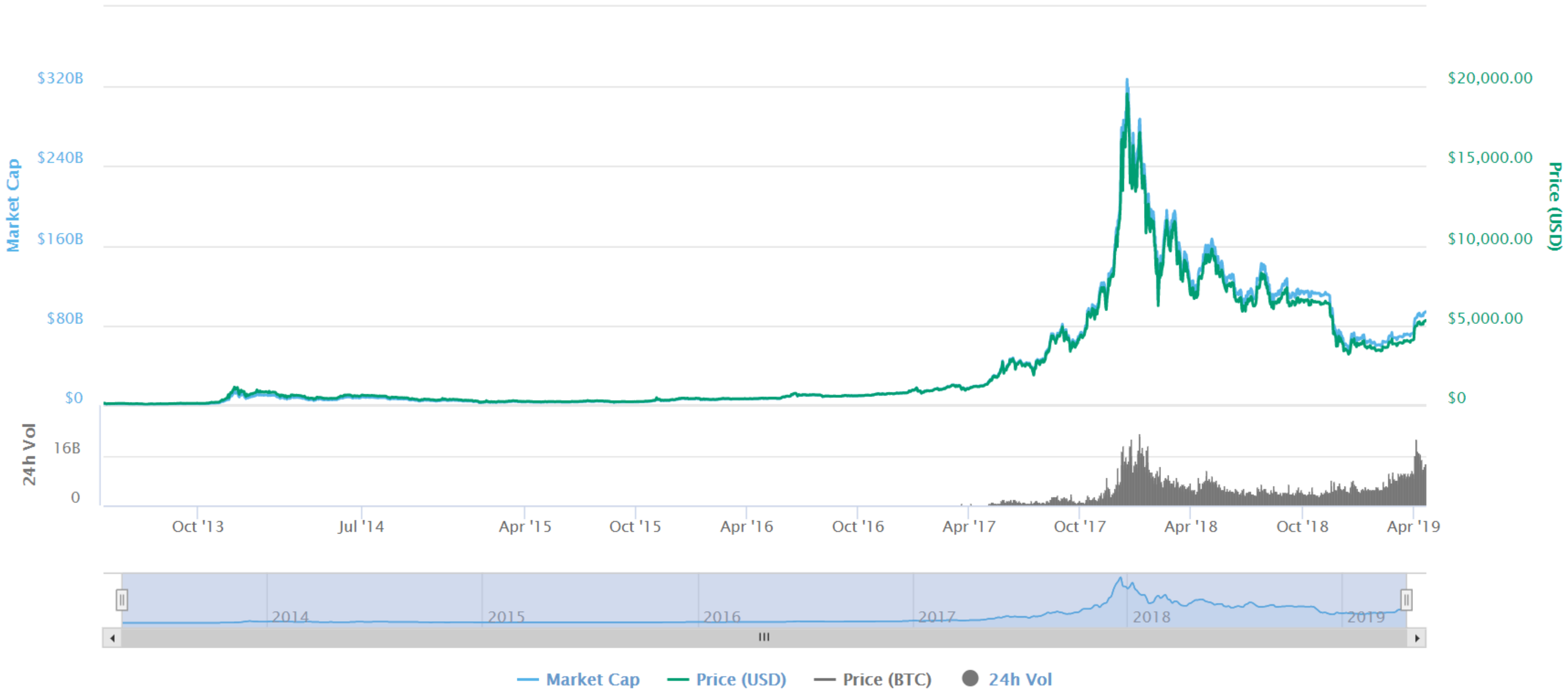
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions,

- **Satoshi Nakamoto** wrote a paper in 2008 about *“Bitcoin: A Peer-to-Peer Electronic Cash System”*
- The **real identity** of Satoshi Nakamoto remains **unknown**. We don’t know whether it was a single person or a group.
- In **January 2009** the **first block** of the Bitcoin Blockchain was **mined**.
- In contrast to public opinion, Bitcoin was **not invented because of the financial crisis**. Satoshi Nakamoto said he started working on Bitcoin in May 2007 (in contrast the financial crisis started in August 2007).

Nathaniel Popper - Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money

[NAKA2008] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

Bitcoin has a long history

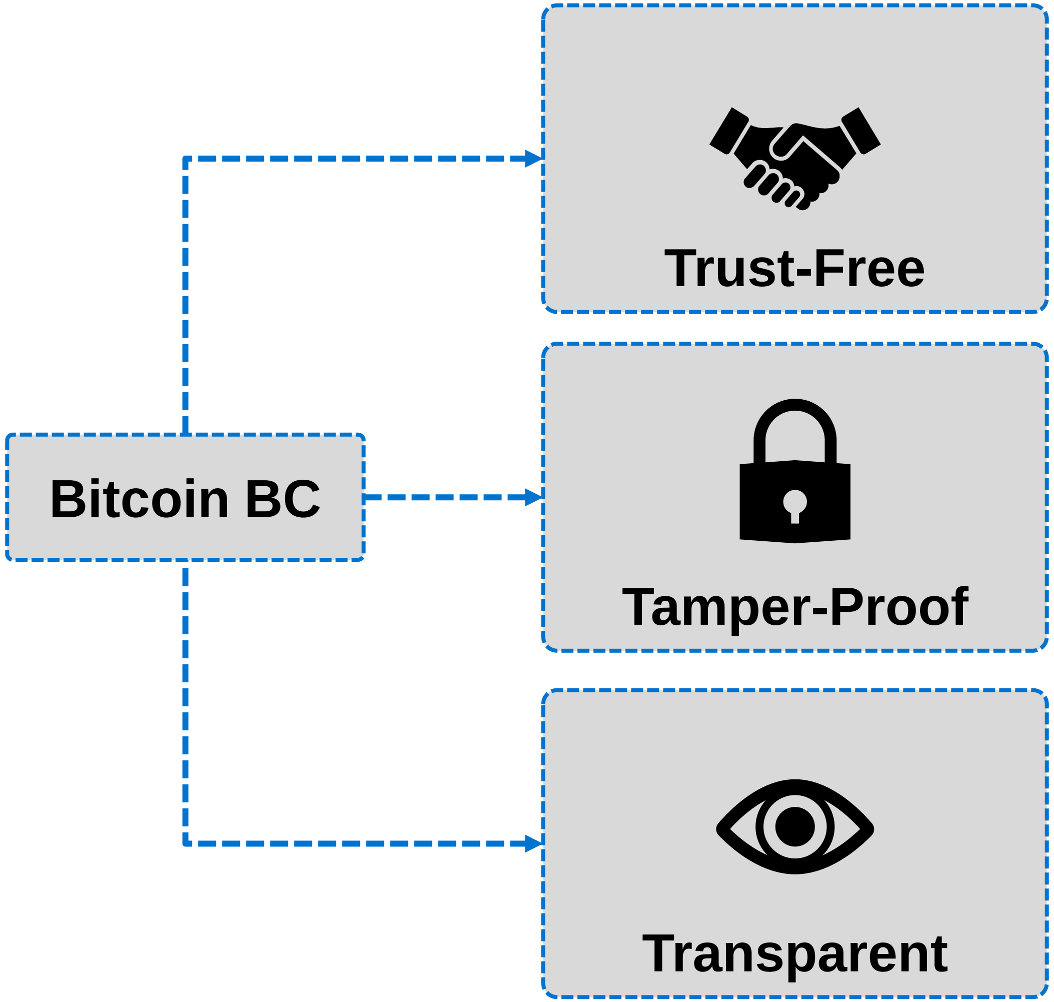


Coinmarketcap, Bitcoin Charts, https://coinmarketcap.com/currencies/bitcoin/#charts, retrieved 20th April 2019

Key properties of the bitcoin blockchain

It has **three key properties**:

- **Trust-Free**: *The system does not require a third party which controls or maintains the system.*
- **Tamper-Proof**: *The system is resistant to manipulation. The history of events cannot be changed.*
- **Transparent**: *Every participant of the system can read and validate all information and the current state.*



Outline

1. Introduction to Bitcoin & Blockchain

2. Setup of the Bitcoin blockchain

- Blockchain & blocks
- Block header & contents
- Genesis block

3. Transactions in Bitcoin

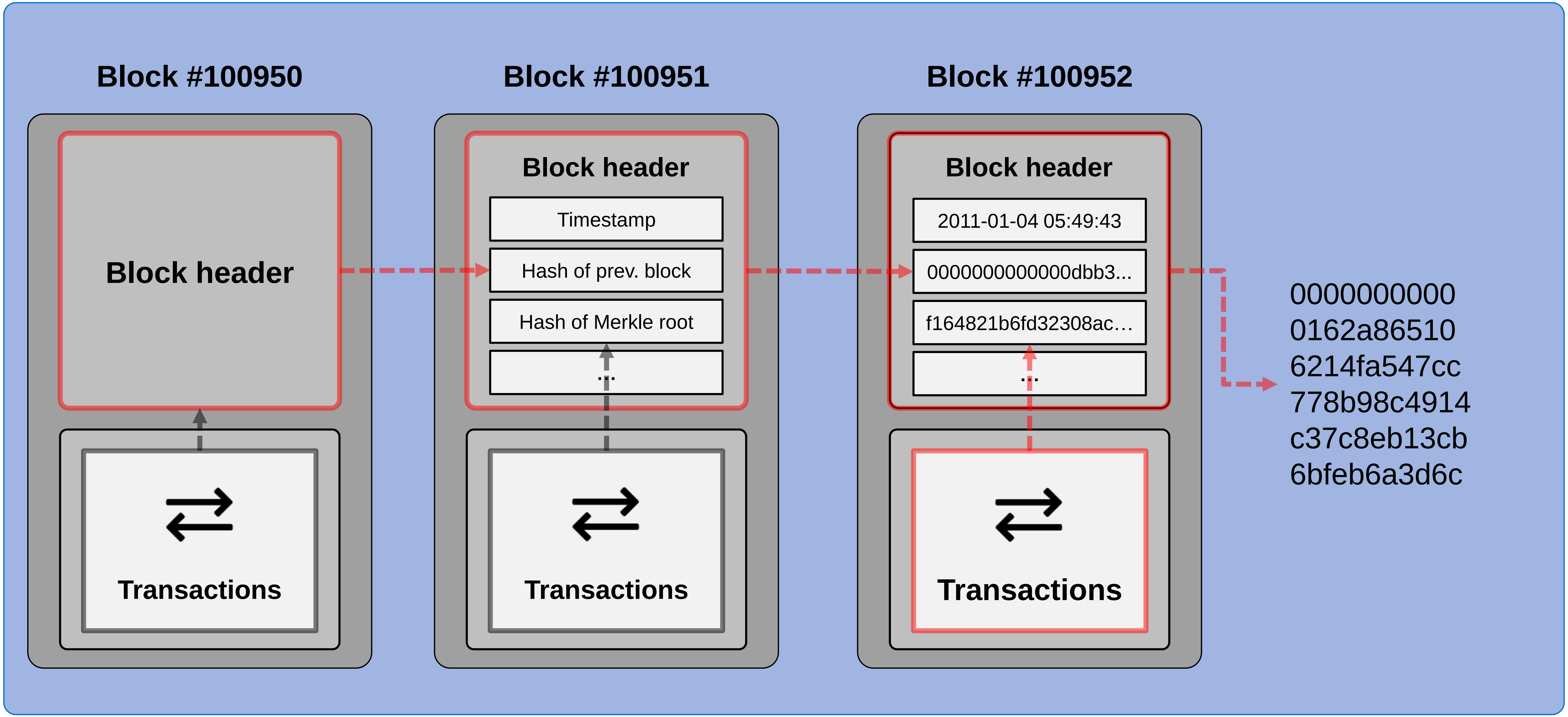
- Account-based vs. transaction-based ledger

4. Bitcoin network

- P2P network
- Types of nodes

5. Storing Bitcoins

How does the Bitcoin Blockchain look like?



Block #100950

Block header

Transactions

Block #100951

Block header

Timestamp

Hash of prev. block

Hash of Merkle root

...

Transactions

Block #100952

Block header

2011-01-04 05:49:43

0000000000000dbb3...

f164821b6fd32308ac…

...

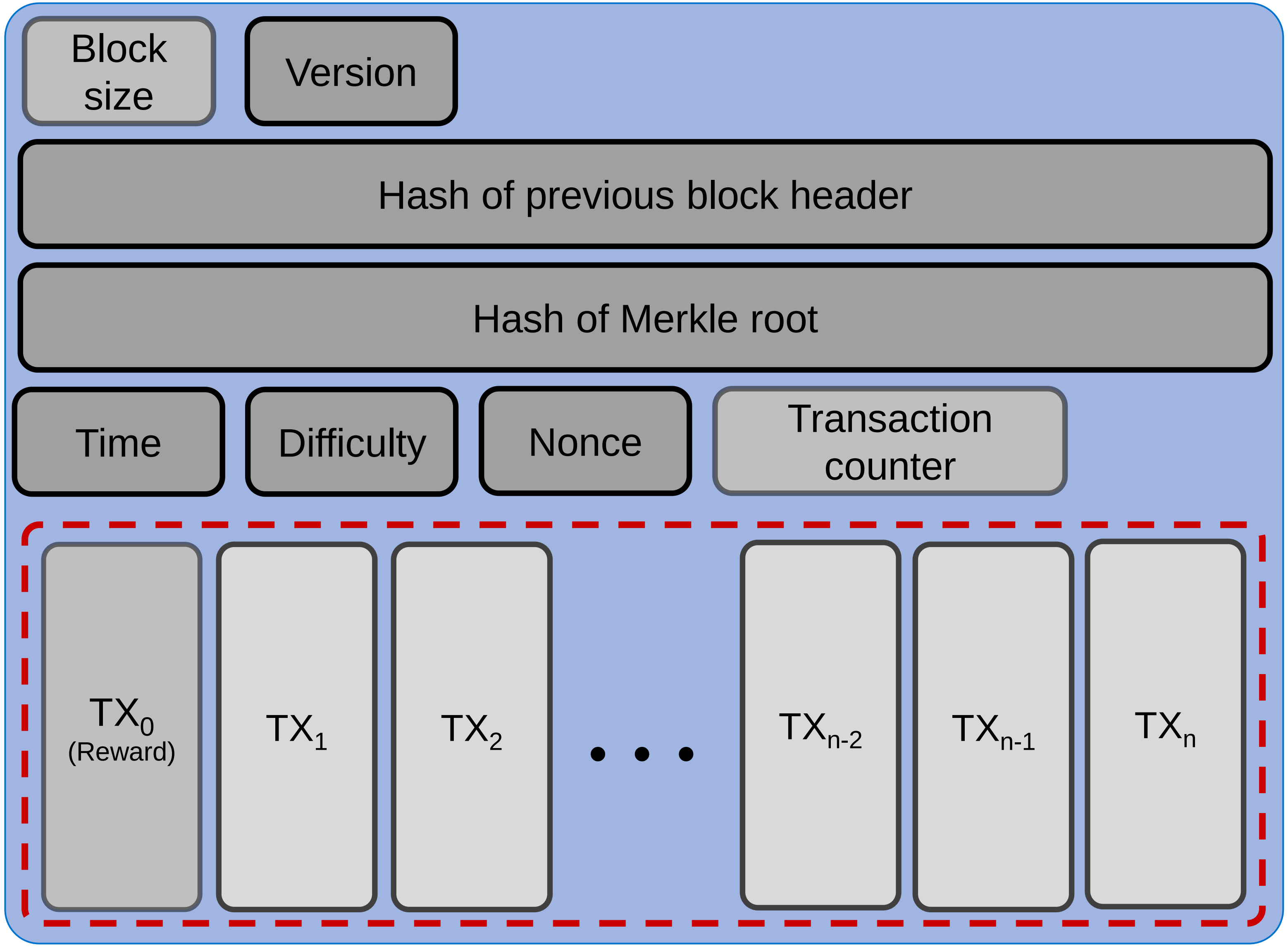
Transactions

0000000000
0162a86510
6214fa547cc
778b98c4914
c37c8eb13cb
6bfeb6a3d6c

03 Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Anatomy of the Bitcoin block chain – Block details

- The *hash of the previous* block creates the chaining.
- The hash of the Merkle root node of a Merkle tree structure with all transactions (as explained in Chapter 2).
- The *nonce* is required for the consensus mechanism in the network.
- The block‘s hash used for chaining is calculated from the *version* until the *nonce* field.
- The height of the block is stored in the coinbase transaction. (TX_0)



The „genesis“ block

Blocks have to reference their predecessor ⟶ **How does a blockchain start?**

Bitcoin‘s genesis block[1]:

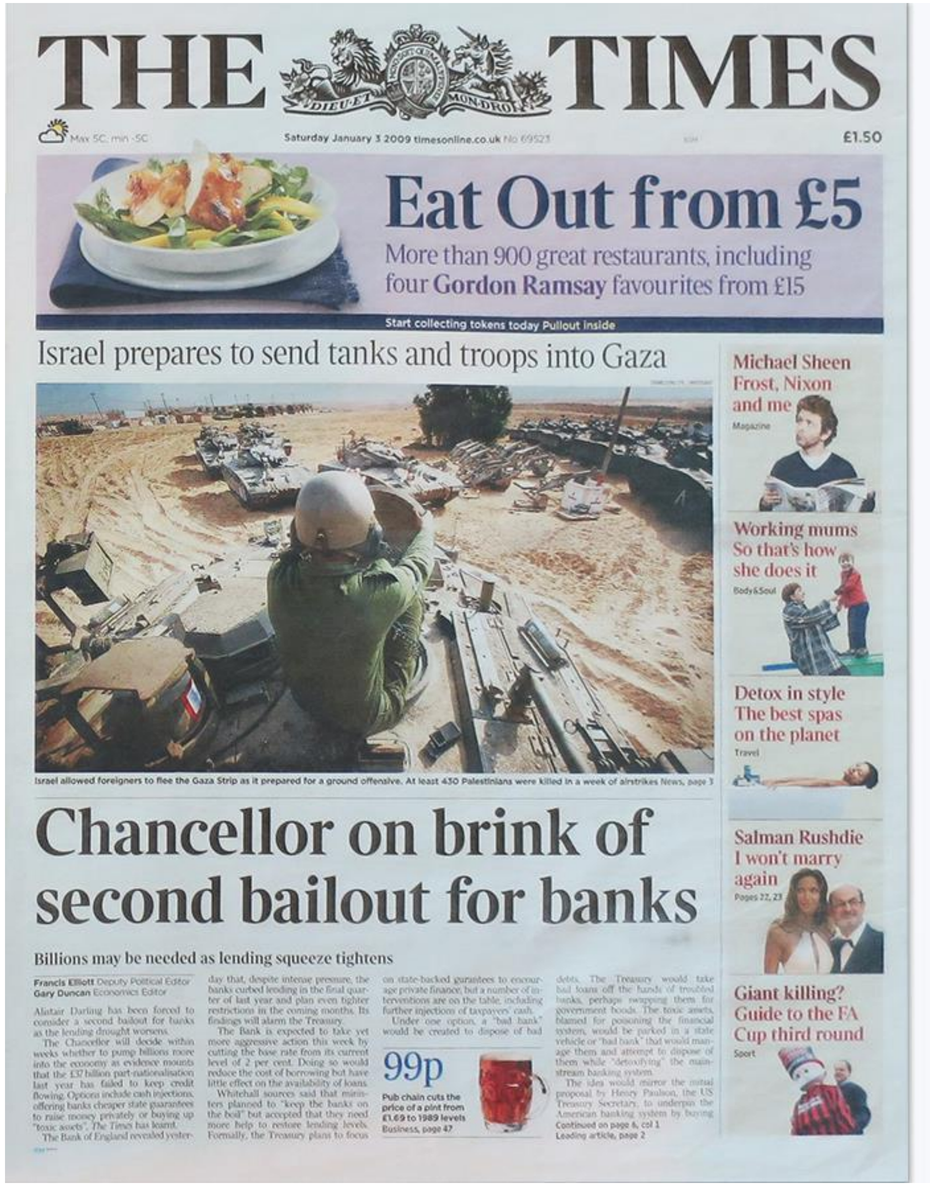
- mined at 2009-01-03 18:15:05
- references a previous block with hash `0`
- contains only the mining reward transaction → first 50 BTC which can never be spent

The fact that it cannot be spent is based on the source code of the current `bitcoin-core` client[2]. The client searches through all blocks in `ConnectBlock` and processes all transactions, however skips the genesis block.

[1] https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (accessed 24.10.2017)

[2] https://github.com/bitcoin/bitcoin/blob/9546a977d354b2ec6cd8455538e68fe4ba343a44/src/main.cpp#L1668 (accessed 24.10.2017)

Data contained in the genesis block



THE TIMES

Max 5C, min -5C Saturday January 3 2009 timesonline.co.uk No 69523 £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

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

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.

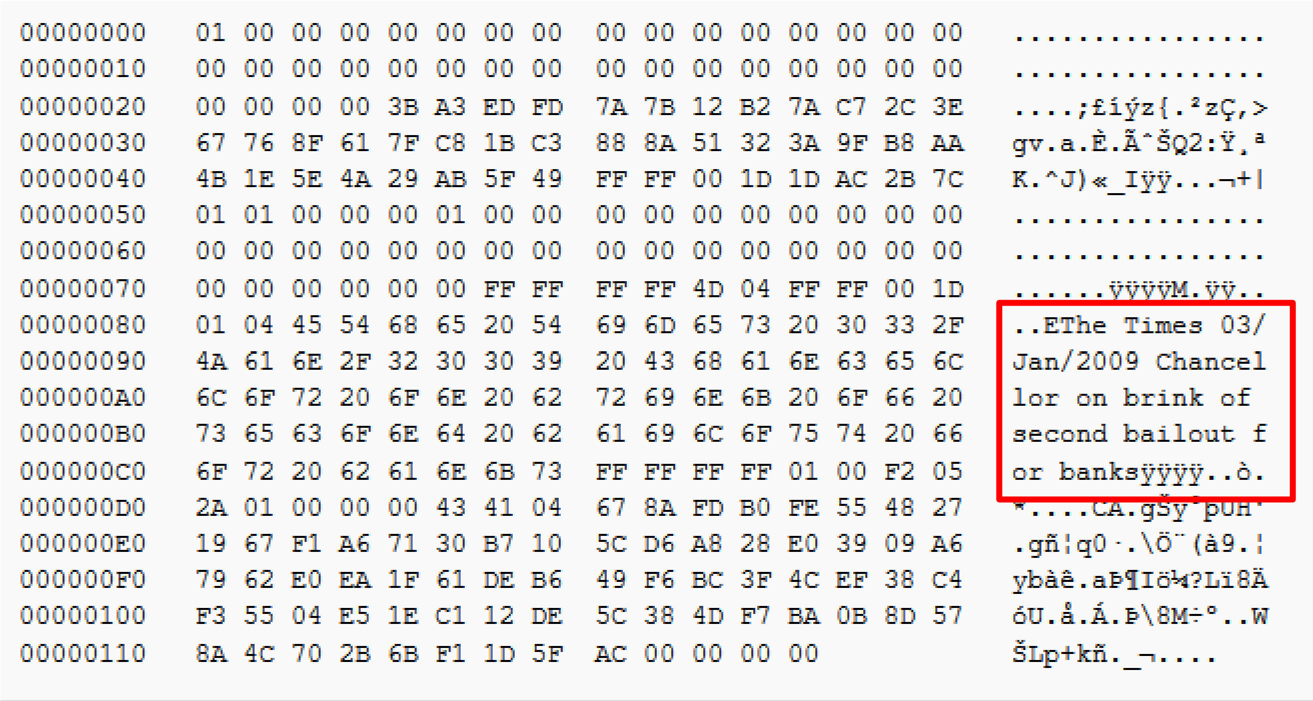
Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further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



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

The data highlighted is stored in the *scriptSig* field of the first transaction (=coinbase transaction).

A possible motivation to put this headline into the genesis block is to prove that no "pre-mining" has happened.

Outline

1. Introduction to Bitcoin & Blockchain

2. Setup of the Bitcoin blockchain

- Blockchain & blocks
- Block header & contents
- Genesis block

3. Transactions in Bitcoin

- Account-based vs. transaction-based ledger

4. Bitcoin network

- P2P network
- Types of nodes

5. Storing Bitcoins

Account-based ledger

Create 25 coins and credit to Alice	signed by miners
Transfer 17 coins from Alice to Bob	signed by Alice
Transfer 8 coins from Bob to Carol	signed by Bob
Transfer 5 coins from Carol to Alice	signed by Carol
Transfer 15 coins from Alice to Bob	signed by Alice

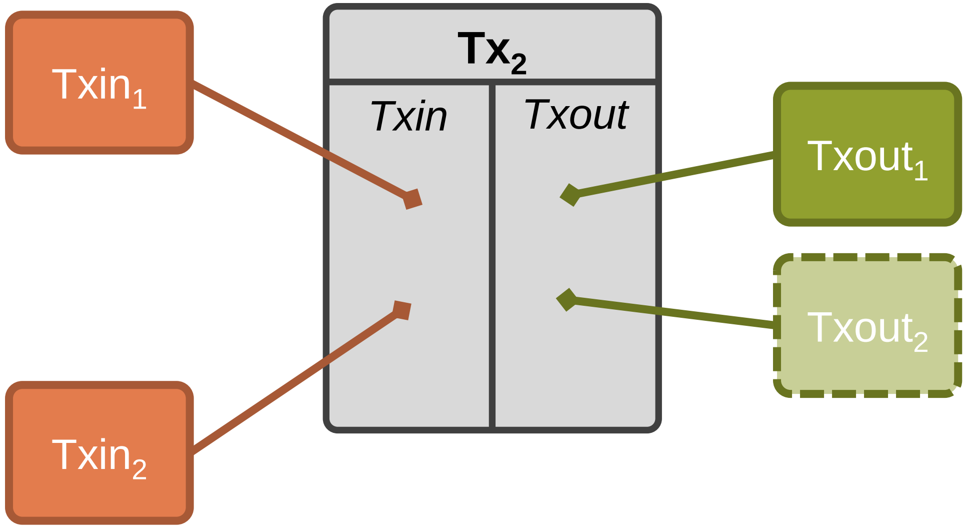
Transactions

Alice	Bob	Carol
25	0	0
8	17	0
8	9	8
13	9	3
-2	24	3

World State

- *Intuitively*: We consider Bitcoin to use an account-based ledger. However, an account-based approach takes a lot of effort to track the balances of every account.
- In an account-based ledger, transactions can transfer arbitrary amounts of coins between accounts.
- Transactions lead to a “world-state” of accounts and account balances.
- In Ethereum, the hash of the Merkle root of the Merkle tree of all accounts and their balances is stored in the block.
- By using a transaction-based ledger, Bitcoin enables wallet owners to define conditional transactions using Bitcoin Script.

Transaction-based ledger



- Transactions (**Tx**) have a number of inputs and a number of outputs.
  - **Inputs (Txin)**: Former outputs, that are being consumed
  - **Outputs (Txout)**: New creation of coins

- In transactions where **new coins** are created, **no Txin** is used (no coins are consumed)

- Each transaction has a unique identifier (**TxID**). Each output has a unique identifier within a transaction. We refer to them (in this example) as *#TX[#txout]*, e.g., 1[1], which is the second Txout of the second transaction.

Transaction-based ledger

0	Txin: ∅ Txout: 25.0 → Alice
1	Txin: 0[0] Txout: 17.0 → Bob, 8.0 → Alice signed by Alice
2	Txin: 1[0] Txout: 8.0 → Carol, 9.0 → Bob signed by Bob
3	Txin: 1[1] Txout: 6.0 → David, 2.0 → Alice signed by Alice

Example:

0. No input required, as coins are created.
1. The Tx is used as an Txin. Two Txout are created, one to Bob and one to Alice. (1[0] and 1[1]) The Tx is signed by Alice.
2. Uses first Txout of Tx1. Creates two Txout to Carol and Bob, signed by Bob.
3. Uses second Txout of Tx1. Creates two Txout to David and Alice, signed by Alice.

Further remarks

Change Address:
Why does Alice have to send money back to herself? In Bitcoin, either all or none of the coins have to be consumed by another transaction. The address the money is sent back to is called a *change address*. This enables an efficient verification, as one only has to keep a list of **unspent transaction outputs** (**UTXO**).

Consolidating funds:
Instead of having many unspent transaction outputs, a user can create a transaction that uses all UTXO she has and creates a single UTXO with all the coins in it.

Joint payments:
Two or more parties can combine their inputs and create one output. Of course, it requires signatures from all involved parties.

Outline

1. Introduction to Bitcoin & Blockchain

2. Setup of the Bitcoin blockchain

- Blockchain & blocks
- Block header & contents
- Genesis block

3. Transactions in Bitcoin

- Account-based vs. transaction-based ledger

4. Bitcoin network

- P2P network
- Types of nodes

5. Storing Bitcoins

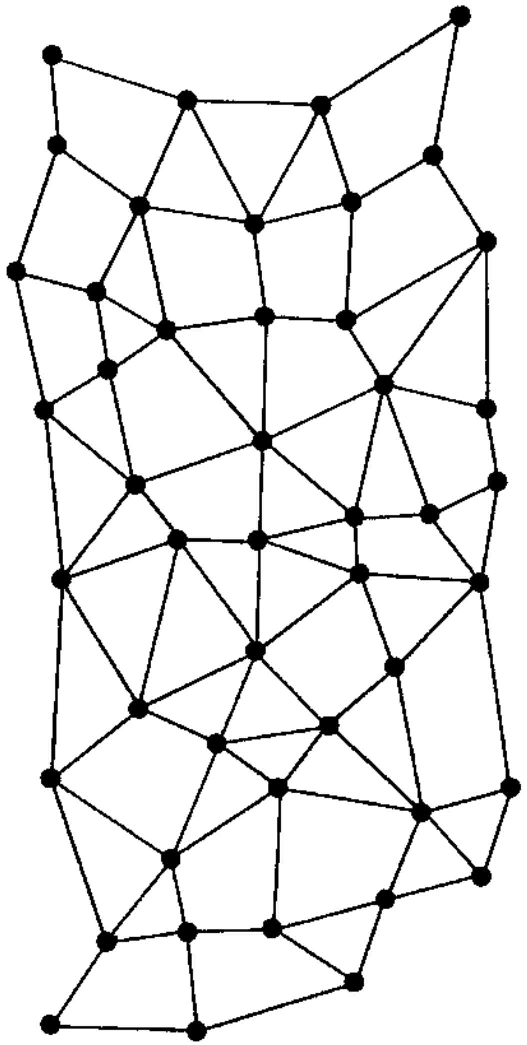
Gossip protocol

- Bitcoin itself consists of different users and nodes. We distinguish between **wallet owners**, **light nodes**, **full nodes** and **miners**. (More on that topic later)

- They communicate in a **decentralized** fashion, meaning that no single entity or node is superior.

- To communicate, they need to have clear rules
  - How to **find** other nodes (bootstrapping)
  - How the **sync** the block chain
  - How to **send** and **receive** transactions
  - How to **send** and **receive** blocks

- The basic network uses a peer-to-peer **gossip** protocol. Messages about new blocks or transactions are **validated** and then **broadcasted**. To prevent a second broadcast, the node keeps track of the transactions and blocks sent by itself.



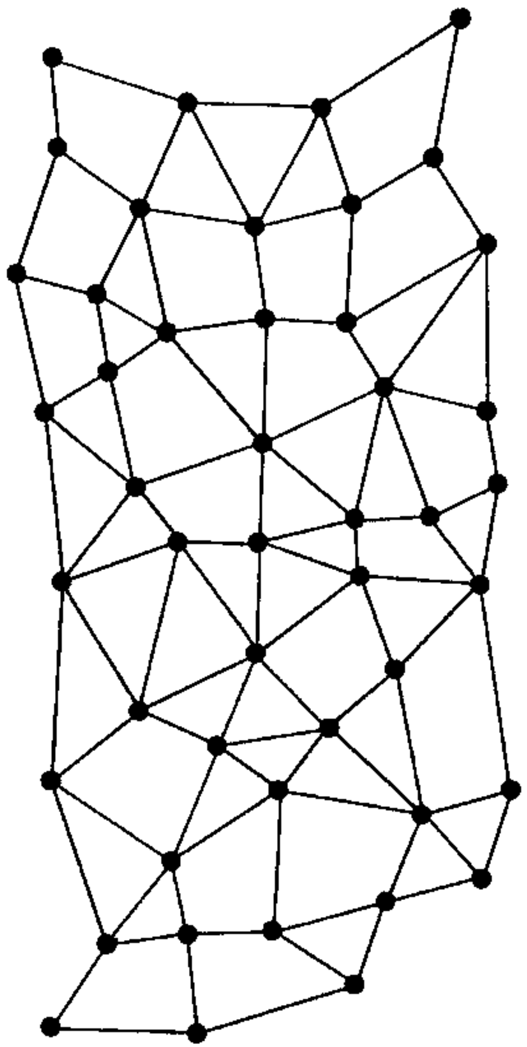
An advanced look into the verification of messages containing transactions or blocks provides The Bitcoin Wiki: Protocol Rules.

Bootstrapping of nodes / client node discovery

How are new nodes introduced into the Bitcoin network?

There are several ways:

- (deprecated) Get to know new clients via **IRC-channels**
- Hard-coded **DNS-services** which offer IP-addresses of nodes
- Hard-coded **seed addresses** (last resort)
- Addresses stored in a **database** maintained locally (to be loaded after a restart)
- **Command-line** provided addresses
- **Text-file** provided addresses



Roles in the Bitcoin network

Wallet Owner (User)

- The wallet owner owns different **private keys** to unspent transaction outputs (UTXOs)
- He is the **owner** of all stored currencies on these addresses
- He sends money by **signing** and **publishing** new transactions to a connected light node, full node or miner

Light Node (Software)

- The light node can **act** as a **relay** for transactions of one **wallet owner**
- It **validates** whether a **single transaction** of the wallet owner was executed correctly
- The light node also **requires a full node** to connect to the network
- **Almost no relevance** in practice today. Today, centralized services are used to create transactions.

Full Node (Software)

- The full node **maintains** the **complete blockchain**. Its record of the chain is complete, it contains every single transaction and block until the genesis block.
- Is **connected to** other **full nodes** and exchanges information. Namely:
  - **Validates** every transaction and block it receives
  - **Relays** all new transactions and blocks

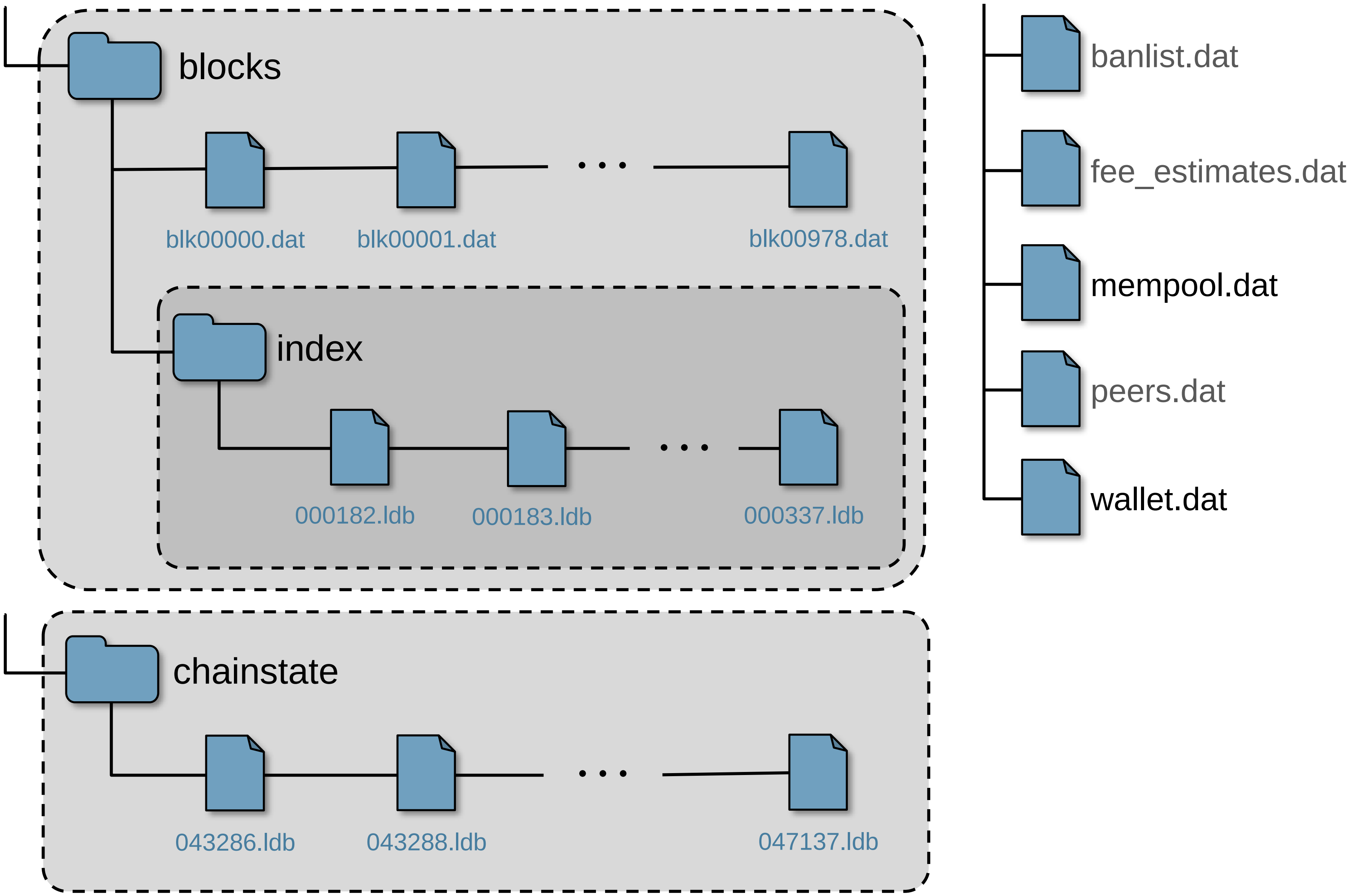
Miner (Software)

- The miner **needs** the **same record** as a **full node** in order to work properly. He also is connected with other nodes and maintains the network.
- Additionally, the miner is **responsible** for **creating** new **blocks** by trying to solve the **mining puzzle**.
- The miner gets rewarded by creating new blocks.

Anatomy of the Bitcoin block chain – Raw data on disk

Miners and full nodes organize their data in a certain way. (Bitcoin core)

As of April 2019, the total data size of the Bitcoin Blockchain is 210 GB.



03 Bitcoin Basics- Gallersdörfer, U., Holl, P., & Matthes, F. (2020). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Anatomy of the Bitcoin block chain – Raw data on disk

blocks and **blocks/index**

Contains .blk files that contain the actual block chain in raw network format; **index** contains a database which stores the location of each block on the disk keyed with its hash.

chainstate

A LevelDB (leveldb.org) database with all currently unspent transaction outputs in the system (UTXO). This is used when operating a bitcoin node in favor of the raw blockchain data.

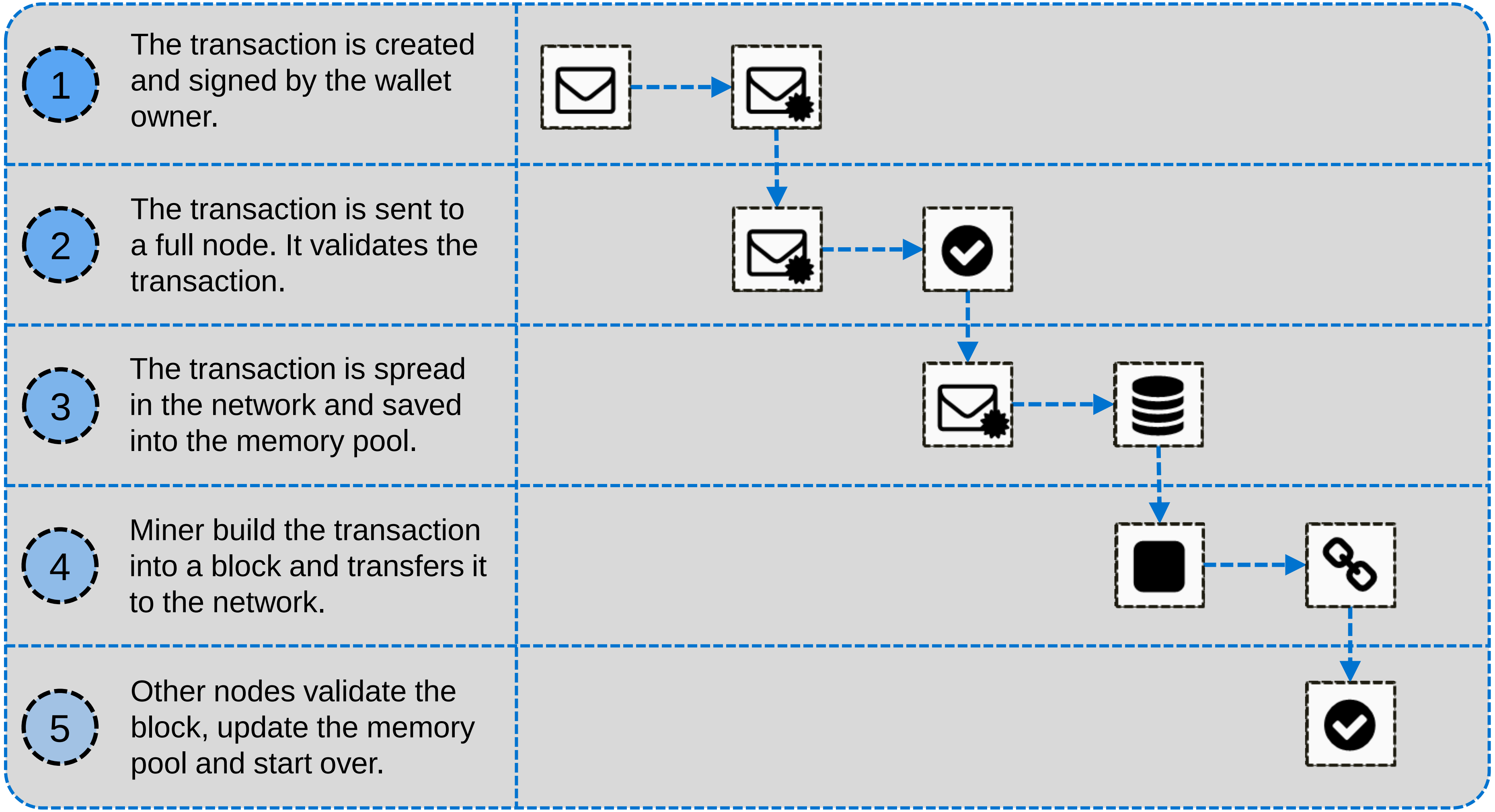
mempool.dat

A list of unconfirmed transactions to be part of a future block.

wallet.dat

Data regarding the user‘s (owner of the node) personal wallet.

How does a newly created transaction find its way into a block?



1 The transaction is created and signed by the wallet owner.

2 The transaction is sent to a full node. It validates the transaction.

3 The transaction is spread in the network and saved into the memory pool.

4 Miner build the transaction into a block and transfers it to the network.

5 Other nodes validate the block, update the memory pool and start over.

A high-level representation of how transactions are included in blocks.

Outline

1. Introduction to Bitcoin & Blockchain

2. Setup of the Bitcoin blockchain

- Blockchain & blocks
- Block header & contents
- Genesis block

3. Transactions in Bitcoin

- Account-based vs. transaction-based ledger

4. Bitcoin network

- P2P network
- Types of nodes

5. Storing Bitcoins

Storing Bitcoins

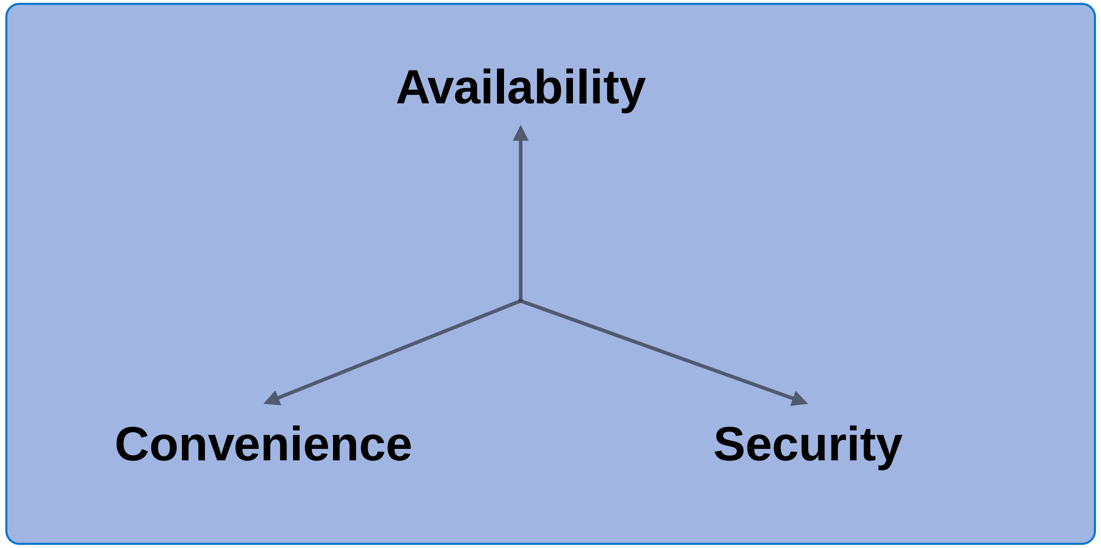
Storing bitcoins is all about storing and managing secret keys.[1]

Different approaches for storing and managing secret keys lead to different trade-offs between **availability**, **security** and **convenience**.

Availability: being able to access the keys when one wants to

Security: restricting access to the keys

Convenience: easy use



Of course: The simplest approach is to store the secret key on one's hard drive. What could *possibly* happen?

[1] Of course, this is not only important for Bitcoin, but for every Blockchain technology in this lecture.

Cryptocurrency wallets – Hot / cold storage

Hot storage

- Is **immediately available**
- Enables **convenience** at the cost of availability and security
- Example: Storage on your pc / mobile

Cold Storage

- Takes some time to “activate”
- **Enhances security** at the cost of convenience and availability
- Example: Offline Computer with RAID, locked away
- Advantage: Cold Storage does not have to be online to receive coins

Cryptocurrency wallets – Brain wallet

- A brain wallet stores bitcoins with nothing but a secret passphrase.
- There is no need for hard drives, paper or else to store information.

- Idea: a deterministic function to generate a private key out of a passphrase.

- However:
  - Source of randomness determines the security → offline guessing / password cracking
  - If passphrase is forgotten, bitcoins are lost forever

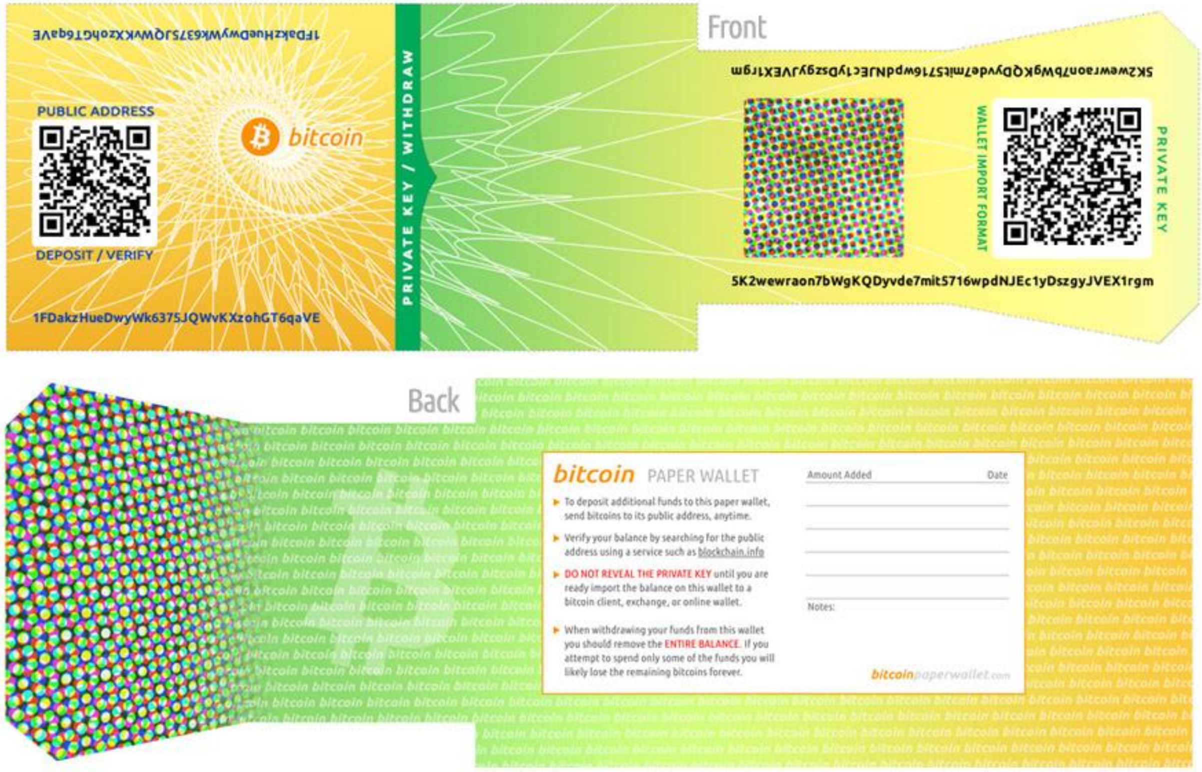
- Example:

witch collapse practice feed shame open despair creek road again ice least

Cryptocurrency wallets – Paper wallet

- **Key material** is **printed** to paper. Paper can be placed in secure places like safes or vaults.

- However, keep in mind:
  - **Source** of **randomness**
  - Side-Channel attacks
    - Infected computer / malware
    - Malicious paper-wallet generator
    - Monitored printer
  - Durability of paper
  - Durability of ink
  - Secure place: dark, 16-19°C, low humidity



- To deposit additional funds to this paper wallet, send bitcoins to its public address, anytime.
- Verify your balance by searching for the public address using a service such as blockchain.info
- DO NOT REVEAL THE PRIVATE KEY until you are ready import the balance on this wallet to a bitcoin client, exchange, or online wallet.
- When withdrawing your funds from this wallet you should remove the ENTIRE BALANCE. If you attempt to spend only some of the funds you will likely lose the remaining bitcoins forever.

Bitcoin Paper Wallet

Cryptocurrency wallets – Hardware wallet

- **Key material** is stored on the **hardware device**.

- Additional: Generation of a 24-word passphrase. If device gets destroyed, the passphrase allows for a recovery.

- Device is designed to keep your private key private. Key is **securely stored** within the device.

- **The display shows the amount and target of a transaction.** The **keys** on the device allow for a **confirmation or rejection** of the transactions.

- Requires trust in manufacturer and intermediaries.
  (Never buy used hardware wallets!)

Hardware Wallet - Ledger Nano S

Cryptocurrency wallets – Online-wallets & risks

- Let other people / companies store your bitcoins / cryptocurrencies for you.
- No access to the private key, coins can only used through a certain interface / website.
- Very common within most exchanges. The money is sent to the exchange, the account on the platform has now a new balance which can be traded or paid out.
- However: Very dangerous!
- Many exchanges got hacked, users lost their funds. Be careful!

MT.GOX

BITFINEX