Blockchain Technology in Healthcare

Source: [3]

Table of contents

- Bitcoin blockchain
- Digression: Hashing
- Block creation using proof-of-work
- Medical data
- Blockchain for medical health records
- Challenges and solutions
- Discussion
- Literature

Motivation of the Bitcoin blockchain

- Bitcoin has no central intermediary → Motivation: How can we solve the peer-to-peer double-spending problem?
  - How can we prevent electronic coins such as bitcoins from being spent twice without having a central intermediary (e.g. bank)

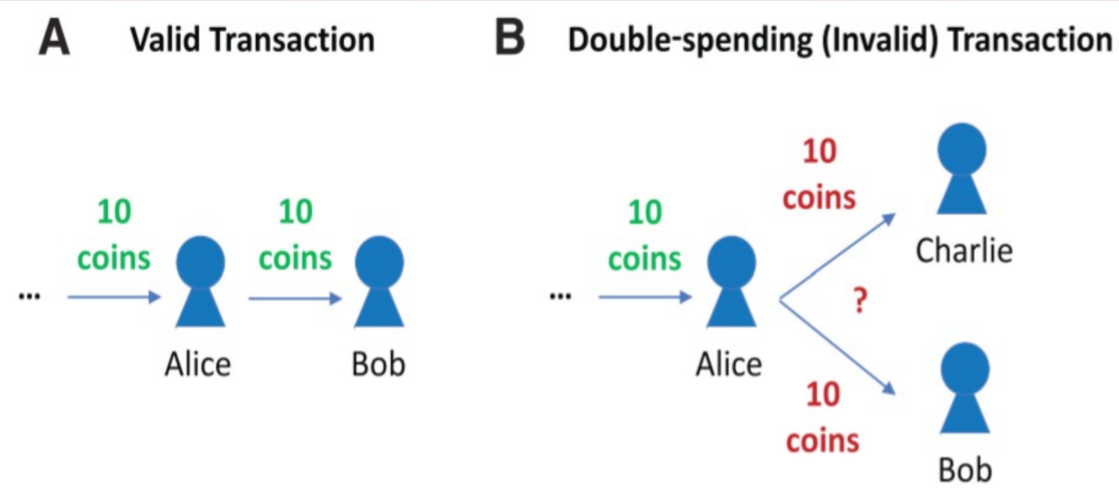

Figure 1: Double-spending problem [1]

Why is a central intermediary not good enough?

Source: [1]

Centralized vs decentralized networks

- A central intermediary creates a single point of failure
- If central intermediary is down
  → entire network stops working
- If central intermediary is intruded upon

  → whole network faces the risk of being invaded

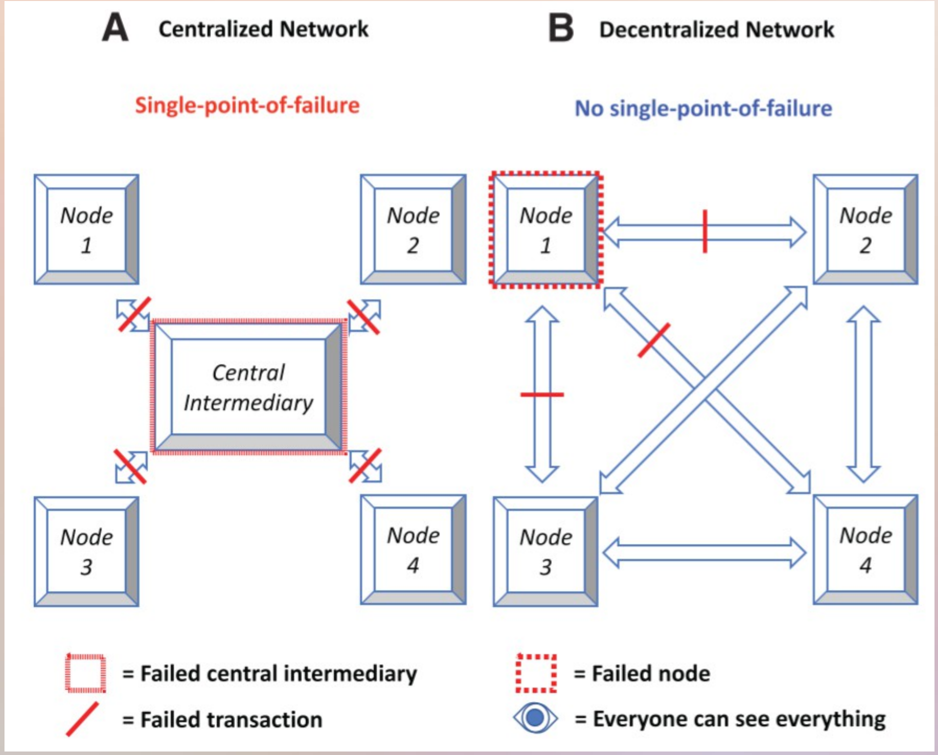

Figure 2: Centralized vs decentralized networks [1]

A decentralized network is preferred

Source: [1]

Even better: Blockchain

Some characteritics of blockchain:

- Every node maintains a copy of the whole blockchain
  → every node can verify every transaction (distributed verification)
- Distributed timestamping mechanism allow to determine, which transactions should be accepted or rejected
- A blockchain is:
  - Decentralized
  - Distributed
  - Immutable (why?)
  - Transparent

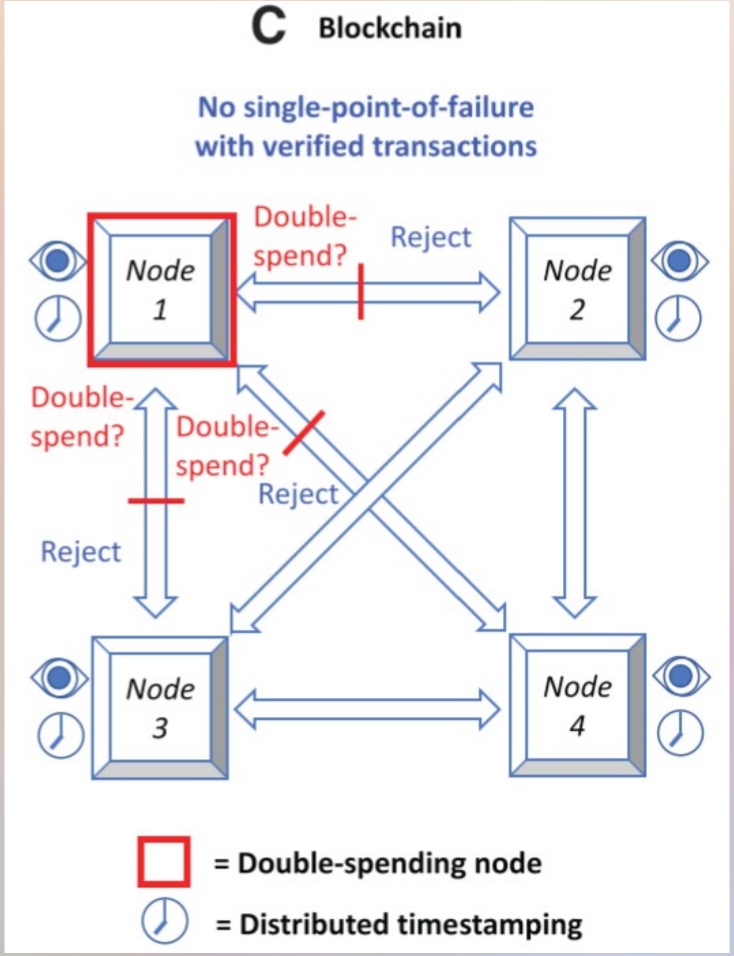

Figure 3: Overview blockchain [1]

Source: [1]

Digression: Hashing

Definition: A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values or hash

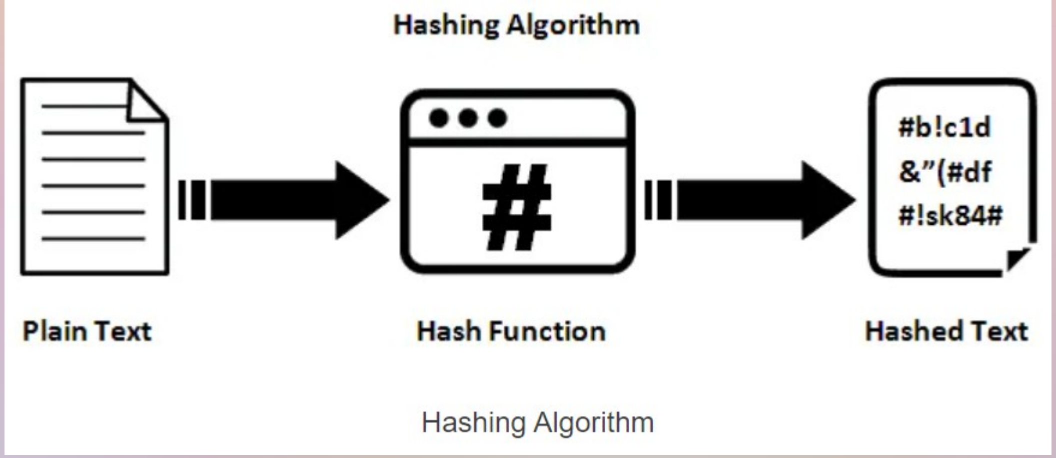

Figure 4: Overview Hashing Algorithm [6]

- A hash function should be very fast to compute and should minimize collisions

[4], [5], [6]

Simplified blockchain example

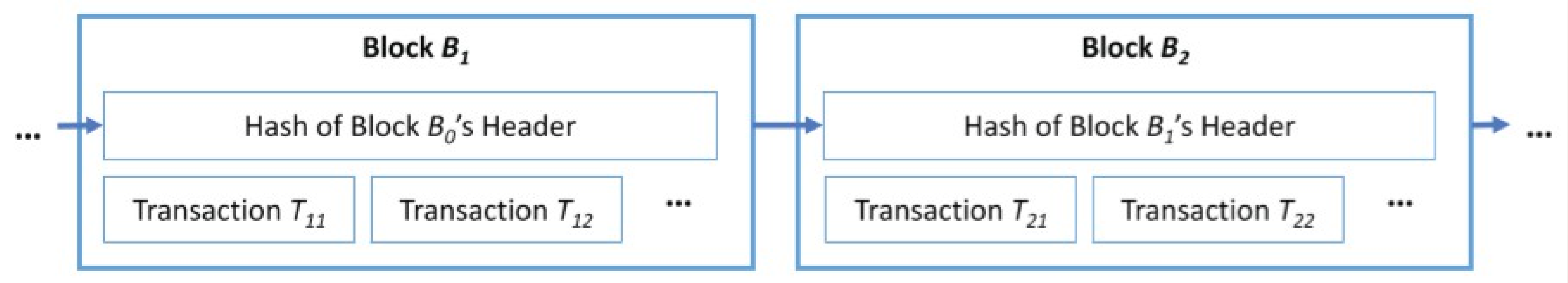

Figure 5: Exemplary blockchain [1]

- Each block in the Bitcon blockchain contains (amongst other things):
  - Transactions
  - The Hash of the previous block (here 256 bits)
    → If a transaction in block B1 is changed, its hash value changes
    → Fraud attempts are detected easily
    → Blockchain is (close to) **immutable**
- Order of blocks is deterministic (because they are chained)
  → Each block serves as a timestamp of the enclosed transactions
  → Prevents double spending (transactions are timestamped)

Source: [1]

Creation of a new block: Proof-of work

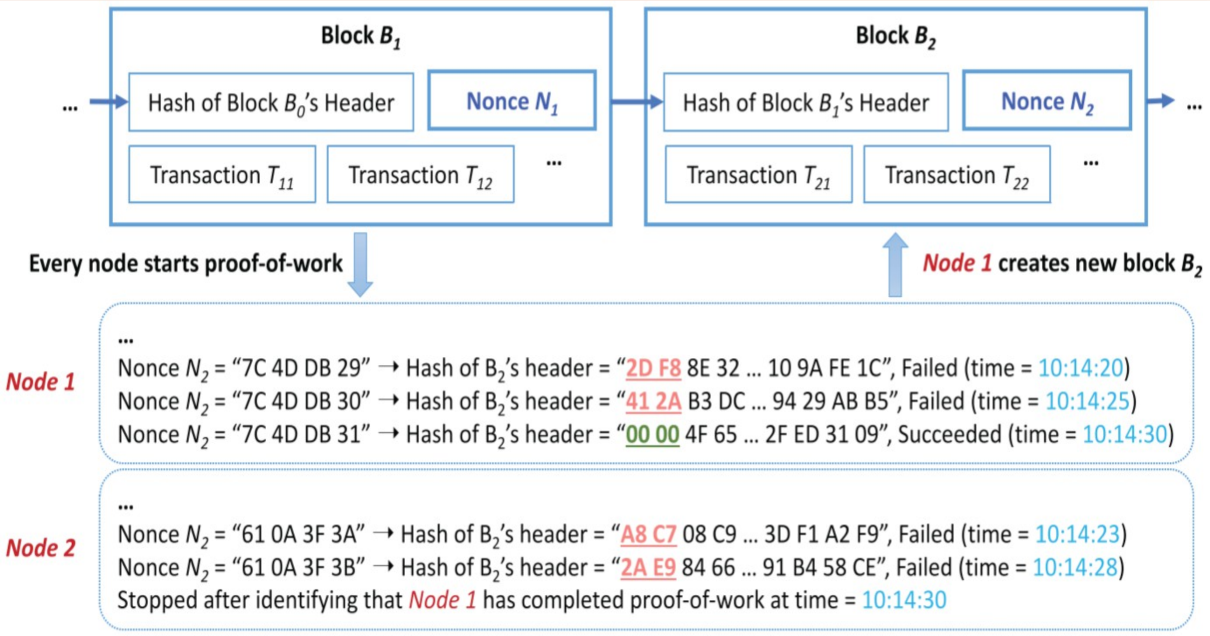

Figure 6: Creation of a new block [1]

- Nonce = only input of hashing function, that can be changed
- Nonce is incremented in steps of 1 bit, until the hashed value (here: 256 bits) contains a prefedined number of leadng zero bits (**Proof** of the work)
- First node that successfully completes the proof-of-work, may create a new block: Verify the transactions and add the block to the longest chain
- The new block is broadcasted to the whole network and verified by each node

Source: [1]

Creation of a new block: Proof-of work

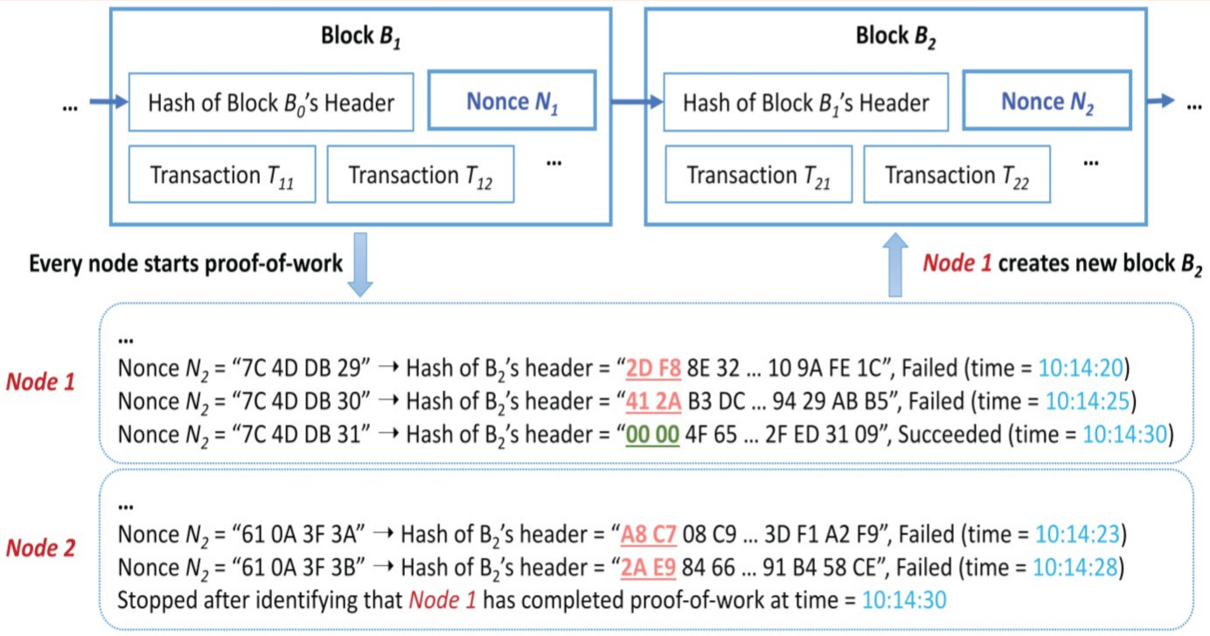

Figure 6: Creation of a new block [1]

The block creation process (mining) is difficult (computationally expensive), but checking is easy

Source: [1]

Source: [1]

Adding new blocks: Mining

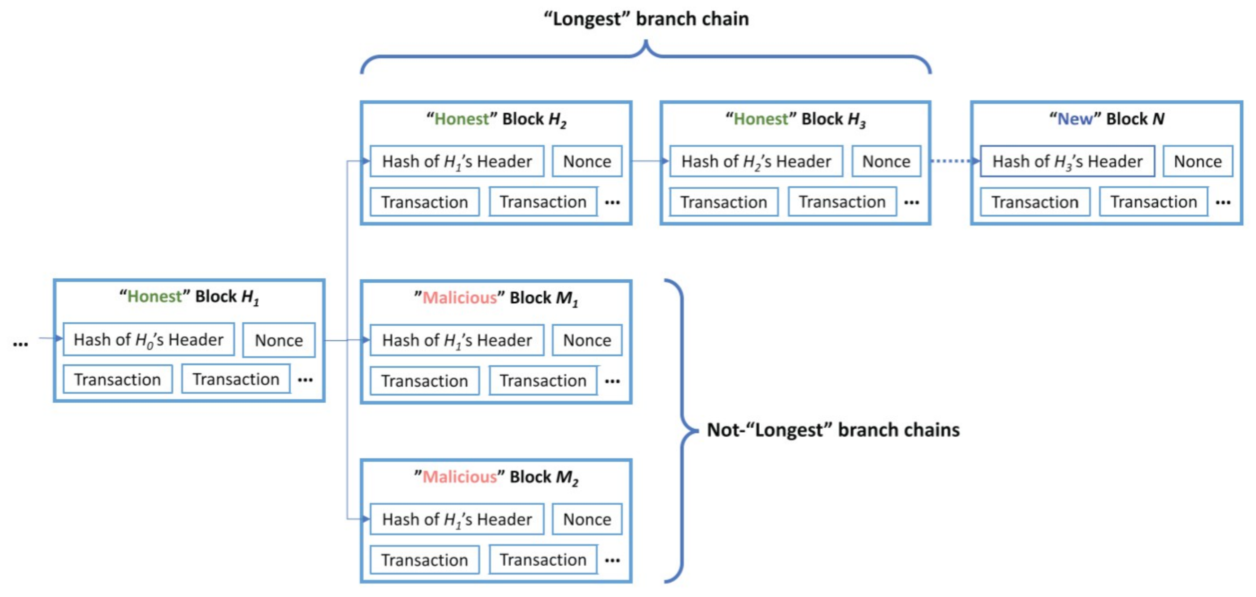

Figure 7: Adding new blocks to the blockchain [1]

- New blocks are added to the longest chain
- Example: Malicious blocks compete with an honest block
- If computational power of honest nodes is larger than that of malicious nodes
  → An honest block H3 is created right after H2, before attackers can create new malicious blocks after M1 or M2
  → Because the mining process is computationally expensive and honest nodes have more computational power, the probability of a successful attack is very small

51% attack

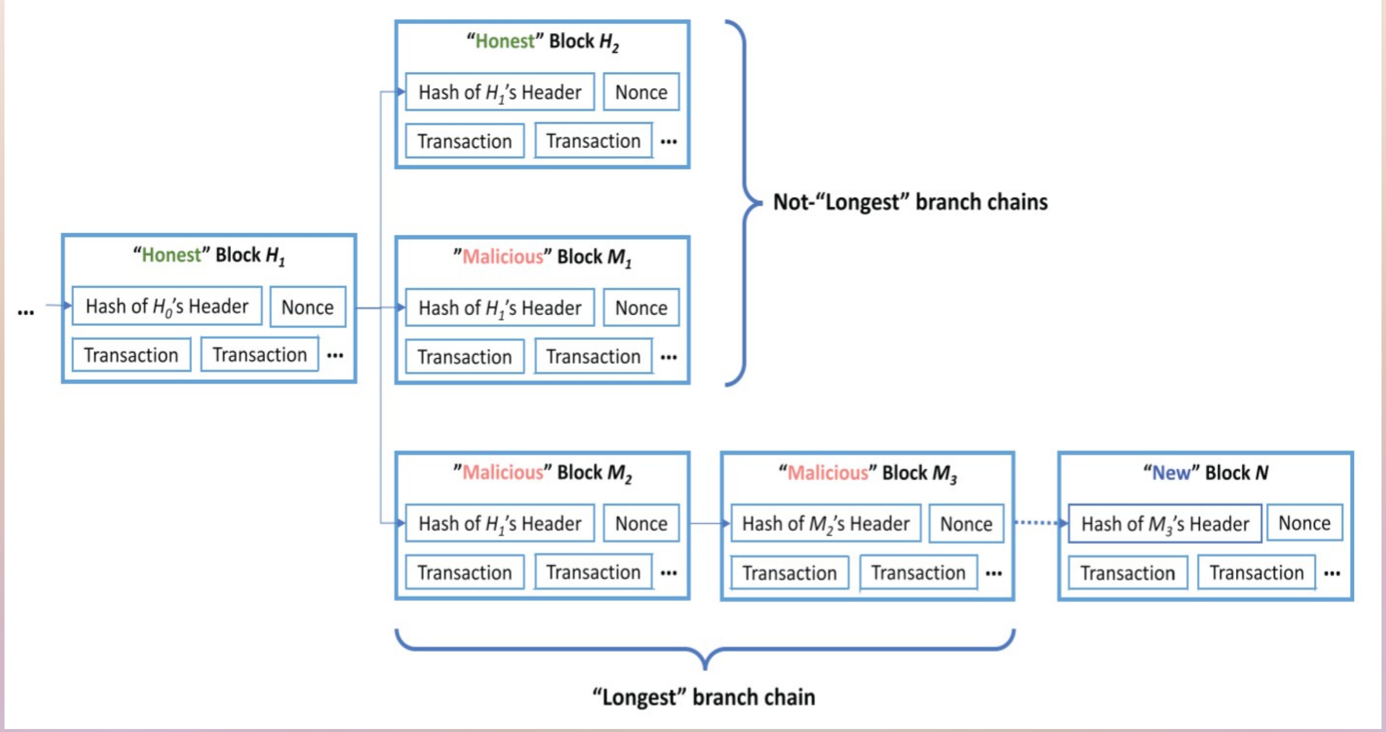

Figure 8: Example of a 51% attack [1]

- Here: Computational power of honest nodes is smaller
  → Malicious block M3 is created after M2
- New block will be added to the longest chain, after M3
  → Attacker has succesfully modified the blockchain

Source: [1]

Some additional information

Alternatives to proof-of-work:

- Proof-of-stake: The node with the oldest coins can create a new block
- Proof-of-burn: the node willing to “burn” or destroy the largest number of coins, by sending it to a “NULL” address, can create a new block

Outlook:

- Blockchain is now regarded as a new form of a distributed ledger/database
  - Arbitrary data can be stored in the metadata of transactions

➡ **Potential use in healthcare**

Sources: [1], [8]

Application in Healthcare

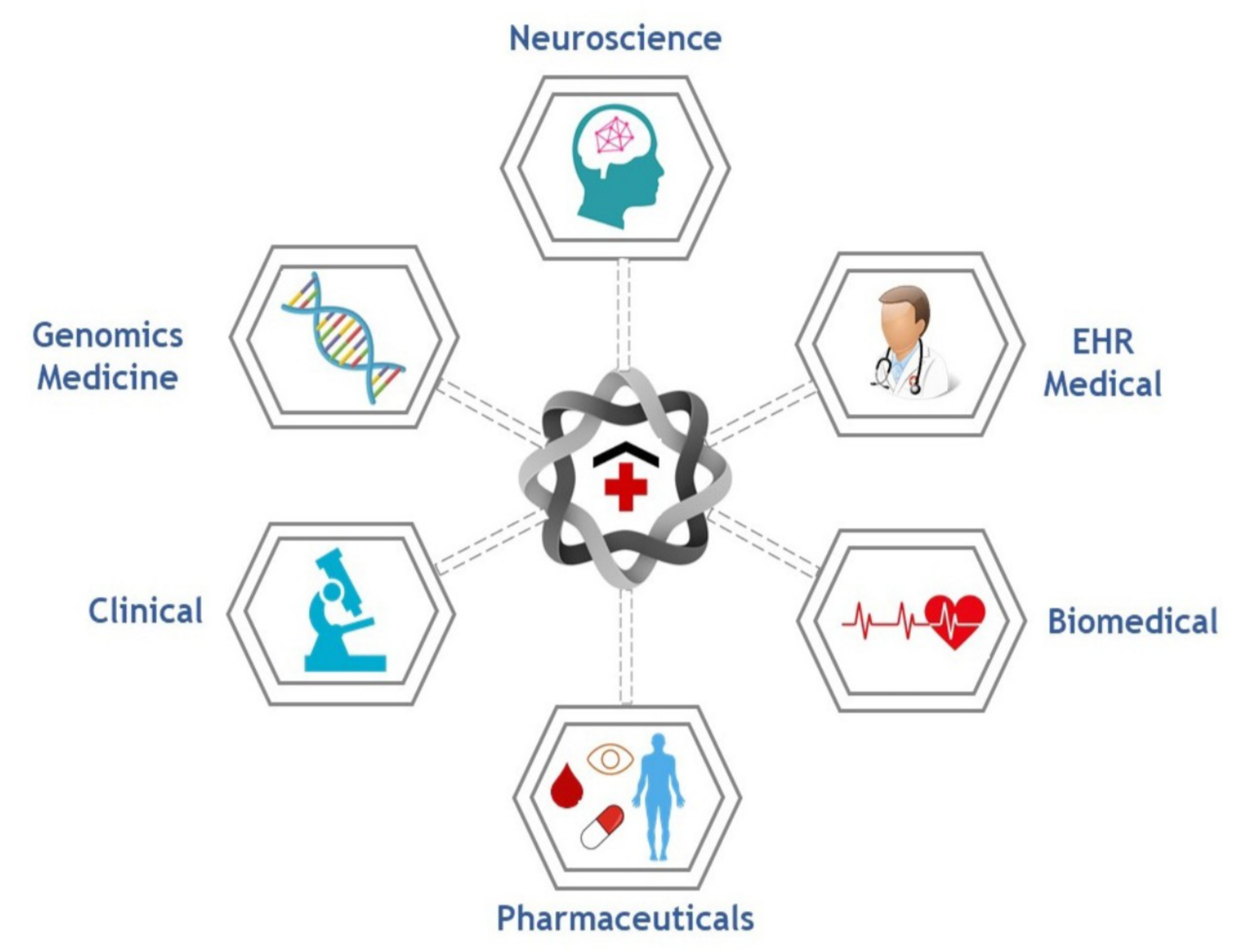

Figure 9: Applications of blockchain in halthcare [8]

Sources: [1], [8]

Sensitive medical data

- In healthcare, huge amounts of data are generated (diagnosis, treatment), accessed (patient records) and disseminated to other medical authorities
- Patients data is very sensitive
- **BUT:** Data-sharing is important for
  - Diagnosis (ask another expert or transfer to another medical authority)
  - Combined clinical decision making (medical tests e.g. blood tests)
  - Tele-medicine: Data is transferred to a specialist for an expert opinion sometimes in real time (remote cases or fragile patients)
    → Patients are remotely diagnosed

Challenge: We need a safe, secure and scalable way to share sensitive data

Sources: [1], [8]

Store patient data on a blockchain

Store the medical records of patients directly on a blockchain:

- Patient manage their own healthcare records: Patients owns and controls the access to their own data
  → Prevents scattering of data
  → Patients can easily transfer the data to another helthcare provider or get a complete copy of their records

Other advantages:

- Blockchain is ***decentalized*** → no single point of failure
- Security/Privacy: Data is encrypted and can only be decrypted with the patient's private key (Remember: Every node maintains a full record of the blockchain)
- Data provenance: Records are signed by the source
  → Legitimacy of records can be verified
- Immutability of medical records (except for 51% attack)

Sources: [1], [8]

Challenges

Challenges:

- No central intermediary to recoup the private key

➡ **What happens, if the patient loses its private key?**

- Users are “anonymous” by using hash values as addresses. User may still be identified through inspection and analysis of the publicly available transaction information on the blockchain network

➡ **Only pseudoanonimity on a blockchain network**

- What happens in the case of an emergency?

→ No trusted third party to authorize data access → patient has to select one/multiple representatives that can access the data on their behalf

Sources: [1], [8]

Challenges

Challenges:

- Threat of 51% attack
  - Threat can be drastically reduced, if the network is private (contrary to Bitcoin). Private means, that not everybody is allowed to join the network
- Speed and scalability:
  - The transaction time of blockchain can be long, depending on the protocol (e.g. Bitcoin, 288.000 transactions per day vs 150 million per day for Visa)
  - Remember: Every node maintains a full record of the blockchain

Sources: [1], [8]

Solutions

- **Speed and scalability**: Storing sensitive data off-blockchain and only disseminating "pointers" (eg, encrypted links) or permission information to the off-chain stored data on the blockchain
  - Of-chain storage has to be done on a decentralized network, otherwise there is a single point of failure
- New blockchain implementations provide higher transaction speed

Sources: [1], [7], [8]

Where do you see the most potential?

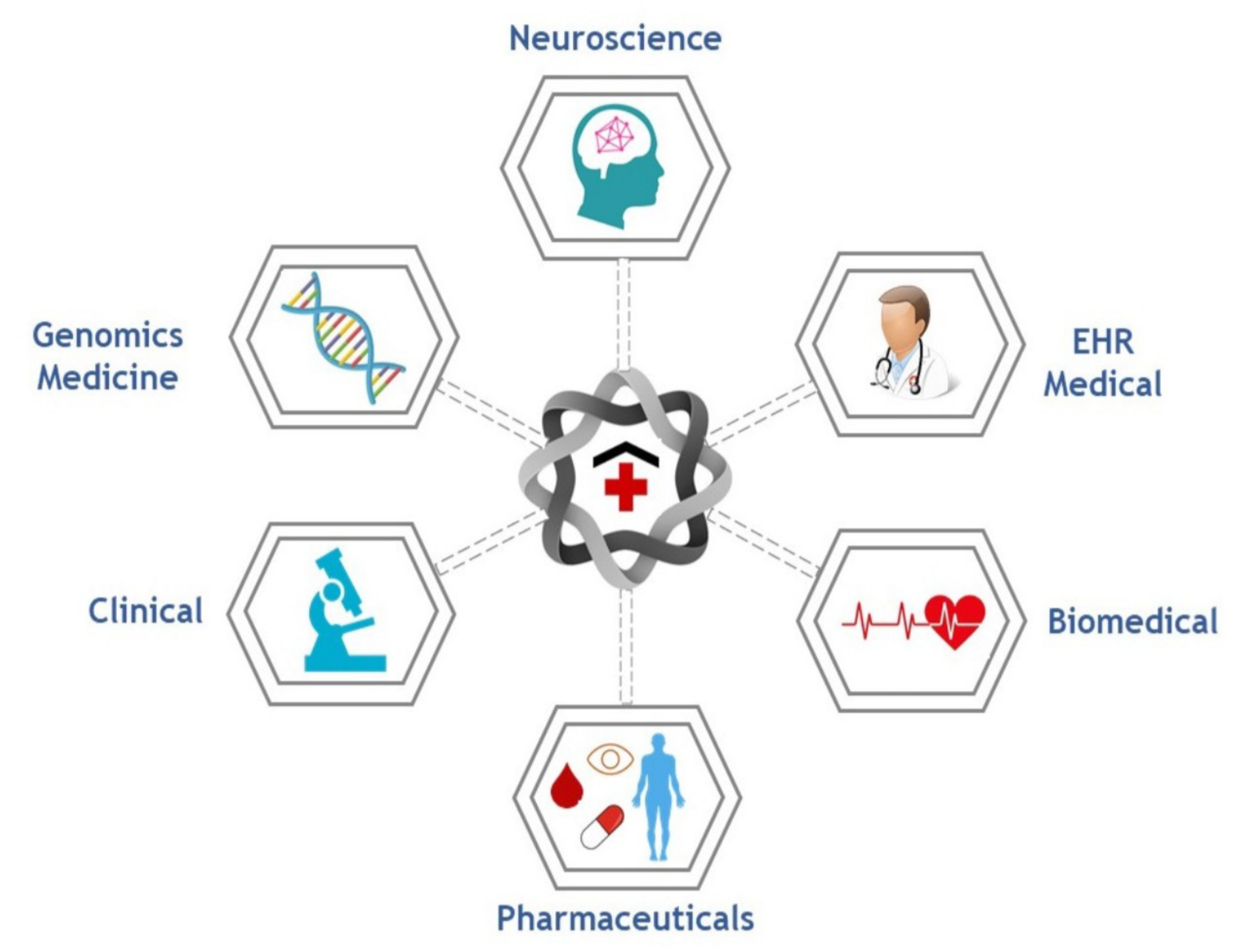

Figure 9: Applications of blockchain in halthcare [8]

Sources: [1], [8]

Literature

[1] T. Kuo, H. Kim and L. Ohno-Machado, (2017): Blockchain distributed ledger technologies for biomedical and health care applications

[2] Netcera, (visited 10.06.2021). https://blog.netcetera.com/blockchain-everything-you-need-to-know-about-the-revolutionary-technology-7579f82b05d.

[3] Asiablockchainreview, (visited 10.06.2021). https://www.asiablockchainreview.com/the-revolution-of-blockchain-in-healthcare-industry

[4] A. Schönhuth (SoSe 2021), 392157 Big Data Analytics (V)

[5] Wikipedia (visited 12.06.2021): https://en.wikipedia.org/wiki/Hash_function

[6] Networkencyclopedia (visited 12.06.2021): https://networkencyclopedia.com/hashing-algorithm/

[7] BigchainDB GmbH, (visited 14.06.2021). BigchainDB The scalable blockchain database. https://www.bigchaindb.com/

[8] A. A. Siyal et al., (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives