BLOCKCHAIN IN HEALTHCARE

AGENDA

- BASICS AND CHARACTERISTICS
- NETWORK AND BLOCKS
- CONSENSUS MODELS
- SMART CONTRACTS
- PYTHON CODE EXAMPLE
- ATTACK ON BLOCKCHAIN
- BLOCKCHAIN IN HEALTHCARE

BLOCKCHAIN INTRODUCTION

- Public digital and distributed database solution
- Provides decentralized management of transaction data
- Data sets consists of a chain of data packages (blocks)
- Each block comprises multiple transactions or information’s
- A Blockchain represents a complete ledger of transaction history
- Blocks are validated by the network using cryptographic

Source [1]

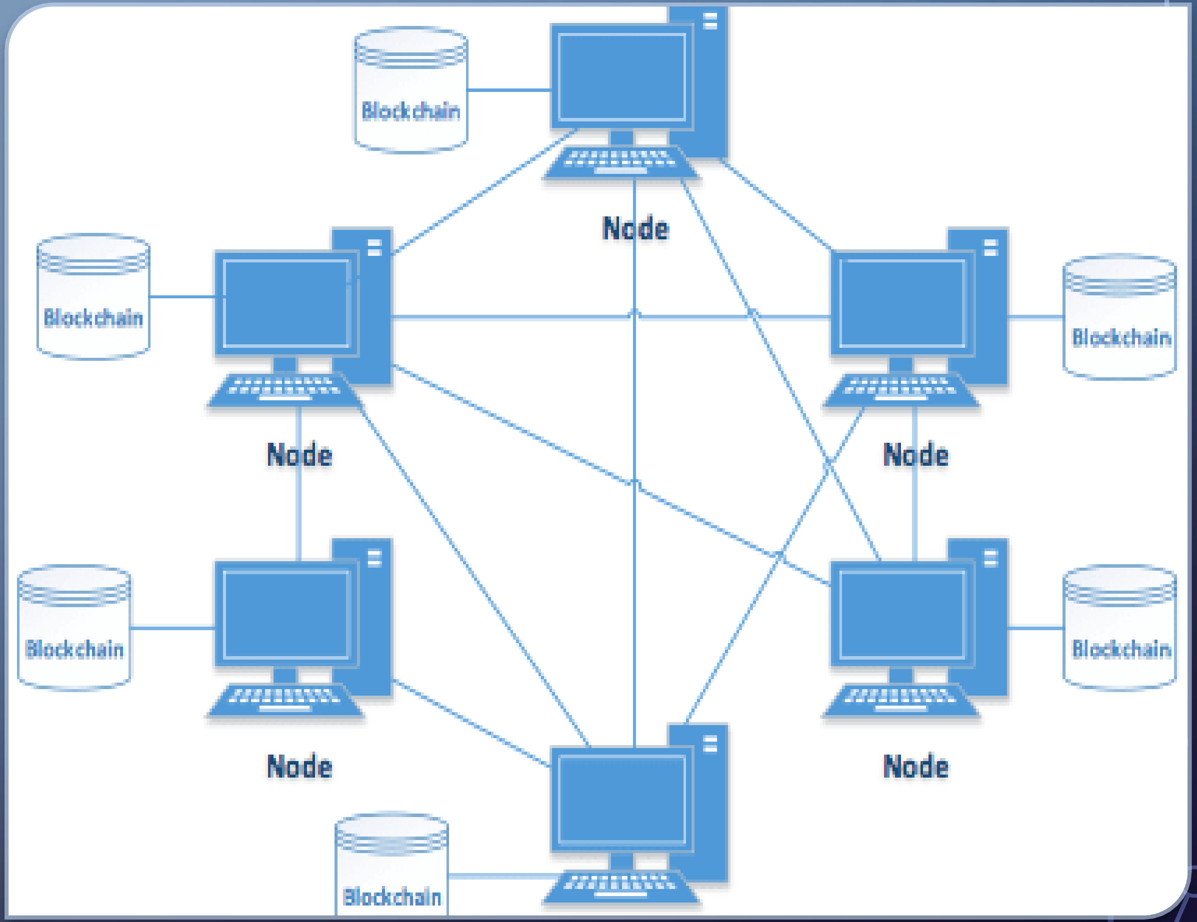
KEY CHARACTERISTICS

- LEDGER: Blockchain uses append only ledger which provide full transactional history. Old transactions and values are not overwritten (immutable)
- SECURE: Blockchain are cryptographically secure
- DECENTRALIZED: The Ledger is shared and stored among multiple participants to provide transparency across the network
- DISTRIBUTED: the blockchain is distributed through a network of nodes. By increasing the number of nodes, the network becomes more resilient to attacks

Source [2], [4]

THE BLOCKCHAIN NETWORK

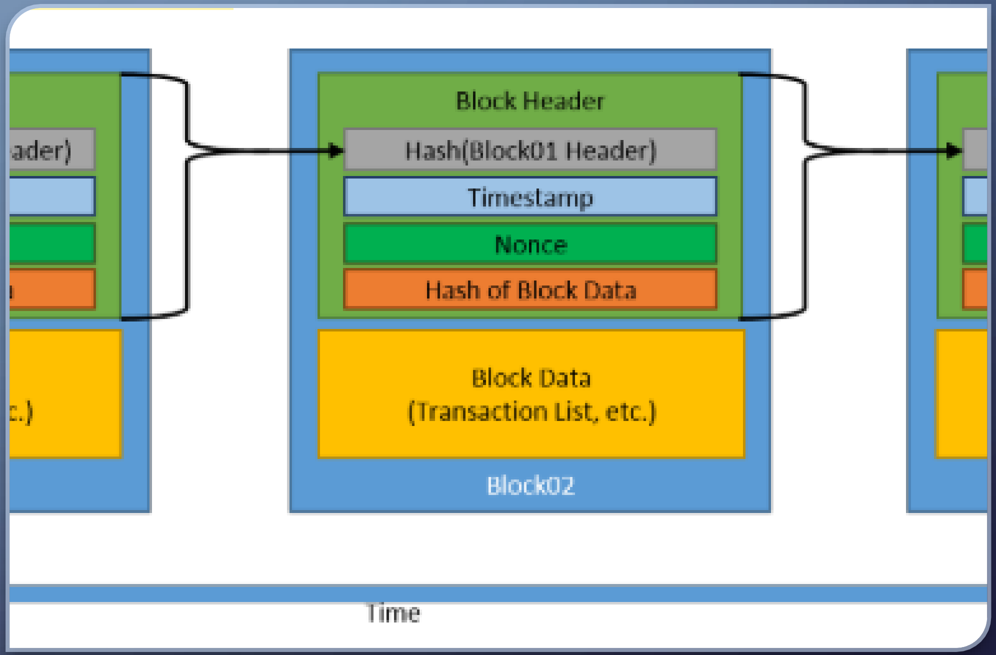
- Distributed Database
- On a Peer-to-Peer (P2P) Network
- Every Node stores a copy of the Ledger
- Every Node is on the same hierarchy level
- If consensus of nodes agree on transaction validity, a transaction is verified



Source [3]

EACH BLOCK CONTAINS:

- A Header and a Body
- The Hash value of the previous block, also called parent block (Header)
- The Nonce, a random number to verify the hash (Header)
- A Timestamp (Header)
- A Hash of the Block Data
- Transactions / Informations (Body)



Source [1],[2]

HASH FUNCTION

- Encrypted version of original string
- Hash values are unique
- A change in a block would immediately change the respective hash value
- If the majority of nodes in the network agree by a consensus mechanism on the validity of transactions in a block and on the validity of the block itself, the block can be added to the chain.
- SHA-256 commonly used

Source [2]

CONSENSUS MODELS

- Determines which user publishes the next block
- Many possible consensus models
- Generally many publishing nodes compete at the same time
- The winner earns reward in cryptocurrency and/or transaction fees

Source [2]

PROOF-OF-WORK

- Used by BITCOIN BLOCKCHAIN, called Mining
- Task that is difficult to compute but easy to verify
- Time- and resource- consuming
- Rewarded in Cryptocurrency
- First node that completes the task verifies the transactions and publishes a new block
- New block is added to the longest chain

Source [2]

PROOF-OF-WORK

- Hash digest of a block be lass than the target value
- Node change nonce to find the right number of leading “0” in the hash
- Hashing the block header many times is computationally intensive
- Difficulty changes by the number of leading zeros
- After solving the task, all other nodes verify the new block by checking the computed nonce

Source [2]

PROOF-OF-WORK EXAMPLE

```
SHA256("blockchain" + Nonce) = Hash Digest starting with "000000"
```

```
SHA256("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938
(not solved)

SHA256("blockchain1") =
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10
(not solved)

...

SHA256("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587
(solved)
```

Source [2]

PROOF-OF-STAKE

- Used by Ethereum Blockchain
- Idea: the more stake a user has invested in the system, the more they want the system to succeed
- Stake is often the amount of cryptocurrency as investment in the system
- Staked currency cant be spent
- Likelihood of creating a new block is tied to the ratio of their stake to the overall staked cryptocurrency

Source [2]

OTHER CONSENSUS MODELS

- ROUND ROBIN: Nodes take turns in creating blocks
- PROOF-OF-AUTHORITY: Nodes with proven identities stake reputation to create a new block
- PROOF-OF-ELAPSED-TIME: Random wait time for publishing nodes

Source [2]

SMART CONTRACTS

- Set of Instructions that are enforced under certain conditions
- Authenticity, conditions and necessities can be observed and approved by everyone
- Operates as an autonomous account on the blockchain
- Related transactions cause an activation and update of the contract
- Best known system is Ethereum

Source [4],[5]

CODE EXAMPLE - HASHING

```
>>> print hashlib.sha1('hello world').hexdigest()
2aae6c35c94fcfb415dbe95f408b9ce91ee846ed
```

```
import hashlib, json, time

def bhash (timestamp, details, prev_hash):
    token = json.dumps([timestamp, details, prev_hash])
    return hashlib.sha1(details).hexdigest()
```

Source [6]

CODE EXAMPLE – CREATING BLOCKS

```
class Blockchain(object):
  def __init__(self, details='new-chain'):
        self.blocks = [(time.time(), details, '')]
  def record(self, details, timestamp = None):
        timestamp = timestamp or time.time()
        prev_hash = self.blocks[−1][2]
        new_hash = bhash(timestamp, details, prev_hash)
        self.blocks.append((timestamp, details, new_hash))
```

Source [6]

CODE EXAMPLE – CREATING BLOCKS

```
>>> bc = Blockchain('A found $1')
>>> bc.record('A gives $1 to B')
>>> bc.record('B gives $1 to C')
>>> bc.record('C gives $1 to D')
```

Then we can print the blocks in the blockchain:

```
>>> print bc.blocks
[(1495941516.704196, 'A found $1', ''),
 (1495941516.704201, 'A gives $1 to B', 'a75a9227f...'),
 (1495941516.704277, 'B gives $1 to C', 'ca911be27...'),
 (1495941516.704290, 'C gived $1 to D', 'cb462885e...')]
```

Source [6]

CODE EXAMPLE – VERIFY BLOCK

```
def verify(blockchain):
    prev = blockchain.blocks[0]
    for block in blockchain.blocks[1:]:
        new_hash = bhash(block[0], block[1], prev[2])
        if block[2] != new_hash: return False
        prev = block
    return True
```

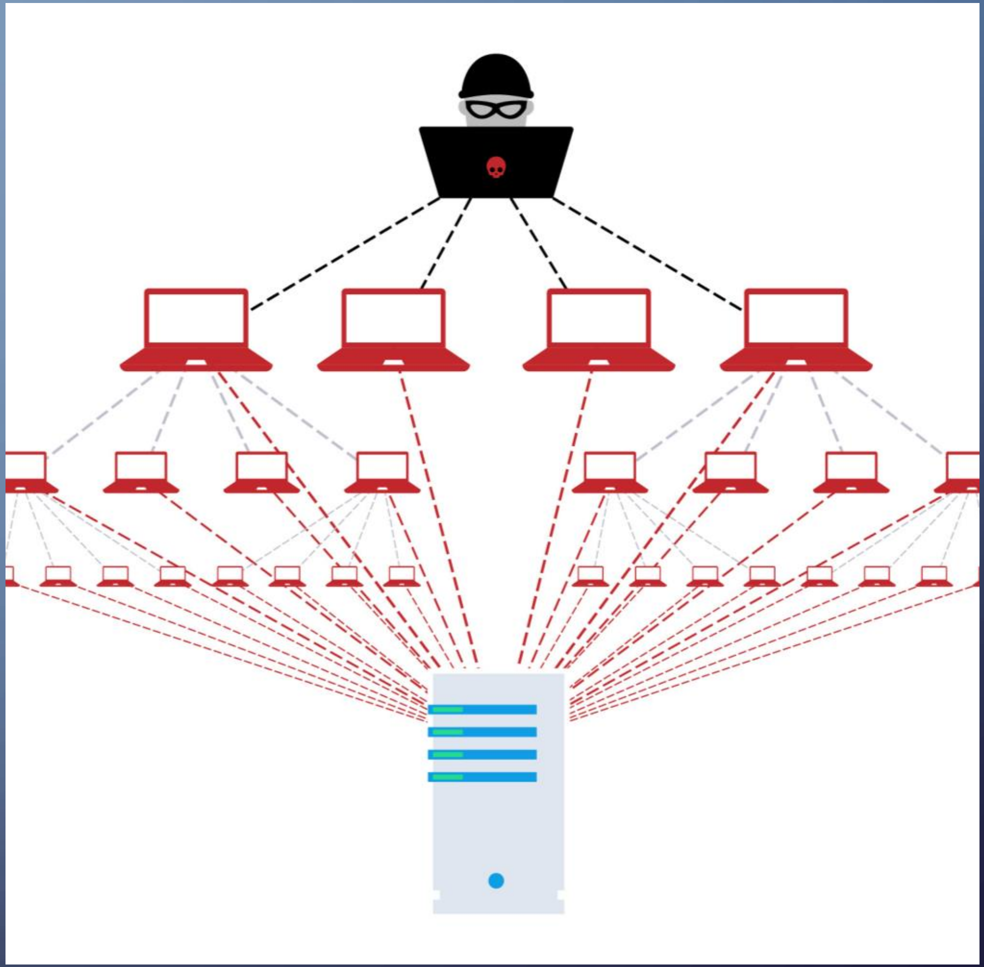
```
>>> print verify(bc)
True
```

Source [6]

THE BLOCKCHAINS

https://www.blockchain.com/explorer

ATTACK ON BLOCKCHAIN



Source [10]

ATTACK ON BLOCKCHAIN

- 51% attack
- DoS attack on miners
- Make the blockchain unusable (Layer-7-DoS)

Source [7]

ATTACK ON BLOCKCHAIN (51% ATTACK)

- Gain at least 51% of the computanional power of the whole network
- ➢ Always produce the newest block
- ➢ control the blockchain

Source [7]

ATTACK ON BLOCKCHAIN (DOS ATTACK ON MINERS)

- Denial of Service attack
- Overload a network with a lot of requests (use botnet for example)
- Attack big mining farms

➢ Easier to get 51% with less competition

Source [7]

ATTACK ON BLOCKCHAIN (LAYER-7-DOS)

- Overload the network itself with transactions
- Reward higher fees for your transaction than anyone else
- Use up all possible transactions (max. 7 per second)

➢ Noone else can use the blockchain anymore

Source [7]

APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE

- EHRs (Electronic Health Records) are often scattered

➢ Blockchain to maintain EHRs

➢ use metadata to store information

Source [8],[9]

BENEFITS OF BLOCKCHAIN

Decentralized management

- Peer to Peer
- Independently managed stakeholders collaborate
- Ceeding control to central management is not necessary

Source [8]

BENEFITS OF BLOCKCHAIN

Immutable audit trail

- Only create and read functions
- Difficult to change data or records
- Unchangeable ledger to record information

Source [8]

BENEFITS OF BLOCKCHAIN

Data provenance

- Ownership of data can only be changed by owner
- Origins of assests are traceable
- Increasing reusabilty of verified data

Source [8]

BENEFITS OF BLOCKCHAIN

Robustness and availability

- High level of data redundancy
- Preservation and continuous availability of records

Source [8]

BENEFITS OF BLOCKCHAIN

Security and privacy

- Private keys as digital signatures
- Ensuring ownership of digital assets
- Higher confidence in security of the record system

Source [8]

BENEFITS OF BLOCKCHAIN

Fraud detection

- Supply chains are vulnerable to fraudulent attacks
- Improved product traceability with blockchain

Source [9]

CHALLENGES TO OVERCOME

Security and Privacy

- Only pseudonymity
- 51% attacks
- Too much or too little access to data

Source [8],[9]

CHALLENGES TO OVERCOME

Speed and storage

- Max 7 transaction per second (due to block size limit)
- Medical data tends to be big
- Speed of record searching becomes low

Source [8],[9]

CHALLENGES TO OVERCOME

Standardization and Interoperability

- Standards for size, format, data nature
- Safety measures
- Various blockchains from different providers need to be able to talk to each other

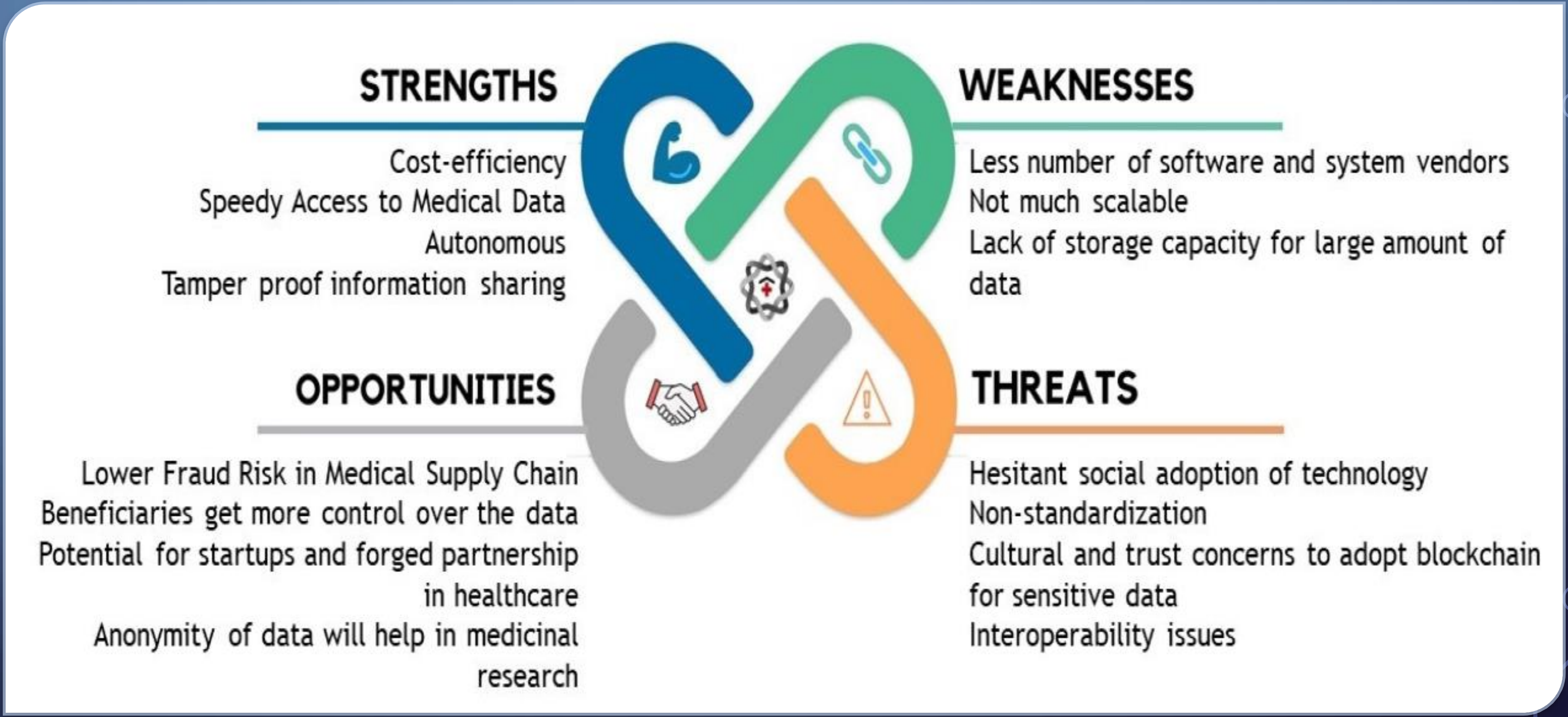
Source [8],[9]

CHALLENGES TO OVERCOME

Social challenges

- Still new technologie
- Untrusted by many
- Need to convince „traditionalists“

Source [9]


STRENGTHS
Cost-efficiency
Speedy Access to Medical Data
Autonomous
Tamper proof information sharing
WEAKNESSES
Less number of software and system vendors
Not much scalable
Lack of storage capacity for large amount of data
OPPORTUNITIES
Lower Fraud Risk in Medical Supply Chain
Beneficiaries get more control over the data
Potential for startups and forged partnership in healthcare
Anonymity of data will help in medicinal research
THREATS
Hesitant social adoption of technology
Non-standardization
Cultural and trust concerns to adopt blockchain for sensitive data
Interoperability issues

Source [9]

SOURCES

[1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[2] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” 2019, doi: 10.6028/NIST.IR.8202.

[3] B. Koteska and A. Mishev, “Blockchain Implementation Quality Challenges : A Literature Review Blockchain Implementation Quality Challenges : A Literature Review,” no. September, 2017.

[4] H. I. Ozercan, A. M. Ileri, E. Ayday, and C. Alkan, “Realizing the potential of blockchain technologies in genomics,” *Genome Res.*, vol. 28, no. 9, pp. 1255–1263, 2018, doi: 10.1101/gr.207464.116.

[5] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *J. Am. Med. Informatics Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017, doi: 10.1093/jamia/ocx068.

[6] M. Di Pierro, “What Is the Cloud? - What Is the Cloud?,” vol. 1, no. October, p. 2, 2017, [Online]. Available: http://www.ecrr.org/River-Restoration/Flood-risk-management/Healthy-Catchments-managing-for-flood-risk-WFD/What-is-the-WFD%0Ahttps://learning.oreilly.com/library/view/what-is-the/9781492052913/titlepage01.html.

SOURCES

[7] https://www.youtube.com/watch?v=_IXqlnd4WeE

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

[9] A. A. Siyal , A. Z. Junejo , M. Zawish , K. Ahmed, A. Khalil and G. Soursou (2019), Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives

[10] https://academy.horizen.io/technology/advanced/attacks-on-blockchain/