Ayush Garg

Blockchain Research

What is blockchain?

Blockchain is an electronic transaction ledger that can be openly shared among different users and that creates an unchangeable record of their transactions, each one time-stamped and linked to the previous one.

Summary:

- Transaction ledgers
- Immutable
- Secured by cryptography
- Consensus-driven
- Decentralized
- Trustless
- Can be made public

- A blockchain is an append-only transaction ledger which means is that new information can be added to the ledger, but the previous information, stored in blocks, cannot be edited, adjusted or changed.[1]
- This is accomplished by using cryptography to link the contents of the newly added block with each block before it, such that any change to the contents of a previous block in the chain would invalidate the data in all blocks after it. [1]
- Blockchains are consensus-driven. A large number of computers are connected to the network, and to reduce the ability for an attacker to maliciously add transactions on the network, those adding to the blockchain must compete to solve a mathematical proof.
- The results are shared with all other computers on the network. The computers, or nodes, connected to the network must agree on the solution.[1]
- Blockchain is decentralized, meaning that no single entity can take control of the information on the blockchain..[1]
- The transactions recorded in the chain can be publicly published and verified, such that anyone can view the contents of the blockchain and verify that events that were recorded into it actually took place. [1]

What are the main advantages/disadvantages of blockchain technology?

Advantages

- ➔ Decentralized
  - ◆ No single entity can take control of the information on the blockchain. Its network lacks centralized points of vulnerability that computer hackers can exploit.

- Durability, reliability and longevity
  - Due to the decentralized networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks
- Process integrity
  - Each transaction is recorded and time-stamped, creating an immutable transaction trail that is transparent, unalterable and permanent.
- Traceability
  - The way the information in disseminated across the blockchain makes it simple to find and solve problems efficiently, should they arise. It also creates a de facto, irreversible audit trail.
- Transparency and immutability
  - Changes to public blockchain are publicly viewable by all parties creating transparency
  - All transactions are immutable, meaning they cannot be altered or deleted.
- Security
  - Each user has their own key to verify identity. The block encryption in the chain makes it much tougher for hackers to disrupt than traditional setups.
  - Users are in control of all their information and transactions.
- High quality data
  - Blockchain data is complete, consistent, timely, accurate and widely available [3][4]

Disadvantages

- Performance
  - Signature verification. Every blockchain transaction must be digitally signed using a cryptography scheme. This is necessary because transactions propagate between nodes in a peer-to-peer fashion, so their source cannot otherwise be proven. By contrast, in centralized databases, once a connection has been established, there is no need to individually verify every request that comes over it.
  - Redundancy. The total amount of computation that a blockchain requires is a lot. Whereas centralized databases process transactions once, in a blockchain they must be processed independently by every node in the network. So lots more work is being done for the same end result.
- Large energy consumption
  - Blockchain networks require substantial amounts of computing power and energy to function
- Cost
  - Blockchain offers tremendous savings in transaction costs and time but the high initial capital costs could be a deterrent.

How is blockchain technology used for record-keeping?

Use of blockchain technology for the creation of trustworthy and transparent records is identified as a unique feature of blockchain technology.

Due to the inherent security of blockchain networks against alteration and fraud, the technology readily lends itself to the recording of events and the management of records.

Recordkeeping uses of blockchain:

- Identity management
  - Identity records, like birth certificates, passports, drivers' licenses and marriage certificates
- Intellectual Property
  - Individuals and organizations adopting the blockchain hope to offer trustworthy registration and verification services for intellectual property.
- Notarization
  - The blockchain is also being used as a substitute for notarization services to verify the authenticity of documents
- Digital signature
  - Digital signatures facilitate the signing of documents, such as contracts, online.
- Privacy Protection
  - Privacy-preserving blockchain solutions take advantage of the fact that documents that are hashed on the blockchain are encrypted. If a user wants to grant someone else the right to view some specific records in decrypted form, but not all of them, they can create a different key for each document
- Provenance tracking
  - The tracing of provenance-- the origins of an asset-- is another interesting recordkeeping area where blockchain technology may be very helpful.
  - The blockchain can also be used to "combine supply chain management with the Internet of Things to tag any asset with a smart chip that communicates its provenance, ownership, warranties, or special information."
- Smart contracts
  - Smart contracts are computer algorithms that embed the terms and conditions of a contract as source code into a blockchain. It allows third parties unknown to each other to enter into contractual relationships at a low cost due to the trust that is built into the blockchain as an authenticated data structure.
  - It is a contract, or an agreement, between parties involved in a transaction that holds each party responsible.
  - Smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

    - Smart contracts implemented using blockchain technology could automate the execution of prior authorization by pulling relevant background data from the electronic medical record (EMR) and using the data to execute a decision on an authorization through a rules engine. [5]

How can blockchain technology be used in a healthcare setting?

Why are private consortium blockchains necessary?

- In a public blockchain network, anyone can transact on the network, actors on the network are pseudo-anonymous and untrusted, and anyone can add nodes to the network.
- In a private consortium blockchain network, member identities and nodes are known and controlled. Actors are often equally mature, with robust and highly controlled IT environments, security policies, and other enterprise characteristics.
- Organizations in this market transact data, and HIPAA limits how that information can be shared. Only authorized organizations and individuals should have access to PHI or Protected Healthcare Information.
- As a well-defined group of trusted entities who benefit from and are authorized to share patient data, healthcare networks can successfully utilize these private blockchains to solve many of their business goals while remaining compliant with applicable regulations and data protection laws.[7]

Blockchain technology ensures sensitive medical data is decentralized, confidential, robust against deletion or alteration, yet able to be shared and accessed with ease and rapidity.

- Shortcomings of the current healthcare system
    - Healthcare data today is localized to provider networks, which leads to the scattering and loss of data as a patient moves between healthcare providers.
    - Hospitals spend lots of time and money setting up involved information storage and management systems, which are non-shareable between providers, inaccessible to patients, and vulnerable to data loss and alteration.
    - Doctors and patients are often unable to obtain the complete and chronological picture of the care they provide and receive, putting lives at risk.
- A blockchain network will generate large, decentralized database of indexed and accurate medical data which will be invaluable to public health researchers, and a means for patients to consensually provide their data for these purposes.
- Provides fast access to patient data in situations where such access may constitute a matter of life-and-death.
- Creates a permanent, time-stamped record of transactions, preventing record-related malpractice and providing a verifiable history of care.

- Patients can easily view their own records, as well as provide access and sharing permissions to different providers
- The issue of privacy can be addressed by making the blockchain a structure where only pre-approved, known users are allowed read access to the distributed ledger[13]
- Millions of dollars worth of software management tools are used on patient identity management today, which could be reduced or replaced by moving this effort to a blockchain.[6]
- Concerns
    - David Houlding, Director of Healthcare Privacy & Security at Intel believes that personal health information, which he defines as anything that can locate, contact, or identify an individual, should be kept off-chain. If a patient no longer wants to participate in a network or wants their data forgotten, their off-chain information can be removed essentially, de-identifying the patient from a blockchain. Another consideration mentioned by David are the data retention laws, like HIPAA, that sometimes conflict with patient requests for deletion of information.[5]
    - Competitive concerns with assets on a blockchain. If you take a network of hospitals and create a private blockchain among them, now each hospital will potentially be able to see how many customers the other hospitals have, the frequency of patient visits, and other information hospitals consider proprietary today. [5]

How has the blockchain timing performance improved with new algorithms?

An important constraint with blockchains is its performance. This speed cannot manage millions of transactions per second and is therefore a limiting factor. By batching transactions into blocks, the throughput rate can be boosted but at the cost of introducing latency.[7]

Waves-NG

- A next-generation technology and consensus algorithm designed and based on Bitcoin-NG
- Increases effective bandwidth, the speed of block creation, and the speed of processing trading
- Allows for conducting microtransactions without any delay, withstanding high loads, and enables blockchains to minimize latency and maximize throughput.
- Capable of processing hundreds of thousands of transactions within a very short timespan. On December 26, 2017, the Waves blockchain protocol cleared 330,000 transactions, 170,000 of which were processed within 20 minutes. According to the Waves team, it is currently possible to process up to 10 million transactions per day. [10]
- Waves' uses an approach called proof-of-stake which further improves speed.

In the proof-of-work algorithm, miners are rewarded for solving mathematical problems with the goal of validating transactions and creating new blocks.

With proof of stake, the creator of a new block is chosen in a pseudo-random way, depending on the user's wealth, also defined as stake, which in most contexts is the number of cryptocurrency units owned by the user.

Vostok

- Private blockchain platform and system integrator that implements Waves-NG
- Also uses proof-of-stake and enables public institutions and large enterprises anywhere in the world to enhance their existing systems
- According to Vostok, these organizations will be able to improve the security, data storage, transparency and stability of their systems.

Blockchain technology has prowess with integrity, availability, and enabling secure, targeted collaboration across a network of healthcare organizations. Microsoft provides technologies to help healthcare organizations who have an interest in implementing blockchain-driven solutions.

Azure Blockchain Workbench

- Rapid prototyping framework that enables any healthcare organization to quickly prototype a use case, spin up blockchain nodes, and deploy through the Microsoft Azure cloud avoiding the need for any in-house hardware.[7]
- A key goal is to empower organizations to quickly learn, rapidly prototype and deploy, test, and incrementally improve their understanding and application of blockchain technology.[7]
- It is not a blockchain platform in and of itself, it is a framework that projects outputs into existing blockchains including Ethereum Enterprise, Hyperledger Fabric, and R3 Corda.[7]
- It is focused on private consortium blockchains, which are the most relevant to a healthcare setting. [7]

Coco Framework

- A blockchain platform itself also directed at private consortium blockchains
- An open-source system that enables high-scale, confidential blockchain networks. It provides a means to accelerate production adoption of blockchain technology by using trusted execution environments (TEEs) such as Intel's SGX and Windows Virtual Secure Mode (VSM), enabling the creation of a trusted network of physical nodes on which to run a distributed ledger.[12]

Blockchain issues that Coco Framework is built to address and solve[8]:

- Throughput and latency – The framework uses a different consensus model assuming a higher degree of trust between organizations which enables higher block throughput rates, thereby addressing the performance limitation

- Confidentiality – The Coco framework offers richer, more flexible, business-specific confidentiality models. It protects the confidentiality and integrity of core code and data running inside blockchain nodes.
- Distributed Governance – With a private blockchain there needs to be adequate controls over the distributive nature of blockchain. Coco addresses this with network policy management through distributed governance.
- Non-Deterministic Transactions – To enhance the capabilities of Blockchain, Coco extends support for non-deterministic transactions to be used within the system.
- Reduced energy usage – Coco improves energy consumption by eliminating computationally intensive consensus algorithms, such as proof of work.

Coco is a distributed network of trusted validating nodes (VNs) that each accept transactions and participate in the network's consensus algorithm, as well as run the Coco Framework and the integrated blockchain protocol. Depending on the chosen consensus algorithm, one or some VNs process transactions and execute smart contract code.

Coco does not require proof-of-work or proof-of-stake algorithms. It is designed to support pluggable consensus algorithms with initial plans to integrate Paxos-like and Caesar consensus algorithms. However, it can be built with other consensus algorithm to achieve efficient agreement and maximum throughput.

Paxos Consensus [12]

- With Paxos consensus, one VN is elected the leader. All other VNs are followers that simply accept transactions and forward them to the leader for processing.
- After the leader processes the transaction, thanks to the use of TEEs in Coco, followers can simply accept the transaction results from the leader.
- Paxos consensus is highly efficient for a smaller number of nodes, and are traditionally limited by the median latency between nodes.
- As such, the suitability of Paxos-like consensus algorithms for a Coco network is dependent on the number of VNs—which, in turn, depends on the number of actors in the consortium and the number of nodes per actor.

Caesar Consensus [12]

- A new consensus algorithm for architecting secure and efficient consortium blockchain networks. It leverages the cryptographic properties of a blockchain to enable nodes in the blockchain network to reach consensus on a valid ledger.
- In the system, follower nodes store small bits of cryptographic information within the distributed ledger to enable distributed consensus, which also tracks progress and keeps the leader accountable.

Terms [12]

Blockchain: A blockchain is a type of distributed ledger, cannot be changed without detection, digitally recorded data in packages called blocks. Each block is then ‘chained’ to the next block, using a cryptographic hash. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions. This can maintain an ever-expanding list of data, each referring to previous items on the list, creating an incorruptible digital record. Blockchain was initially introduced as Bitcoin's underlying technology.

Cryptography: Discipline that embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof

Mining: Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain.

Peer-to-Peer: Pertaining to a form of distributed processing, in which the front-end and backend of a conversation switch control between themselves. It is communication between equals.

Smart Contract: A set of business terms that are embedded into a blockchain and executed with transactions. A smart contract can also include a digital representation of a set of business rules and defines conditions under which transfers occur.

Transaction: A request by a transactor to the blockchain to execute a function on the ledger.

Transaction Block: A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

Links to Sources

[1]
https://www.forbes.com/sites/forbesagencycouncil/2018/04/05/what-is-blockchain-and-what-can-businesses-benefit-from-it/#76dce7be675f

[2] https://blockgeeks.com/guides/what-is-blockchain-technology/

[3] https://www.e-spincorp.com/2017/11/24/pros-and-cons-of-blockchain-technology/

[4] https://www.mimics.com/news/entry/the-pros-and-cons-of-blockchain-technology

[5]
https://www.medgadget.com/2018/05/healthcare-on-the-blockchain-day-1-tech-primer-use-cases-privacy.html

[6]
https://www.medgadget.com/2018/05/healthcare-on-the-blockchain-day-2-drug-management-machine-learning-private-vs-public-blockchains.html

[7]https://www.medgadget.com/2018/06/a-conversation-with-blockchain-thought-leader-david-houlding-microsoft-principal-healthcare-program-manager.html

[8] https://buildazure.com/2017/11/22/introducing-microsoft-coco-framework-for-blockchain/

[9]
https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf

[10]https://www.forbes.com/sites/rogeraitken/2017/11/08/waves-set-to-become-fastest-decentralized-blockchain-platform-globally/#4a23c4fe38b6

[11]https://www.enterprisetimes.co.uk/2018/06/25/vostok-a-universal-blockchain-enterprises-and-public-bodies/

[12]
https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html

[13] https://www.iris.co/IrisWhitepaper.pdf

Other Links:

- https://arxiv.org/pdf/1712.03659.pdf
- https://arxiv.org/pdf/1703.04057.pdf
- https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
- https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html
- http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
- https://www.iris.co/IrisWhitepaper.pdf
- https://howtotoken.com/ico/how-to-write-a-smart-contract-for-your-ico-an-ultimate-guide/#contracts
- https://blockgeeks.com/guides/smart-contracts/
- https://www.capgemini.com/wp-content/uploads/2017/07/blockchain-a_healthcare_industry_view_2017_web.pdf