A Report on Block Chain

A new technology is redefining the way we transact. If that sounds incredibly far-reaching, that's because it is. Blockchain has the potential to change the way we buy and sell, interact with government and verify the authenticity of everything from property titles to organic vegetables.It combines the openness of the internet with the security of cryptography to give everyone a faster, safer way to verify key information and establish trust. Blockchain technology has shown its considerable adaptability in recent years as a variety of market sectors sought ways of incorporating its abilities into their operations. While so far most of the focus has been on the financial services industry, several projects in other service related areas such as healthcare show this is beginning to change. Numerous starting points for Blockchain technology in the healthcare industry are the focus of this report. With examples for public healthcare management, user-oriented medical research and drug counterfeiting in the pharmaceutical sector, this report aims to illustrate possible influences, goals and potentials connected to this disruptive technology.

Types of blockchains

Currently, there are three types of blockchain networks — public blockchains, private blockchains and consortium blockchains.

Public blockchains

A public blockchain has absolutely no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm.

Some of the largest, most known public blockchains are the bitcoin blockchain and the Ethereum blockchain.

Private blockchains

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

Consortium blockchains

A consortium blockchain is often said to be semi-decentralized. It, too, is permissioned but instead of a single organization controlling it, a number of companies might each operate a node on such a network. The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

Structure:

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a *value-exchange protocol*. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blocks:

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

Block time:

The *block time* is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds.By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is 10 minutes.

Uses:

Blockchain technology can be integrated into multiple areas. The primary use of blockchains today is as a distributed ledger for cryptocurrencies, most notably bitcoin. There are a few operational products maturing from proof of concept by late 2016.

As of 2016, some observers remain skeptical. Steve Wilson, of Constellation Research, believes the technology has been hyped with unrealistic claims. To mitigate risk, businesses are reluctant to place blockchain at the core of the business structure.

Cryptocurrencies

Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain. On May 8, 2018 Facebook confirmed that it is opening a new blockchain group which will be headed by David Marcus who previously was in charge of Messenger. According to The Verge Facebook is planning to launch its own cryptocurrency for facilitating payments on the platform.

Smart contracts:

Blockchain-based smart contracts are proposed contracts that could be partially or fully executed or enforced without human interaction.One of the main objectives of a smart contract is automated escrow. An IMF staff discussion reported that smart contracts based on blockchain technology might reduce moral hazards and optimize the use of contracts in general. But "no viable smart contract systems have yet emerged." Due to the lack of widespread use their legal status is unclear.

Financial services

Major portions of the financial industry are implementing distributed ledgers for use in banking, and according to a September 2016 IBM study, this is occurring faster than expected.

Banks are interested in this technology because it has potential to speed up back office settlement systems.

Banks such as UBS are opening new research labs dedicated to blockchain technology in order to explore how blockchain can be used in financial services to increase efficiency and reduce costs.

Berenberg, a German bank, believes that blockchain is an "overhyped technology" that has had a large number of "proofs of concept", but still has major challenges, and very few success stories.

Blockchain with video games

Some video games are based on blockchain technology. The first such game, *Huntercoin*, was released in February, 2014 Another blockchain game is *CryptoKitties*, launched in November 2017. The game made headlines in December 2017 when a cryptokitty character - an-in game virtual pet - was sold for US$100,000. *CryptoKitties* illustrated scalability problems for games on Ethereum when it created significant congestion on the Ethereum network with about 30% of all Ethereum transactions being for the game.

Cryptokitties also demonstrated how blockchains can be used to catalog game assets (digital assets)

The Blockchain Game Alliance was formed in September 2018 to explore alternative uses of blockchains in video gaming with support of Ubisoft and Fig, among others.

Supply chain

There are a number of efforts and industry organizations working to employ blockchains in supply chain logistics and supply chain management.

The Blockchain in Transport Alliance (BiTA) works to develop open standards for supply chains.

Everledger is one of the inaugural clients of IBM's blockchain-based tracking service.

Walmart and IBM are running a trial to use a blockchain-backed system for supply chain monitoring — all nodes of the blockchain are administered by Walmart and are located on the IBM cloud

Hyperledger Grid develops open components for blockchain supply chain solutions.

Other uses

Blockchain technology can be used to create a permanent, public, transparent ledger system for compiling data on sales, tracking digital use and payments to content creators, such as wireless users or musicians. In 2017, IBM partnered with ASCAP and PRS for Music to adopt blockchain technology in music distribution. Imogen Heap's Mycelia service has also been proposed as blockchain-based alternative "that gives artists more control over how their songs and associated data circulate among fans and other musicians.

New distribution methods are available for the insurance industry such as peer-to-peer insurance, parametric insurance and microinsurance following the adoption of blockchain.
The sharing economy and IoT are also set to benefit from blockchains because they involve many collaborating peers. Online voting is another application of the blockchain.

Other designs include:

- Hyperledger is a cross-industry collaborative effort from the Linux Foundation to support blockchain-based distributed ledgers, with projects under this initiative including Hyperledger Burrow (by Monax) and Hyperledger Fabric (spearheaded by IBM)
- Quorum – a permissionable private blockchain by JPMorgan Chase with private storage, used for contract applications
- Tezos decentralized voting.
- Proof of Existence is an online service that verifies the existence of computer files as of a specific time·

A Digital Record

At its heart, a blockchain is a record of transactions, like a traditional ledger. These transactions can be any movement of money, goods or secure data—a purchase at a supermarket, for example, or the assignment of a government ID number.

Secure

Blockchain is designed to store information in a way that makes it virtually impossible to add, remove or change data without being detected by other users.

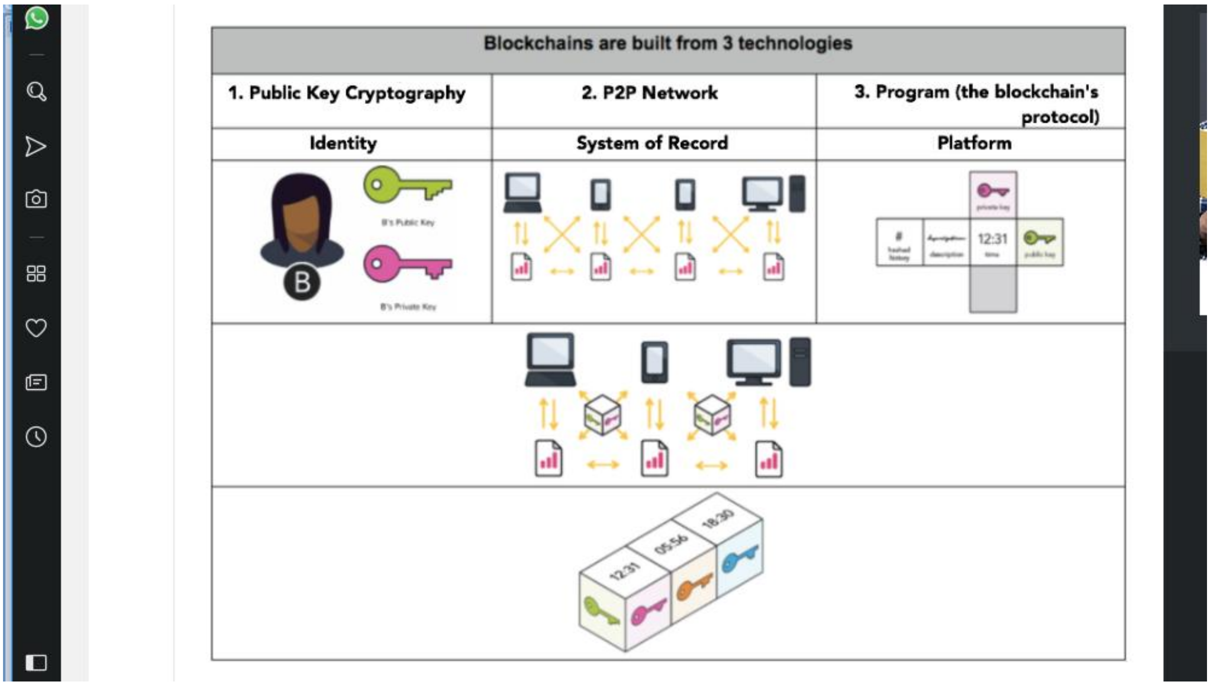
Decentralized

Today, transactions are verified by a central authority—like a government or a credit card clearinghouse. Blockchain applications could replace these centralized systems with decentralized ones, where verification comes from the consensus of multiple users.

How does it work?

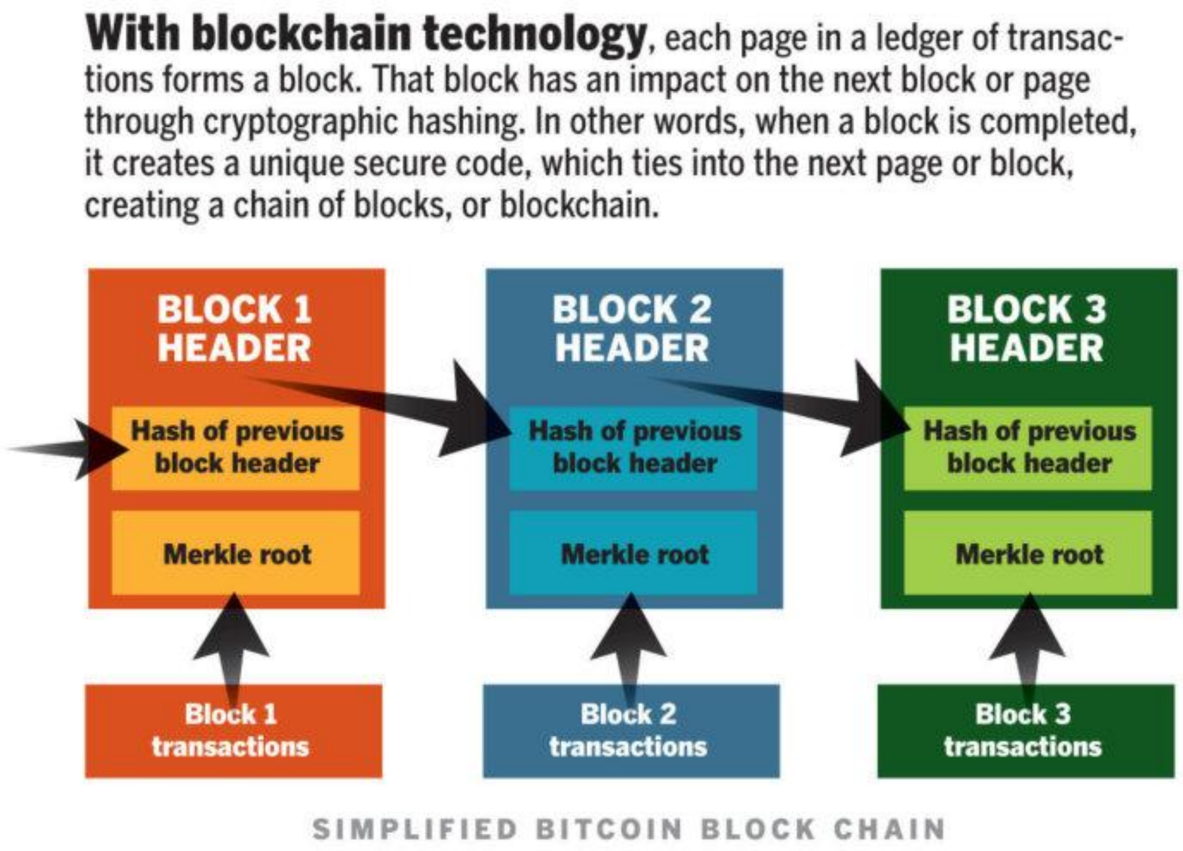
A blockchain needs to do two things: gather and order data into blocks, and then chain them together securely using cryptography.

.



Blockchains are built from 3 technologies		
1. Public Key Cryptography	2. P2P Network	3. Program (the blockchain's protocol)
Identity	System of Record	Platform

When a new transaction or an edit to an existing transaction comes in to a blockchain, generally a majority of the nodes within a blockchain implementation must execute algorithms to evaluate and verify the history of the individual blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.



With blockchain technology, each page in a ledger of transactions forms a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.

SIMPLIFIED BITCOIN BLOCK CHAIN

Blockchain technology backs up Bitcoin and other cryptocurrencies to this day, but there's been a recent groundswell of interest from a variety of industries in making distributed ledger technology work, especially in business. Here's a primer on what blockchain technology is, how it works, and where it is showing the most promise in business.

What is a blockchain?

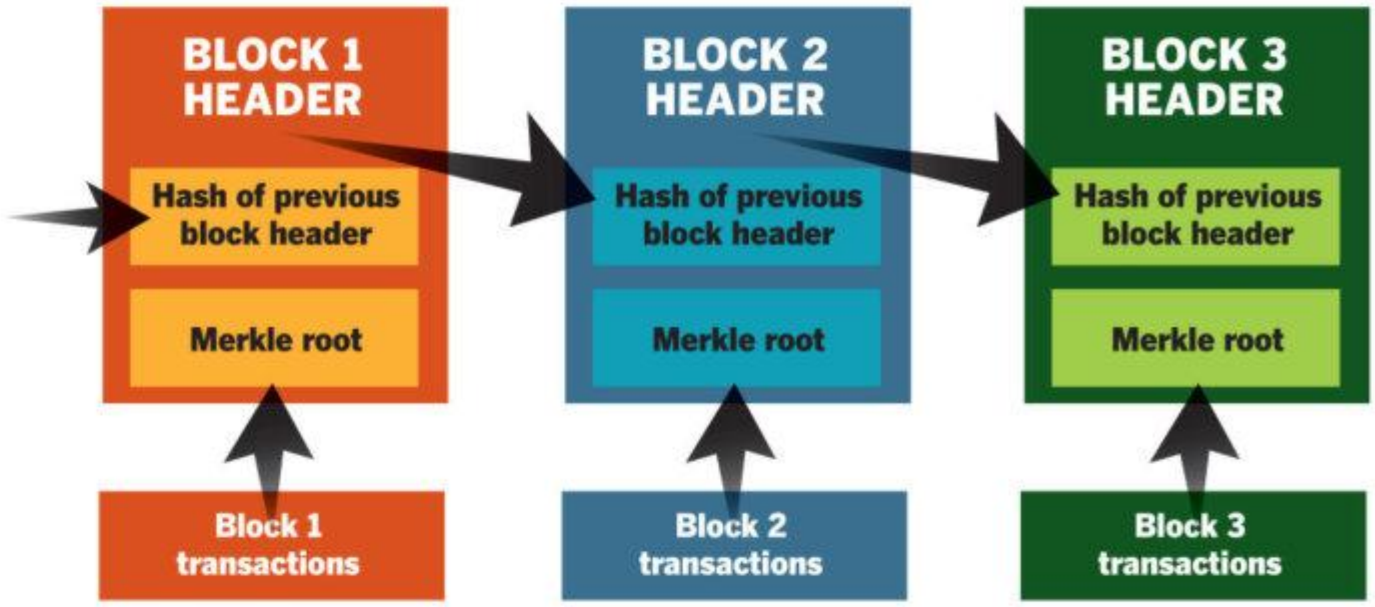
A blockchain is the structure of data that represents a financial ledger entry, or a record of a transaction. Each transaction is digitally signed to ensure its authenticity and that no one tampers with it, so the ledger itself and the existing transactions within it are assumed to be of high integrity.

The real magic comes, however, from these digital ledger entries being distributed among a deployment or infrastructure. These additional nodes and layers in the infrastructure serve the purpose of providing a consensus about the state of a transaction at any given second; they all have copies of the existing authenticated ledger distributed amongst them.

How do blockchains work?

When a new transaction or an edit to an existing transaction comes in to a blockchain, generally a majority of the nodes within a blockchain implementation must execute algorithms to evaluate and verify the history of the individual blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.

With blockchain technology, each page in a ledger of transactions forms a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.



SIMPLIFIED BITCOIN BLOCK CHAIN

How can blockchains be structured?

Blockchains can be configured to work in a number of ways that use different mechanisms to achieve consensus on transactions and, in particular, to define known participants in the chain and exclude everyone else. The largest example of blockchain in use, Bitcoin, employs an anonymous public ledger in which anyone can participate. For more private uses of blockchain among a smaller number of known actors, many organizations are deploying permissioned blockchains to control who participates in transaction activity.

What are the benefits of blockchains?

Blockchain is attractive to a number of different constituencies for a variety of reasons, including the following:

- The lack of a requirement for a central authority makes it an ideal ledger and settlement solution for joint ventures and affiliate relationships that are generally made on an equal or 50/50 footing without a provision for an arbitrator or manager. Indeed, having the computers verify transactions and settle them eliminates the need for clearinghouses and other settlement agents, providing disintermediation in a business arrangement and generally reducing costs while improving the speed at which transactions can be made, verified, settled, and recorded.

- The digital signatures and verifications make it difficult to envision a scenario wherein a bad actor could cause fraud and introduce problems that are costly to remove and resolve. The cryptographic integrity of the whole pending transaction, as well as examination by multiple nodes of the blockchain architecture, protect against threats and malevolent use of the technology. (It is important to note that this security protection has largely been untested in the marketplace and, while strong on a theoretical basis, questions remain about how well the protections will hold up in the reality of the digital economy we live in today.)

- The concept of blockchain works really well at tracking how assets move through a supply chain, through certain vendors and factories to transmission and transportation lines and into their final locations.

What are the downsides of blockchain technology:

- The biggest problem with blockchain technology now is that it is hard to apply, mainly because, as is typical with open source projects, there are numerous projects each with their own teams and ideals. Marrying all of the functionality into a practical application is difficult. “The only thing that gives me pause about Blockchain is the community that builds the code,” says Matt Reynolds, blockchain application development expert. “Bitcoin is open source, but the team that manages it do not behave in the way you’d ideally like FOSS maintainers to maintain. They behave more like an ‘answerable to no one’ proprietary software team, and that’s not good for anyone using Bitcoin’s blockchain implementation in their own projects.”