Block Chain Technology

Yashasvi Raje
Dept. of Computer Science, Lovely Professional University
Phagwara, Punjab (India) -144411
Reg. No. 11610025, Roll no. 33, K1625

Abstract

This term paper aims at giving an in-depth understanding of the Block Chain technology. The Block Chain is rapidly becoming one of the most popular technologies around the world. The building block of the crypto-currencies around the world, block chain is claimed to be one of the most secure transaction technology by experts. Blockchain came into origin in 2008, as a public ledger of transactions which proved invaluable for the most popular cryptocurrency, Bitcoin. The invention of Block Chain for Bitcoin made it the first cryptocurrency to solve the double spending problem eliminating the need for trusted authority and central server. Block Chain has inspired other applications as well, the public block chains are being rapidly adopted for various popular cryptocurrencies and the private block chains are leaving their mark in industrial transactional both intra and inter organisations as well.

The fundamental basis is that the Blockchain manages a system of creating a distributed consensus in digital online world, allowing the involved parties the certainty of the happening or occurrence of a transactional event by creating a no refutable record in that digital public ledger. It creates many novel avenues for the evolution of a democratic, transparent and scalable digital economy from the current centralised version. As that happens, this disruptive technology will have made a mark in the world arena with tremendous opportunities and a revolution of its kind in its native domain.

Introduction

A **Blockchain,** initially called a Block Chain, is a rapidly expanding list of records which are termed as blocks, and are linked together using cryptography. Each single block contains a cryptographic hash of the previously linked block, a timestamp of the transaction and the data of the transaction. The hash is generally represented as the merkle tree root hash.

The Blockchain is designed in such a way to disable the modification of data stored in each block. It can be simplified as an "open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".

For being used as a distributed ledger, a Blockchain is usually maintained by a peer-to-peer network, and collectively adheres to a protocol for inter-node communication and validation of new blocks.

One of the unique selling points of Blockchain is precisely that, once recorded, the data of any particular block can never be altered after the completion of transaction without the alterations of all the other blocks after that particular block in the Blockchain, therefore requiring the consensus of the network majority. Hence, any changes made in the Blockchain can only be made if all the parties are aware of it and consent to the change. Despite being highly secure, Blockchains are not unalterable; the security is augmented by a distributed computing system with a high Byzantine Fault Tolerance. Therefore, Blockchain can be signified by decentralised consensus.

Concept

Currency transactions between two parties; people and/or organisations are often done through a trusted mediator or third party to authenticate and verify the genuineness of the transactions. Making a digital currency transfer needs a bank or a credit card provider as a middleman to complete the transaction. The bank or the credit card provider charge fee for the services rendered. The same concept applies for other domains as well, e.g. - games, music, software, etc. The normal transactions thus, are

typically centralized and all the data and information are controlled and managed by the third party instead of the two parties actually involved in the deal.

The goal of Blockchain technology is to solve this issue and create a decentralised environment where third party involvement is not required to complete a transaction.

According to the article "Where Is Current Research on Blockchain Technology?—A Systematic Review", the Blockchain is "a distributed database solution that maintains a continuously growing list of data records that are confirmed by the nodes participating in it." The data is recorded in a digital public ledger which contains the information of every transaction ever completed. It is a decentralised solution which does not require any third party organization in the middle. The information and record of every completed transaction is always available to and shared with all the nodes in the chain.

This attribute of block chain makes the entire system transparent as compared to the centralised transactions involving a third party. Additionally, the nodes of a Blockchain are all anonymous, making it more secure for other nodes to verify and confirm the transactions. Bitcoin was the first application ever to have used and introduced the Blockchain technology. It created a decentralised network for cryptocurrency where all the involved parties could buy, exchange goods, services, mine Bitcoins with digital money.

However, despite the seemingly obvious and ubiquitous solution for transaction conduction using cryptocurrencies, Blockchain has many technical challenges and limitations which need to be eliminated before the full-fledged adoption of Blockchain into every day transactions. Some of which being the high integrity and security, as well as privacy of nodes in order to prevent the attacks and attempts to disturb transactions in Blockchain. Additionally, the confirmation of transactions in Blockchain requires significant computational power.

History and Current Reception

The foundation of Blockchain was laid down in 1991 by Stuart Haber and W. Scott Stornetta, who wanted to implement a system where the tampering of timestamps of a document could not be done. In 1992, Bayer, Haber and Stornetta implemented Merkle trees to their design which consequently improved its efficiency by allowing several document certificates to be collected into one block.

The Blockchain as it is we know today was conceptualised by a person (anonymous) named as Satoshi Nakamoto in 2008. They improved the design significantly using a Hashcash-like method to add blocks to the chain without the requirement of third party authentication. The same design was implemented a year later by Nakamoto, as a foundation block of the cryptocurrency Bitcoin, where it serves as the public ledger for all the transactions on the network.
The words *Block* and *Chain* were used distinctly in Nakamoto's original paper, but were eventually adopted in language as singular *Blockchain*, by 2016.

Smart contracts which run on Blockchain; e.g., the ones which create self-payable invoices after shipment arrival or share certificates to send dividends to owners after the profit reaches a certain level; require an off-chain oracle to access any external data or events based on time or market conditions which need to interact with the Blockchain.

Blockchain is becoming rapidly popular in the IT world of today as is evident by the fact that IBM opened a Blockchain innovation research centre in Singapore in July 2016. A World Economic Forum summit was held in November 2016 to discuss the development of governance models related to blockchain.

According to Accenture, the application of diffusion of innovations theory suggests that Blockchains attained a 13.5% adoption rate within FinTech enterprises, therefore reaching the 'Early Adopters' phase. Industry trade groups merged to form the Global Blockchain Forum in 2016, initiated by the Chamber of Digital Commerce.

However as the popularity receded, only 1% of the CIOs indicated any kind of blockchain adoption within their organisations and only 8% of CIOs were in the short term 'planning or looking at active experimentation with

blockchain', evident by the survey conducted by Gartner in May 2018.

Structure of a Typical Blockchain

As mentioned earlier, a Blockchain database is managed autonomously by a peer-to-peer network and a distributed time-stamping server. It is authenticated by mass collaboration driven by collective self-interests. The decentralized design facilitates a robust workflow where the uncertainty regarding data security is marginal compared to centralized ledgers.

The use of blockchain eliminates the characteristic of infinite reproducibility from a digital asset by confirming that each unit of a certain value was transferred only once, thus solving the long-standing problem of double spending. Described as a value-exchange protocol, a blockchain can maintain title rights because, when set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blocks

Blocks hold batches of valid completed transactions which are hashed and encoded into Merkle tree. Each block includes the hash value of the prior block in the blockchain, linking the two. The linked blocks form a chain. The iterative process confirms the integrity of the previous block, all the way back to the first block. The first block of a blockchain, called Genesis Block or Block 0, is the ancestor that every block in the chain can trace its lineage back to. 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.

Hard Fork

A *hard fork* is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid. In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software.

If one group of nodes continues to use the old software while the other nodes use the new software, a split can occur. For example, Ethereum has hard-forked to "make whole" the investors in The DAO, which had been hacked by exploiting vulnerability in its code. In this case, the fork resulted in a split creating Ethereum and Ethereum Classic chains. In 2014 the Nxt community was asked to consider a hard fork that would have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT from a major cryptocurrency exchange. The hard fork proposal was rejected, and some of the funds were recovered after negotiations and ransom payment. Alternatively, to prevent a permanent split, a majority of nodes using the new software may return to the old rules, as was the case of Bitcoin split on 12 March 2013.

Functioning

The blockchain technology is applicable to any digital asset transaction exchanged online. The

working process of a Blockchain has three components:

1. Validate Entries

2. Safeguard Entries

3. Preserve Historic Record

A typical Block chain uses cryptographic proof instead of the trust-in-the-third-party mechanism for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature, is sent to the "public key" of the receiver, and is digitally signed using the "private key" of the sender. In order to spend money, the owner of the cryptocurrency needs to prove his ownership of the "private key".

The entity receiving the digital currency then verifies the digital signature, which implies ownership of the corresponding "private key", by using the "public key" of the sender on the respective transaction. Each transaction is broadcasted to every node in the Blockchain network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger.

The verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency, through the digital signature verification on the transaction.

2. Spender has sufficient cryptocurrency in his account, through checking every transaction against the spender's account, through checking every transaction against the spender's account, or "public key" that is registered in the ledger. This ensures that there is sufficient balance in his account before finalizing the transaction.

Earlier, there was the question of maintaining the order of these transactions that were broadcasted to every other node in the Bitcoin peer-to-peer network. The transactions did not come in order in which they are generated, and hence there was a need for a system to make sure that double-spending of the cryptocurrency did not occur. Considering that the transactions are passed node by node through the Bitcoin network, there was no guarantee that orders in which they are received at a node are the same order in which these transactions were generated. The above means that there was a need to develop a mechanism so that the entire Bitcoin network can agree regarding the order of transactions, which was a daunting task in a distributed system.

The Bitcoin solved this problem by a mechanism that is now popularly known as Blockchain technology. The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are considered to have happened at the same time. These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous block.

There still remains one more problem: Any node in the network can collect unconfirmed transactions and create a block and then broadcast it to the rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain?

There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network. Blockchain solves this problem by introducing a mathematical puzzle: each block will be accepted in the block chain provided it contains an answer to a very special mathematical problem. This is also known as "proof of work": a node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For instance, a node can be required to find a "nonce" which when hashed with both transactions and hashes of previous blocks produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a node in the Bitcoin network to make a right guess and generate a block. There is very small probability that more than one block will be generated in the system at a given time. The first node, to solve the problem, broadcasts the block to the rest of the network. Occasionally, however, more than one block will be solved at the same time, leading to several possible branches.

However, the math needed to be solved is very complicated and hence the blockchain quickly stabilizes: after this, every node is in agreement about the ordering of blocks. The nodes donating their computing resources to solve the puzzle and

generate blocks are called “miner” nodes” and are financially awarded for their efforts. The network only accepts the longest blockchain as the valid one. Hence, it is next to impossible for an attacker to introduce a fraudulent transaction since it has not only to generate a block by solving a mathematical puzzle, but it also has to race mathematically against the good nodes to generate all subsequent blocks in order for it to make the other nodes in the network accept its transaction and block as the valid one. This job becomes even more difficult since blocks in the blockchain are linked cryptographically together.

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).[1] 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 Bitcoin and Ethereum.

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.

Uses of Blockchain

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 micro insurance 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

Risks of Adoption

BlockChain is a promising breakthrough technology. As described before, there are vast array of applications or problems that can be solved using BlockChain based technology, spanning from Financial (remittance to investment banking) to non-financial applications like Notary services. Most of these are radical innovations. As it happens with the adoption of radical innovations, there are significant risks of adoption.

Behaviour change: Change is constant, but there is resistance to change. In the world of non-tangible trusted third parties introduced by BlockChain, customers need to get used to the fact that their electronic transactions are safe, secured and complete. The present day intermediaries like Visa or Mastercard (in case of a credit card) will also go through a change of roles and responsibilities. We envision that these companies will also invest and move their platforms to be BlockChain-based. They will continue to provide services to further customer relationship.

***Scaling*:** Scaling of the current nascent services based on BlockChain presents a challenge. Imagine yourself executing a BlockChain transaction for the first time. You will have to go through downloading the entire set of existing BlockChains and validate before executing your first transaction. This may take hours or longer as the number of blocks increase exponentially.

Bootstrapping: Moving the existing contracts or business documents/ frameworks to the new BlockChain based methodology presents a significant set of migration tasks that need to be executed. For example, in case of Real Estate ownerships, the existing documents lying in County or Escrow companies need to be migrated to the equivalent BlockChain form. This may involve time and costs. Government

Regulations: In the new world of BlockChain-based transactions, government agencies like FTC and SEC may slow down the adoption by introducing new laws to monitor and regulate the industry for compliance. In a way, this may help

adoption in the United States as these agencies carry customer trust. In more controlled economies like China, the adoption will face significant headwind.

Fraudulent Activities: Given the pseudonymous nature of BlockChain transactions, coupled with ease of moving valuables, the "bad guys" may misuse the technology for fraudulent activities like money trafficking. That said, with enough regulations and technology-support, law enforcement agencies will be able to monitor and prosecute these individuals.

Quantum Computing: The basis of BlockChain technology relies on the very fact that it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the future advent of Quantum Computers, the cryptographic keys may be easy enough to crack within a reasonable time through a sheer brute force approach. This would bring the whole system to its knee. The counter-argument would be for keys to become even stronger so that they may not be easy to crack.

Conclusion

BlockChain is Bitcoin's backbone technology. The distributed ledger functionality coupled with the security of BlockChain makes it a very attractive technology to solve the current financial as well as non-financial industry problems.

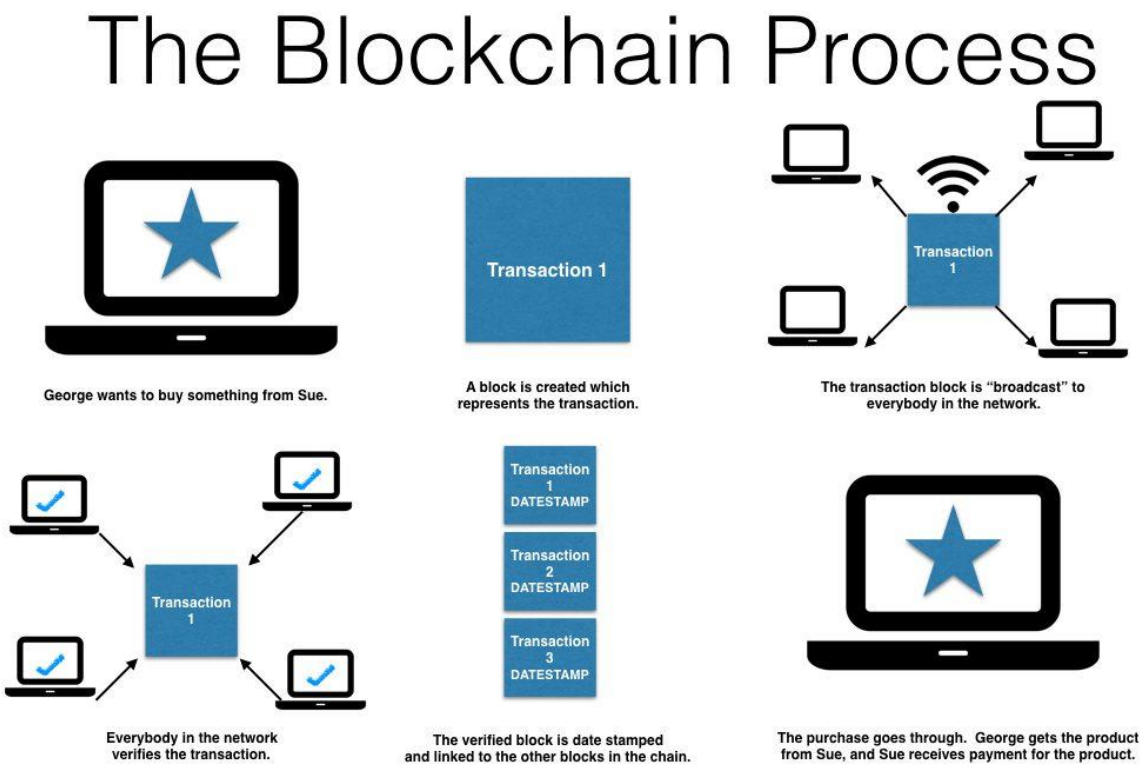
There is enormous interest in BlockChain-based business applications and hence numerous start-ups working on them. The adoption definitely faces strong headwind as described before. However, even large financial institutions such as Visa, Mastercard, Banks, and NASDAQ, are investing in exploring applications of current business models on BlockChain. In fact, some of them are searching for new business models in the world of BlockChain. Some would like to stay that they are even ahead of the curve in terms of transformed regulatory environments for BlockChain. It is envisioned that BlockChain technology going through slow adoption due to the risks associated. Most of the startups will fail with few winners. Having said this, we should be seeing significant adoption in a decade or two.

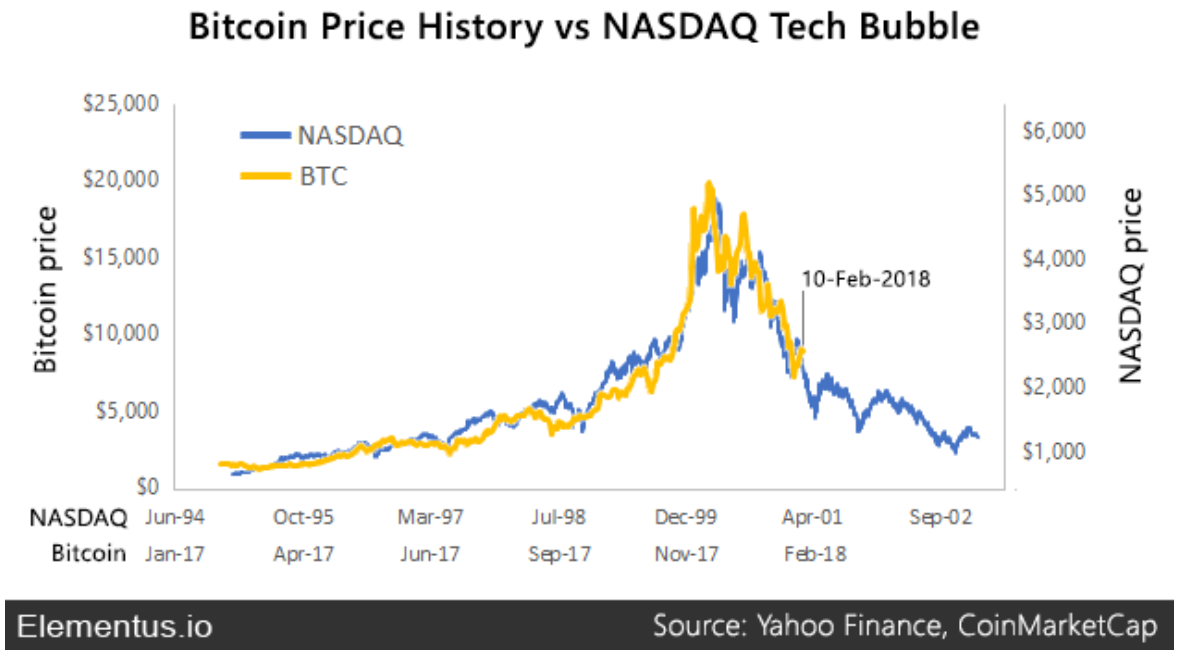
.

References

1. Borenstein, Joram. "A RiskBased View of Why Banks Are Experimenting with Bitcoin and the Blockchain." Spotlight on Risk Technology. N.p., 18 Sept. 2015. Web. 03 May 2016.
2. Barski, Conrad, and Chris Wilmer. "The Blockchain Lottery: How Miners Are Rewarded - CoinDesk." CoinDesk RSS. CoinDesk, 23 Nov. 2014. Web. 03 May 2016.
3. "Chain | Enterprise Blockchain Infrastructure." Chain | Enterprise Blockchain Infrastructure. N.p., n.d. Web. 03 May 2016.
4. **"**Research Handbook on Digital Transformations." F. Xavier Olleros, Majlinda Zhegu.
5. "Where is current research on Blockchain Technology? – A systematic review." Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander. Oct 3, 2016.
6. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang. June 2017.

Appendix


The Blockchain Process
Transaction 1
Transaction 1
George wants to buy something from Sue.
A block is created which represents the transaction.
The transaction block is "broadcast" to everybody in the network.
Transaction 1
Transaction 1 DATESTAMP
Transaction 2 DATESTAMP
Transaction 3 DATESTAMP
Everybody in the network verifies the transaction.
The verified block is date stamped and linked to the other blocks in the chain.
The purchase goes through. George gets the product from Sue, and Sue receives payment for the product.


Bitcoin Price History vs NASDAQ Tech Bubble
NASDAQ
BTC
10-Feb-2018
Bitcoin price
NASDAQ price
$25,000
$20,000
$15,000
$10,000
$5,000
$0
$6,000
$5,000
$4,000
$3,000
$2,000
$1,000
NASDAQ Jun-94 Oct-95 Mar-97 Jul-98 Dec-99 Apr-01 Sep-02
Bitcoin Jan-17 Apr-17 Jun-17 Sep-17 Nov-17 Feb-18
Elementus.io
Source: Yahoo Finance, CoinMarketCap

Appendix

Types of ledgers