An overview of blockchain technology: background, history, challenges, examples

Science, Computer Science

Blockchain is defined as a dispersed database clarification preserving an expanding number of files and documents accepted by the junctions engaging in it. The data is documented in a people’s log, consisting knowledge regarding each accomplished financial bargain. Blockchain is a redistributed solution where there has to be no requirement of another group standardization in between. The information regarding each accomplished execution in Blockchain is equally integrated and present at all junctions. It is due to this characteristic that the system becomes more explicit as compared to rationalized financial settlements consisting of another group. Additionally, the junctions in Blockchain are unacknowledged, making it mostly protected for other junctions to accept financial bargain. Bitcoin was the initial function to be started in blockchain technology. It generated localized surroundings for cryptocurrency, where people can purchase and swap items through electronic cash i. e., either by credit card or visa debit card.

Funds transfer or financial bargain between people or enterprises are redistributed and handled by a third group coordination. Making a digital remittance or financial settlement requires a credit card provider as a mediator to accomplish execution. Additionally, any financial settlement needs a fees from a bank or credit card company. In many areas like games, music, software etc. this feature is applied. The system of execution is incorporated, and all data and information are handled by a third group coordination, rather than the two groups involved. Blockchain technology was therefore designed to sort out this matter. The important goal of

Blockchain technology is to produce a localized atmosphere where there is no constriction on another group to handle financial negotiations.

Although Blockchain seems to be a compatible outcome for supervising financial settlements by using cryptocurrencies, it has faced some technical confrontations requiring further research. There needs to be a high combination of financial settlements and security of junctions to obstruct the invasions and threats interrupting financial executions in Blockchain. Additionally, authenticating financial activities in Blockchain requires a computer system power.

Background

Blockchain, popularly known as a technology running a cryptocurrency called bitcoin, is a people’s log preserving the accuracy and completeness of financial execution. It was used when the bitcoin cryptocurrency was launched. Bitcoin is mostly used for function using blockchain technology. Bitcoin is a redistributed digital financial remittance process involving a people’s execution log known as blockchain. The vital characteristic of Bitcoin is acceptable and reasonable without any organization or government in control. Bitcoin is consistently grabbing more acceptance regarding financial settlements and number of users. Additionally, the conversions with conventional currencies, e. g. KRW are consistently occurring in financial exchange markets. Bitcoin has become successful in grabbing attention from different communities.

In Bitcoin, a people’s key framework mechanism is followed. In PKI, the user has a couple of people’s keys and private keys. The people’s key is used in user’s location handling a bitcoin wallet, and the private key is generally used for user’s authentication. The execution of bitcoin involves sender’s people’s key, several people’s keys of the receiver, and the transferred value.

A duration of ten minutes is utilized by data execution process to be inscribed in a block. This new block is connected to a formerly inscribed block. All blocks including financial negotiation regarding each accomplished execution, are kept in user’s disk storage, known as junctions . All junctions have information regarding every updated execution of bitcoin network and verifies the accuracy of every financial execution accomplished through the help of former blocks. The junctions are recognized by verifying the accuracy of transactions. This technique is called extraction or digging, the most essential concept of blockchain technology. When all transactions are done successfully, there is an agreement which occurs between all junctions. The new blocks are connected to former blocks and all blocks are constructed in one particular expanding chain. This chain of blocks is a people’s log mechanism of bitcoin known as blockchain.

Blockchain is a localized controlling procedure of Bitcoin, implemented for doing financial settlements of bitcoin users. This mechanism supports people’s log of all accomplished Bitcoin transactions, without any unnecessary interference of the third group coordination. The main advantage of blockchain is that the people’s register can’t be reorganized or erased after the data gets acceptance by all junctions. This is the reason why blockchain has been known for its data unification and security features. Blockchain mechanism can also be implemented to other types of uses. It can produce an atmosphere for digital undertaking and peer to peer data merging in cloud service. The main strength of blockchain mechanism is data solidarity due to which its use is extended to other applications.

Challenges faced by the Blockchain

Throughput: It is defined as the output with respect to input; or the amount passing through a system from input to output (especially of a computer program over a period of time). The capacity of throughput of issues in the bitcoin is presently 7 executions per second. Other processing networks are VISA (2000tps) and Twitter (5000tps). When there is an increase in the number of financial executions, upgrading of throughput is required in blockchain network.

Latency: It is defined as the delay prior to the transfer of data starts following an instruction for transfer. In Blockchain technology, an execution regarding a financial settlement takes ten minutes. More time is spent on the block to achieve high efficiency in security, because counterbalancing the double expenditure of attacks is needed by the block. Therefore every transaction is authenticated at the Blockchain assuring that the inputs used for execution have not been spent before and this process is handled by the bitcoin. While preserving security, implementing a block and ensuring the financial bargain has to occur in seconds, and this makes latency a great obstacle in Blockchain. In order to execute a financial agreement, like in VISA it takes little time which is profitable as compared to blockchain.

Size and Bandwidth: Presently, the size of a blockchain in bitcoin network is greater as compared to 50, 000 MB. When there is an increase in throughput up to that of VISA, there would be a rise in blockchain up to 214PB every year. It is expected that the size of the block is 1 MB, and it requires ten minutes to generate a fresh block. Therefore there are limitations on the frequency of executions; only 500 executions in a single block should be permitted.

Security: There are chances for a blockchain to counter 51% security threat. In this threat a single unit can acquire full control over the majority of the network's mining hash rate and could maneuver Blockchain. Therefore it requires more research to settle this issue.

Wasted Resources: Large amount of energy is exhausted in extracting a bitcoin ($15 million/day). This decay in bitcoin is caused by Proof-of-Work effort. This issue requires to be solved to get sufficient extraction in Blockchain.

Versioning , hard forks, multiple chains: A minute chain that involves a tiny nodes has more chances to have 51% attack. Another issue arises when chains are divided for administrative or translation purposes.

Blockchain possesses the calibre to alter the mechanism of financial executions conducted in daily life. Its uses are not only restricted to cryptocurrencies, but it’s technique can be applied in different surroundings where some business is executed. Its uses are found to be an area for future research, but unfortunately it has technical limitations and objections in which Anonymity, data integrity, security attributes are one of them. Scalability is another problem that needs to be tackled.

History of Blockchain

Blockchain, a peer-to-peer network was introduced in October 2008 developed by a person or the group under the nick name Satoshi Nakamoto and became operational since early 2009. In this there are no financial institutions in extracting a bitcoin. It is initially a localized virtual legal tender. It involves an electronic remittance system based on encrypted proof. It consists of no third group engaging in it.. The transaction involves the owner and the receiver and transmitted through the point to point network . Unearthing of bitcoins at the junctions accumulate the executions into blocks. A block consists of information about executions and the former block was connected to the first block when the bitcoin network started. A file is maintained on every junction. Each block contained a Proof of Work. Every new block is started and connected to the Blockchain. The first execution process which occurred was considered as a special agreement and this was equal to the latest coins owned by the block creator. This new status was transmitted to the network. Reinterpreting the Proof of Work from a Transaction block was equivalent to the extraction process. The extraction process of bitcoins approves executions and augments security. The workers involved in extraction process are remunerated by number of executions they prove. Bitcoins are produced in blocks. Presently, 25 bitcoins are manufactured per block. A new block is produced after every ten minutes duration.

More than 11. 5 million bitcoins were produced since September 2013. In January 2009, one transaction block executed fifty bitcoin transactions. Initially, CPU power was needed to solve the Proof of Work regarding transaction blocks. Graphic cards were used to solve this problem faster and new chips were introduced during extraction process. Proof of Work is defined as a protocol which challenges the extraction process. It is hard puzzle to be solved and easy to be authenticated. After a gap of two weeks, bitcoin production rate is adjusted automatically. It uses cryptographic hash SHA256. It acts as a solution to order the execution blocks. A general desktop system requires many years to solve the Proof of Work problem, whereas a bitcoin network takes ten minutes to solve.

A bitcoin is redistributed digital legal tender system which uses at its core a disseminated data structure called blockchain- a register involving all transactions done with the legal tender. Many systems like Ethereum, an example of bitcoin have increased its functionality, but it still depends on a similar blockchain to harmonize information between junctions. As Ethereum, a bitcoin has acquired popularity, it is revealed that more data will be accumulated in the blocks. Large blocks penetrate through the network inefficiently and this leads to insignificant performance if several executions are included. This occurs due to the unskillful creation of blocks by various junctions leading to conflicts.

A General Example of a Blockchain

An example of a Blockchain lies in health care systems in MedRec. In this system design changes were required for Electronic Health Records. MedRec is a redistributed record management system used to control EHRs, using blockchain technology. This system provides patients with an unchangeable log and easy approach to their medical records across providers. MedRec manages authentication, confidentiality, accountability and data storage and retrieval in case of handling sensitive information providing advantage to unique blockchain properties. A modular design merges with existing details of the provider promoting compatibility, making our system adaptable. We build our hopes on medical stakeholders to get involved in the network as blockchain “ minors”. This mechanism gives them approach to aggregate, anonymized data as mining rewards, in return for sustaining and protecting the network via proof of work. MedRec enhances the emergence of data economics, providing big data to strengthen researchers while dealing with patients and providers in the choice to release metadata. Patients have data dispersed across various organizations and due to this they lose route to approach data as the provider retains primary stewardship. According to the HIPAA Privacy rule, providers require maximum two months to answer to a request for upgrading or erasing a record that was added fallaciously. If the time delay exceeds, maintaining a data proves to be challenging to start as patients are rarely motivated and told to check their complete record. Patients therefore communicate with records in a fragmented manner exhibiting the nature of these records about how they are handled.

Interoperability challenges between various provider and hospital systems act as additional hurdles to stronger data sharing. This inaccurate coordinated data management and exchange means health records are separated, rather than organized. Patients and providers face obstacles regarding data recuperation and sharing due to economic impulse which promote “ health information blocking”. A latest ONC report consists of details regarding the topic, namely health IT developers restricting the data flow by charging excessive prices for data exchange mediums.

Therefore patient agency needs to be prioritized while designing new systems to mitigate these hurdles. In this era of internet banking and social media, patients are interested in handling their information on the web page. The ONC’s report lays stress on biomedical and public health researchers which possess the capability to analyze information from several sources in order to know public health risks, implement new treatments and enhance precision medicine. In this example, a blockchain structure is applied to EHRs. It is made on an allocated register protocol linked with Bitcoin. It uses public key cryptography to create an unchangeable, time stamped chain of content. Versions of the blockchain are delivered on each node in the network. The Proof of Work algorithm is used to protect the content from interfering depending on a trustless model, where individual nodes participate to sort out exhaustive puzzles before the next block of chain can be adjoined to the chain. These worker nodes are known as “ miners”, and the work needed to subjoin blocks assures that rewriting history on blockchain is difficult.

MedRec blockchain implementation assigns the four important issues like fragmented, slow approach to medical data; system interoperability; patient agency; improved data quality and quantity for medical research. References to data are assembled and encrypted as hashed pointers on a blockchain log. These references are assembled to create an approachable record for medical history, without collecting raw medical data on the blockchain. Our system supplements these pointers with on-chain authorization and data integrity logic, strengthening individuals with record verification, inspection and data sharing. Robust systems are built to merge with present databases for interoperability. A data extraction scheme is designed to sustain the MedRec network and fetch big data to medical researchers. MedRec is presented not only as an antidote for record control, but also to signify innovative EHR solutions applying blockchain technology.