ISSN: 2349-4891
International
Journal of Recent Research and Applied Studies
(Multidisciplinary Open Access Refereed e-Journal)

BLOCKCHAIN TECHNOLOGY: THE REVOLUTION THAT THE DIGITAL NEPAL DESERVES

Reyan Kumar Sapkota
St. Xavier's College, Maitighar, Kathmandu

Received 6th April 2021, Accepted 20th September 2021

Abstract

The staggering rate at which cryptocurrencies have climbed up the ladder has caused some serious speculation on the currencies and the technology behind them. The 2008 financial crisis caused an overwhelming response to the proposals of decentralized money and made the pre-existing proposals a living reality. Many companies have started adopting Blockchain technology which has initiated widespread attention toward the technology itself. Blockchain technology has emanated to every nook and corner of the world, and the pace at which it is decentralizing money and other services is alarming to banks and other third-party institutions. Nepal has been a mere spectator, while the world has been reaping the fruits of this profound application of the internet. Over 99 percent of Nepalese teens do not know what Blockchain is and this can cause unnecessary trouble to the country's administration system soon. The paper is divided into two sections. The first serves as an introduction to the technology and the mechanism underlying it. The second half proposes the smart application of Blockchain Technology to enforce Digital Currency in Nepal. The paper does not attempt to disregard the existing system as useless but tries to propose an efficient alternative way to replace the system for the good. The infant Nepalese technological industry will rise to a sufficiently convenient spot only when the industry embraces the Innovations before it's too late. So, the research below tries to propose new ways of running day-to-day services with the profound efficiency that Blockchain Technology offers.

Keywords:

Blockchain, Cryptography, Hash function, Merkle Root, Bitcoin White Paper, MDR, Nonce, Proof of Work, Consensus, Mining, Interoperability, Public Key, Private Key, Avalanche Effect.

1. INTRODUCTION

Blockchain is a distributed ledger technology that makes the history of transactions unalterable and transparent through the use of DECENTRALIZATION and CRYPTOGRAPHIC hashing. It allows peer-to-peer transactions without the centralization of authority over a single party. The cost of transactions is reduced dramatically as there is no intermediary. Blockchain is the face behind the success of cryptocurrencies like Ethereum, Bitcoin, DogeCoin, Litecoin, etc. After the financial crash of 2008, people's lack of trust in third-party agents like banks, brokers, and other such merchants was at its peak. People couldn't trust third parties as their transaction medium. In 2008, an anonymous person/group called Satoshi Nakamoto published a paper:" Bitcoin: A Peer to Peer Electronic Cash System". In 2009, the first Bitcoin transaction occurred between computer scientist Hal Finney and the anonymous Satoshi Nakamoto. Blockchain technology allowed the transfer of monetary value between two unknown parties without the need for intermediaries, like banks. Bitcoin was the first platform that allowed decentralized and internet-based consensus for the transfer of data. After that Bitcoin and the technology behind it have witnessed an overwhelming boom, foreshadowing a new future of Transactions and Data Security.

1.1. History

While Blockchain came into the spotlight only after Nakamoto's paper, it was developed and introduced back in the 90s.

ISSN: 2349 – 4891

The concept of Blockchain was first introduced by David Chaum in his dissertation namely ”Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”. *(Source: Wikipedia)*. The conceptualization of Blockchain as a cryptographically secured transaction model was described in 1991 by Stuart Haber and W.Scott Stornetta. They developed Merkel Trees for a system where the document timestamps could not be tampered with. Merkel Trees improved the efficiency by allowing several documents to be collected into a single block. The proposed working on Cryptographically secured documents in a chain of blocks as TimeStamps where no one could tamper with the TimeStamps of documents. They published a paper “How to Time-Stamp a Digital Document” (https://link.springer.com/content/pdf/10.1007/BF00196791.pdf) in the Journal of Cryptography in 1991. “*Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service*.”

This was the statement mentioned in the abstract of the research paper. This led to the foundational idea of Blockchain technology.

HashCash was developed in 1997 by Adan Back. HashCash used the concept of Proof Of Work to validate the transactions done over the web. Hashcash was tested in email systems from Microsoft and the open-source software provider Apache, but it never took off. Conceptually, Hashcash was a great example of how to introduce the digital scarcity required for internet-based money, but the technology itself wasn’t really a good form of digital currency.

In **2004**, computer scientist and cryptographic activist **Hal Finney** introduced a system called **Reusable Proof Of Work(RPoW)** as a prototype for digital cash. It was a significant early step in the history of cryptocurrencies. Reusable Proof of Work (RPoW) solved the double-spending problem by keeping the ownership of tokens registered on a trusted server. This server was designed to allow users across the globe to verify the transaction and maintain integrity.

Another attempt was made to take the value of a tangible object (Gold, Money) and make it digital. This is the example of Bit Gold. It was introduced in 2005 by Computer Scientist Nick Szabo. Szabo’s idea came after the advent of E-gold, which used gold to back digital value. However, his design utilized a “client puzzle function” type of proof-of-work. The system proposed using a “challenge string” generated on a user’s computer that is then securely timestamped “in a distributed fashion.” This would then be submitted to a “distributed property title registry” to digitally provide proof of ownership.

After the 2008 Financial Crisis, a person (or group of persons) called Satoshi Nakamoto introduced Bitcoin as a decentralized and peer-to-peer electronic transaction system. The technology used all the bits and pieces of the previously failed attempts of decentralizing money (E-Gold, HashCash, Bit Gold) and brought a trusted Internet-Based Decentralized Transaction system.

In 2009, a successful transaction took place between Satoshi Nakamoto and Computer scientist Hal Finely. After that agencies like “WikiLeaks” started accepting Bitcoin as donations. A computer programmer named Laszlo Hanyecz was the first customer to pay using bitcoin. He bought 2 pizzas for 10,000 BTC, which was equivalent to $25 dollars on May 22, 2010. This famous transaction was done on May 22. The Bitcoin community celebrates May 22 as Bitcoin Pizza Day.

Bitcoin's popularity led to the invention of other cryptocurrencies like Ethereum, LiteCoin, DogeCoin, etc. People and businesses realized that Blockchain was not only feasible to cryptocurrency but was also extremely useful in maintaining Data Security and integrity in various tasks like storage, messaging, transfer of files, E-Commerce, etc. Now, companies like Walmart, Amazon incorporate private Blockchain technology to ensure safe and transparent data transfer involved in E-Commerce. Blockchain has been used to improve supply chains, food distribution, financial services, government, retail, and more. Blockchain eliminates various threats like duplication of effort, tampering of data, fraud, and all those shortcomings that prevail in centralized transaction models. IBM Blockchain is one of the leading entities that has been providing the service of Blockchain deployment in various companies. El Salvador has accepted Bitcoin as a legal currency. Now, the citizens of El Salvador can use Bitcoin for their national and international payments, with bare minimum charges. This is expected to revive El Salvador’s economy. Blockchain has already polished its foundations and its future seems no less than the next industrial revolution.

ISSN: 2349 – 4891

2. HOW DOES A TRANSACTION WORK IN A BLOCKCHAIN?

Blockchain technology seems sophisticated at first sight. The complex network of blocks, the billions of permutations and combinations, hashing algorithm and all such mathematical complexities involved in the technology makes it look beyond one's intellectual fragment. But, it isn't so.

Blockchain primarily contains a Block that is interconnected with other blocks to form a chain of interrelated circuits. A block is formed when the user makes a transaction over the blockchain network, indicating that a transaction has occurred.

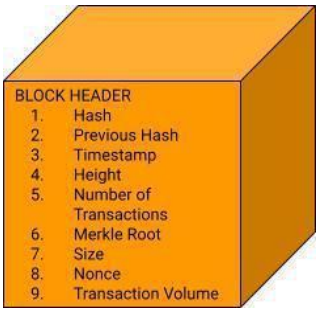


Fig 1: Block Header

Each block contains the following information:

1. **Block Height**: The block height of that particular block is the number of blocks that precede that block in the network. If the Block Height of a particular block is 15, it means there are 15 blocks created before it. In short, that particular block is the 16th block in the network.

2. **Hash:** Hash is a unique code that identifies the block uniquely. It is obtained using the Hash Function or Hashing Algorithm. Hash is like the fingerprint of the block. SHA-256 is an example of a Hash Function.

3. **Timestamp**: It is the exact time at which the block is added to the chain.

4. **Number of Transactions**: A block contains a collection of transaction ledgers. 1 transaction gives 1 ledger. The block stores the ledger inside it. Block Header contains the number of transactions the block has stored.

5. **Merkle Root**: To reduce the size of the block, the transaction ledgers are arranged in a Merkle Tree. The root of the tree is called Merkle Root. Merkle Tree is explained below.

6. **Size**: It is the size of the block. For Bitcoin, the size of 1 block is 1 MB.

7. **Nonce**: It is the unique number of the Block which was passed to the Hash Function to obtain the Hash of the block. Nonce has been conceptualized in the paper.

8. **Transaction Volume**: It is the total amount of money that has been involved in all the transaction ledgers stored in the block.

Let us take three consecutive blocks from an anonymous Blockchain Network: Block "A", Block B, and Block C. Block B contains its data, hash and the hash of its previous i.e Block A. Block C contains its data, hash, and the hash of its previous block i.e. Block B. Since each block contains the hash of the previous block, every block in the network is interconnected to each other. In some blockchains, the Hash of a Block depends upon the hash of the previous block. Thus, a chain of interconnected blocks is formed. Change in the data of Block B directly affects its hash, which in turn affects the hash of the subsequent block in the network. Block A (first block) cannot contain the hash of any previous blocks. Block A i.e first block in the chain is called Genesis Block.

Let us understand how a transaction is accomplished in a Blockchain network. When person A sends some money to person B, the transaction record is created. For the transaction to occur successfully, the record has to be added to the Block and the block thereafter has to be added into the public network. The Block contains the transaction history between person A and person B, and the necessary identity metrics to identify the transaction as unique. The nodes of the network check the authenticity of the transaction receipt (amount, sender-receiver details, identification codes like Public key, Private Key, Digital Signatures). Once the nodes confirm the transaction as valid, the transaction receipt is eligible to be added to the block. For the transaction to happen successfully, the Block has to be added to the Blockchain Network. Miner is the one who adds the block into the network in the favour of some transaction

ISSN: 2349 – 4891

fee and reward incentives (incentive is decided by the respective Blockchain Protocol). To add the Block into the chain, two things have to be achieved:

a) Proof of Work
b) Consensus

a. Proof of Work

Block contains a Block Header and transaction details. Block Header primarily contains Nonce, Hash, and Hash of the previous block. The nonce is data whose value depends on the data inside the block. The value of Hash depends on the value of Nonce. Hash is obtained from the Nonce through Hash function or Hashing algorithm (eg; SHA-256 hashing algorithm). Hash serves as the fingerprint of the block after the block is added to the Blockchain network.

Before diving into the process of Proof of Work, the foundational concept of Hashing algorithm or cryptographic Hash function is important. The hash function takes a certain character as a domain and returns a Hash code for that particular domain. The process of converting a character into a unique Hash through the Hash function is called Hashing. Here is an example from a Hash function. SHA-256 online hash function has been used for the illustration below.

SHA-256 converts any character into a 256-bit code (64 digits alphanumeric character). Source:

https://emn178.github.io/online-tools/sha256.html

Example:

Here, text “Rex”, “rex”, and “reX” are passed as the argument or domain of the function SHA-256.

SHA-256(“Rex”)=
80f1e148f14f3b82aaec65244d7685c1096a8174d748fdc497ecd28ad41ee0b0

SHA-256(“rex”)=
3227fe6bde46249b0aae4b69ef6efd806422a46788e281d050d32d0d9fbde723

SHA-256(“reX”)=
936c23ab6eb8c5977577f6c288841b1ff95d9a4bb1d7b23b25f11f370b059d69

Notice how even a minor change in uppercase and lowercase position causes such significantly different hash codes. This significant change in the value of hash due to a slight change in the value of the input is called the “Avalanche Effect”.

Such an algorithm is used to ensure uniqueness in Hash generation and eventually ensure uniqueness among the Blocks in the Blockchain Network.

SHA-256 can give more than 10^77 values.

SHA-512 can give more than 10^154 values.

SHA1 can give more than 10^48 values.

Hash is obtained when Nonce is passed as the argument to the hash function. Similarly, a unique number is obtained when the hash is passed to the hash function. This number should be less than a Target Number in order to get added to the blockchain network.

Generally,
SHA-256 (Nonce) = Hash -------- (1)
SHA-256 (Hash) = Number-------- (2)

To add the Block in the chain, a unique number has to be obtained after hashing that is less or equal to the Target Number.

The target number is set by the Blockchain Protocol.
Let's call the unique number, **“Golden Number”**.

To obtain the Golden Number (any number less than the Target Number), the mining device (ASIC in the case of Bitcoin) has to obtain a unique Nonce (Number used only once). The nonce is located in the Block Header. The miner can change the Nonce for the Block until the Nonce gives the Golden Number after Hashing (according to the Final equation given below). Miners use the hashing algorithm to obtain the equivalent hash for the given nonce. In the case of Bitcoin, the SHA-256 hashing algorithm is used. Thus obtained hash is further fed into the hashing algorithm to obtain the Golden Number. There is only a single nonce for a single block which leads to the Golden Number. Obtaining such nonce is a matter of hit and trial. Extensive computing power is expended to obtain such a nonce. This nonce can be called “Golden Nonce”. The hash which leads to Golden Number can be called Golden Hash.

ISSN: 2349 – 4891

Chances that two miners with the same computing power will get that nonce is similar to two people striving for heads during a coin toss. The chances of success remain the same no matter how many times the miner double hashes (applying the Hash function twice) the nonce to the Golden Number(see the combined equation below). This belief is analogous to Gambler's Fallacy.

Mathematically,
For Mining purposes,

SHA-256(GoldenNonce) = GoldenHash ---------- (3)
SHA-256(GoldenHash) = Golden Number ---------- (4)
Golden Number < Target Number ---------- (5)
Combining equations (3), (4), and (5),

SHA-256(SHA-256(GoldenNonce)) < Target Number ---------- (Final)

The main purpose of the Target Number is to increase the difficulty in obtaining the Golden Nonce. Block cannot be added to the network until the Golden Nonce is obtained. The target number is coded into the source code of every node. The target number is adjusted by the respective protocol as per the number of miners involved. How is the value of the Target Number determined in the Protocol? More miners involved means the target number value should be less. This is to ensure difficulty in finding the target number and maintain the Mining Difficulty. Difficulty in finding target numbers means difficulty in finding Golden Nonce. Since Mining efficiency and the number of miners are increasing daily, this leads to increased chances of obtaining the target in less time and eventually decrease in Mining Difficulty. This decrease in mining effort decreases the value of the currency and leaves the miners with no incentive to continue the mining. To maintain the Mining Difficulty, at regular intervals, the target number is reduced. The calculation is done by putting all the factors into account: Mining efficiency of the engine, number of miners, reduction in mining time over the period, mining cost, and many more. For the bitcoin network, the Target number is reduced after every 2 weeks (it takes 2 weeks to add 2016 new blocks to the network), under the consensus of 51 percent nodes in the network. 1 CPU gives 1 vote. Such consensus can only change in Protocol (In the case of Bitcoin and other blockchain networks). Such is the decentralization in Blockchain technology. Mining Difficulty is necessary for maintaining the immutability of the block. Mining difficulty is also one of the factors which incentivize the miners to add the block into the network by maintaining the high price value of the CryptoCurrency. (Simple economics says, difficulty in obtaining the object automatically increases its value, e.g. Gold, Oil).

**Golden Nonce, Golden Hash, and Golden Number are not conventional terms. They have been coined by the author for the convenience of understanding the transaction through Blockchain.*

If the value of SHA-256(Hash) exceeds the Target Number, the process is tried until the Golden Number is obtained. Golden Number is any number that is less than the Target Number. The nonce is altered by the miner until the Number obtained from (3) and (4) is less than the Target number. Thus, when the condition is met (i.e SHA-256(SHA-256(Nonce) < Target Number), the block is ready to be added to the network.

To obtain the Golden Number, lots of computing power is needed. The Hash and Golden Number obtained from the golden nonce must be a unique character. If the Golden number is not obtained, then the Miner has to alter the Nonce to obtain the target. That Nonce that leads to the Golden Target Number is the Golden Nonce. Since there are millions of blocks already existing in the chain, the probability of obtaining the unique hash and unique golden number is 1 in 16 trillion (in Bitcoin). Out of the trillions of permutations and combinations of Hashcode and matching the unique Hash and Golden number consumes massive CPU computing power. Out of trillions of guesses per second, 1 unique code is needed for the assignment of the Block. After obtaining the Golden Number and after assigning the hash

code to the Block, the Block can be added to the network. The miner who obtained the Golden Number first gets the right to add the Block to the chain. To add the Block to the chain, a consensus agreement is needed.

ISSN: 2349 – 4891

b. Consensus

A Blockchain network is a peer-to-peer network. Every node (a computer) is connected to the nodes all across the network. There is a peer-to-peer connection among the nodes of the blockchain network. After Miner obtains the Golden Number and the unique hash, Miner has to show proof that he has expended massive computing power to obtain the Golden number. After the nodes in the network verify the Block as authentic and acknowledge the effort of the Miner, the block adheres to the network. 51 percent of the nodes should vote for the confirmation of Block as a valid block. Only after such confirmation, Block can be added to the network.

Miner gets the share of his transaction fee and a reward (6.25 Bitcoin in Bitcoin Network as per updated Bitcoin Protocol) for such a tedious process. He gets 6.25 BTC per block added. Crypto Mining is analogous to actual Gold Mining. The ones with powerful digging tools get the Gold. Similarly, the one with a powerful computing device wins the race and gets the reward.

This is how the overall process of Proof of Work makes the addition of Block into the network very difficult. The electricity involved in the processing, and time makes the process expensive but profitable when incentivized.

2.1. Merkle Tree

Merkle tree, also known as a hash tree, is a data structure used for data verification and synchronization.

It is a tree data structure where each non-leaf node is a hash of its child nodes. All the leaf nodes are at the same depth and are as far left as possible. It maintains data integrity and uses hash functions for this purpose.
The transactions are stored inside the block in a Merkle Tree. Suppose there are 'n' transactions stored in a blockchain.

Transactions = { **Tx_1, Tx_2, Tx_3, Tx_4, Tx_5, ……Txn** }

If the transactions were stored serially in the block, without the use of Merkle trees, and if I had to verify whether my Transaction (eg; Tx_{45}) has been added to the block or not, then I had to download the entire block into my memory and search for my transaction details. To avoid this, a Merkle Tree is used. Arrangement of transactions in Merkle Tree allows us to view the desired transaction without downloading the entire block.
Suppose there are four transactions inside the block, Tx_1, Tx_2, Tx_3, and Tx_4 (as shown in the figure below). We can easily obtain the hash of transactions Tx_1, Tx_2, Tx_3, and Tx_4. Tx means Transaction. Mathematically,

Let H be the Hash function.
Calculating the hash of transaction Tx_1, Tx_2, Tx_3, Tx_4,
Hash1 = H(Tx1) Hash3 = H(Tx3)
Hash2 = H(Tx2) Hash4 = H(Tx4)

Now, using the Hash of Tx_1 and Tx_2, another new hash can be obtained.

Hash {1,2} = H(Hash1, Hash2)
Similarly, using the Hash of Tx_3 and Tx_4,
Hash {3,4} = H(Hash3, Hash4)

Again, using Hash{1,2} and Hash {3,4}, another new combined hash can be obtained.

Using Hash {1,2} and Hash {3,4},
Hash (Hash {1,2}, Hash {3,4}) = Hash {1,2,3,4}

Since this hash has been obtained by utilizing all hash of all the available transactions in the block, this Hash is called Merkle Root of the block. No more new hashes can be obtained hereafter.

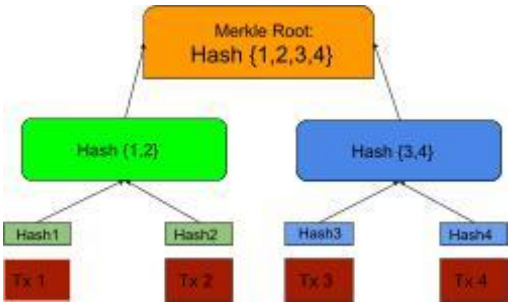
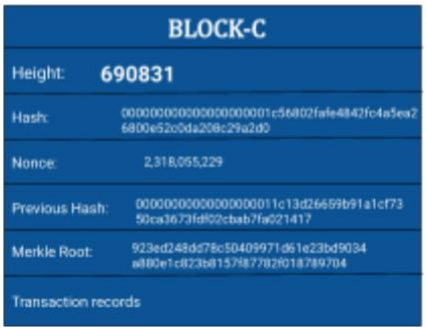


Fig 2: Merkle Tree arrangement of the Transactions in the block.

When transaction records are arranged in such a way, it becomes memory efficient and time-efficient to fetch the

ISSN: 2349 – 4891

desired transaction record. Suppose I want to access Transaction 4 (Tx_4). To access the transaction, I first have to find the Merkle root of the block which contains my Transaction. Then, instead of downloading all the transaction records, I have to find the hash of the sibling of Tx_4 which is Tx_3 in this case. Tx_3 is the sibling because the hash of Tx $_4$ and Tx_3 is used to form the combined hash. Again, we need to find the sibling hash of this combined hash. This process of finding the sibling hash goes until we reach the Merkle root of the Block. In this way, we can track our desired Transaction record, without bothering about the other records. The path followed along the Merkle tree to reach Tx_4 is called Merkle Branch for Tx_3. In the case of Fig 2, Sibling Search occurs only in the first stage. After the first stage, the Merkle root is found. In this way, we need not download the entire block. In addition to efficient organization of data, the Merkle tree also helps reduce the size of the block.



Source: blockchain.com/explorer

3. SECURITY

Once the block is added to the network, the data inside it cannot be changed. For modifying the data, another block has to be added to the chain. The already existing block cannot be deleted or modified.

The network is encrypted with a powerful encryption algorithm. Even if someone breaks through the encryption algorithm, tampering with the block is next to impossible. Here's why.

Let us take three random but consecutive blocks from a blockchain network. Let the three random consecutive blocks be Block A, Block B, and Block C.

Getting access to the data in any block is virtually impossible for any hacker. If the intruder tries to somehow tamper with the data inside block B, the hash of that block changes. Since Block C's hash is dependent on the hash of block B, the orientation of Block C also changes. The same effect permeates along with the blocks thereafter. (To the blocks after block C). This causes the Block Owner (Nodes) to get notified about the tampering attempt. How quickly the nodes get notified about the tampering depends upon the Internet speed.

To safely tamper with the data of Block B, the intruder should find a new nonce to obtain the new hash. Then the Golden Number obtained after undergoing SHA-256(Golden Hash) should gather 51 percent consensus from 51 percent of the nodes across the network. This takes around 10 minutes for Bitcoin. Then, he should also do the same process for all the blocks after C. Guessing the correct nonce (i.e Golden Nonce) for a single block and achieving the proof of work consensus is so energy consuming and tedious, let alone for the millions of blocks in the network. The time for successfully obtaining the proof of work (even if 51 percent of the nodes agree) for all the blocks in the network would be 10 minutes times x millions (x is the number of blocks in the network), which is approximately 200+ years. Even if the intruder uses the most efficient ASIC, the time per block remains 10

ISSN: 2349 – 4891

minutes (for bitcoin). The Bitcoin protocol restricts the time to 10 minutes, to prevent such fraudulent attempts.

The cost of tampering with a single block is around $10,000 (electricity consumption by the Mining engines). The same cost goes for all of the blocks, which accounts for billions of dollars. Additional costs of gaining 51 percent consensus (either by owning 51 percent of the blocks in the entire chain or by hacking into the 51 percent of block owners) are very high. The time, cost, and chances of getting busted are very high, which makes the process of tampering impossible.

The application of the Merkle tree also increases the security of the data. Even if someone gets access to 51 percent consensus (which is theoretically possible), he/she cannot tamper with the individual transaction record inside the block. Since the transaction records are arranged in Merkle Tree, if data of one record is tampered with, this causes its hash to change. Since the entire chain has interdependency upon each other's hashes to form the Merkle root, the change in one record's data demands a change in the hash of its sibling record and the entire records subsequently. Entire records' hash has to be changed, the hashing of sibling hashes has to be done once again to reach a valid Merkle root.

Let us assume the Merkle tree above. It has four transactions. For four transactions, the Merkle tree contains 7 different hashes (manually counting).

We know,
The number of nodes in a complete binary tree with N leaves is = 2N - 1
Nodes in a complete binary tree= Number of hashes possible (In case of Merkle Tree)

Leaves, N = Number of transactions stored in the block

Generally, a Blockchain contains 1000 transactions per block. So, the number of hashes in the Merkle tree of that block with 1000 transactions is 2x1000 - 1 = 1999. So, 1999 new hashes have to be formed to tamper 1 record successfully.

4. HOW CAN NEPAL MAKE USE OF BLOCKCHAIN TECHNOLOGY?

4.1. Digital Currency

4.2.1 History

The Nepalese currency is issued by the Nepal Rastra Bank, the central bank of Nepal. It was introduced in 1932, replacing the silver mohar at the exchange rate of 2 Mohar = 1 Rupee. Nepalese rupee is pegged to the Indian Rupee, which means the Exchange rate between Nepalese Rupee and Indian Rupee is fixed at 1.60 NPR = 1 INR. This means the power of Nepalese currency is dependent upon the value of Indian Rupees in the Global Economy. Indian Rupee is a free-floating currency backed by assets like Gold, Government Securities, and Foreign Currency Assets. Indian Rupee maintains its autonomy in the global market. But, the Nepalese Rupee has no autonomy because it's pegged to a significantly powerful Indian Rupee. It means an economic recession in the Indian Economy affects the Nepalese Economy as well. The control of the RBI over Nepalese Currency is such that any time Nepalese Currency and Economy can be brought into dust by the RBI. If NPR is unpegged to INR, the value of NPR becomes worthless (because NPR is not backed by tangible assets like gold). Although USD is a fiat (not backed by any asset), it is a powerful currency because of its position in Global Trade. All the global businesses use USD. USD's global dominance as a pegging currency (currently 14 currencies of different countries are pegged to the USD), has solidified its spot as a stable currency. But, NPR cannot maintain fiat standards even for a second.

Although currency pegging helps in conducting free trade between India and Nepal, it still poses a risk of Market downfall in Nepal, during the Indian market recession. There is no Economic autonomy in Nepal's position in the Global Market.

The Inflation rate of the Nepalese currency as per 2020 reports is 6.15 percent. Since the inflation of up to 3 percent per annum is considered healthy, NPR is in serious trouble with its 6.15 percent inflation per annum. The inflation rate in India and Nepal remains the same because the Nepalese Rupee is pegged to Indian Rupee.

ISSN: 2349 – 4891

Nepal Rastra Bank regulates Nepalese currency. But, it cannot regulate currency circulation for corruption, money laundering, and other criminal purposes. To regulate the source of such flows, a digital currency has to be introduced. To maintain the internal strength of the Nepalese currency, Nepal Rastra Bank should introduce a digital currency to regulate circulation. Instead of pegging the Nepalese rupee to Indian currency, Nepal should peg its currency to the USD for the time being. This will ensure Nepal's global exposure in the economic battleground and reduce economic dependencies with India. When NPR is pegged to USD, Nepal can freely conduct international trade, without fearing Indian sanctions. Whilst attempts to destabilize currency circulation inside Nepal can occur to undermine NPR's value, Nepal should enforce regulatory methods to prevent such attempts. To regulate the inflow of the Indian rupee into Nepal and to prevent the disruption by the Indian currency, Nepal should enforce effective and transparent regulatory modules. And, to date, Digital Currency is the best proposal that can regulate money circulation and prevent excess inflow and outflow of money from foreign sources, and hence prevent currency dominance. The use of Digital currency prevents Nepal from using INR, which can maintain NPR's value. Pegging to USD is safer than pegging to INR. USD global dominance will make sure Nepal's position in Global trade remains stable. The chances of facing sanctions from the US are far less than that of India. (in the context of Nepal)

4.1.2 How can Nepal make use of Blockchain Technology to enforce Digital Currency?

Nepal should enforce centralized Digital Currency. Nepal cannot afford to enact decentralized currency because of the increasing risks of market manipulation by the inflow of huge amounts of foreign money and the inability of Nepal to regulate it. So, Central Bank Issued Digital Currency should be introduced.

The proposed model is an MDR-based blockchain system for exchange between two parties within the regulatory guidelines of the Central Bank of the particular country. Let us first learn about the MDR data registration system.

The ISO/IEC 11179 metadata registry is an international standard for data interoperability. Interoperability is a property in which systems can be used interchangeably with other systems of the same or different types. The ISO/IEC 11179 Metadata Registry (MDR) is a metamodel that manages metadata through registration and authentication of metadata. The MDR (Metadata Registry) supports data element creation, registration, and management to share information between systems; it structurally supports the sharing, expression, and identification of the meaning of data and can involve interoperability using the data.

For eg; when we use the word, "Cricket", it can have two meanings, "The Sport" and "An insect". To correctly identify it as a sport or as an insect (as per the intention of the argument), the word or data cricket has to be stored in a more elaborative descriptive model. That descriptive model correctly identifies if that "Cricket" is a sport or an insect. And that, out of many descriptive models, one of the descriptive models is the ISO/IEC 11179 Metadata Registry (MDR).

In this paper, digital transactions among the 100 digital banks all across the country are explained. Those 100 digital banks are accredited by the Central Bank. The transaction among those 100 digital banks is monitored by the central bank i.e. The Nepal Rastra Bank.

When bank A sends transaction details to bank B, the data of the transaction should be understood by both of the banks to validate and approve the transaction. If transaction data sent by bank A is not operable by bank B, then the transaction cannot occur. It's like if I speak Nepali with my non-Nepali-speaking Korean friend. The Korean friend would have no idea what I am trying to say, and he would thus disregard my Nepali words. So, I should speak in a language which both of us understand i.e. English. The purpose of ISO/IEC 11179 Metadata Registry is to ensure that both the communicating parties (banks in this case) can understand, validate and approve the transaction data successfully, thus obliterating ambiguity. MDR can finely express the data and represent it to the Concept Layer and Representation Layer. We can identify the data in its actuality, using the MDR. MDR helps maintain the integrity of data. So, the ISO/IEC 11179 Metadata Registry is for the purpose of removing ambiguity and maintaining interoperability between the systems.

ISSN: 2349 – 4891

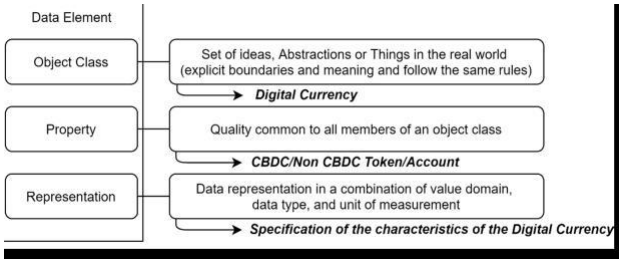


Fig 3: Data Element structure in MDR

(Source: Martínez, V.G., Hernández-Álvarez, L. and Encinas, L.H. (2020). Analysis of the Cryptographic Tools for Blockchain and Bitcoin. *Mathematics*, [online] 8(1), p.131. Available at: https://www.mdpi.com/2227-7390/8/1/131)

Data is expressed as shown in the figure above.

Eg; If the Data is the Central Bank Digital Currency of Nepal, then the MDR registry:

Data Element: Central Bank Digital Currency of Nepal
Object Class: Digital Currency
Property: CBDC (Central Bank Digital Currency)
Representation: Digital currency with interoperability

The data value of the MDR is expressed using a conceptual domain and a value domain. The figure below shows the relationship between the Conceptual Domain and the Value Domain. The MDR expresses the data in the descriptive or enumerated form. The descriptive form expresses the data values in the Described Conceptual Domain and Described Value Domain. The enumerated form expresses the meaning of the data in the Enumerated Conceptual Domain, Value meaning, Permissible value, and Enumerated Value Domain. The CBDC can represent data using enumerations. For example, Digital Dollar expresses itself as Dollar and Cents units (100 Cents = 1 Dollar). The digital rupee expressed itself as the Rupee and Paisa unit. (100 paisa = 1 rupee)

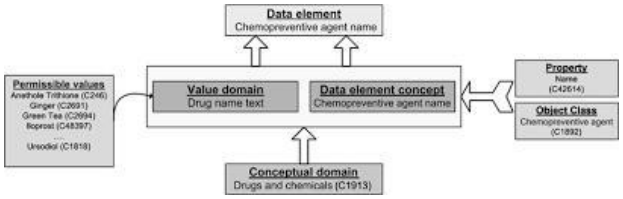


Fig 4: Data representation in MDR

The central bank manages and approves the registration of the MDR from respective banks. The Central Bank forms a working committee that focuses on approving the MDR. The committee agrees on Identification, Submission, Checking, and confirmation. After this, it can approve and register the Bank Data in the MDR.

In the Blockchain network, the accredited banks work as the nodes. The Central Bank however has the power to reject the consensus made by the accredited banks. This is an exceptional case for the Nepalese economy to maintain the integrity of the transaction block. Thus,

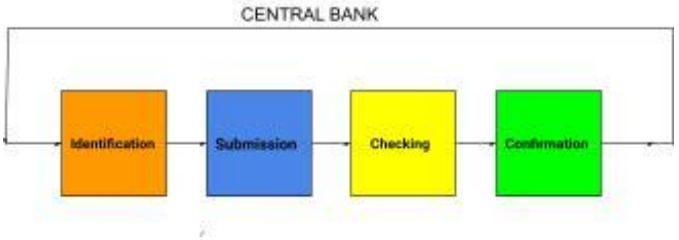


Fig5:Registration Procedure in CBDC

currency manipulation and unhealthy influx from anonymous sources are prevented.

If Person A sends Nrs X to Person B through Bank A, the translation details are entered in a contract by Bank A. The contract contains Transaction Public Key, Private Key, and a hash. Key Algorithm is used to generate necessary Public Key and Private Key. DES, AES, RSA are some of the cryptographic key algorithms. The private key of the contract cannot be calculated from the Public key of the same transaction sheet or contract. This is the feature offered by Asymmetric Encryption. In Bitcoin, the transaction private key (i.e Owner's Digital Signature) is calculated using the Previous Transaction's Public Key and Private Key. Such protocol shall be set up in the Nepal CBDC. This helps to maintain the immutability of the transaction sheet. The hash can be created using a Hashing Algorithm like SHA-256. Since the transaction setup and verification is a private process involved within the Central Bank's responsibility, the private function has to be created. No other entity in the world should have the access to that unique Hashing Algorithm.

ISSN: 2349 – 4891

The transactions are validated as Clean and Unclean by the nodes (i.e. Banks). Data in the transaction contract is written in accordance with ISO/IEC 11179 Metadata Registry. All the banks, through the 51 percent consensus method, validate the transaction and send it to the Central Bank for Block formation. Bank-1 cannot validate the transaction alone. This provision decentralizes the banking power of private banks. After consensus from 51 percent of the Banks, CDBC again verifies whether the transaction is clean and then forms a block that encloses the transaction contracts. The verification committee inside the Central Bank adds the Block to the chain after a series of processes as shown in fig: 6.

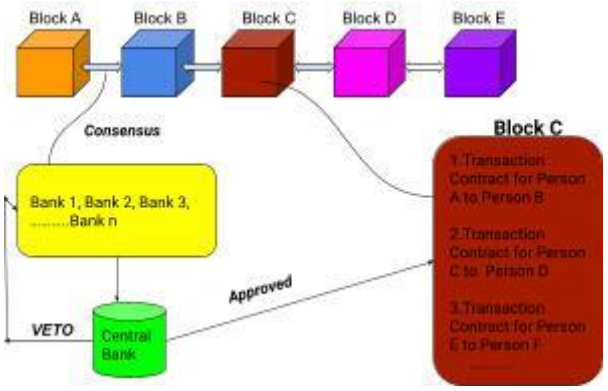


Fig 6: Blockchain Model for CBDC transaction in Nepal

The transactions are compiled into the block. The size limit for the block can be set as per the capacity of the data centers and the size of transaction contracts. The number of transactions inside one block depends upon the size of a transaction contract and the storage capacity of the Block.

A transaction contract with details like Public Key, Private Key, Hash, Sender-Receiver details, Amount details will not exceed 1000 bits. The limit can be set by Network Protocol. The protocol has to be issued by the Central Bank. The size of 1 block is 20kb to 30kb in the case of ethereum and 1 MB in the case of the Bitcoin Network. The lower size of the block means less time to add the block into the chain. So the recommended size of the block is 10 to 20-kilo bits so that the block is attached to the network within 1 second.

Let us assume that the Central Bank sets the size of 1 block as 20 kilobits and the size of 1 transaction contract as1 kilobit in its protocol. Then 1 Block contains 20 transactions. If 1 block is added to the network in 1 second, then 20 transactions can occur in 1 second. 20 transactions per second are the limit for that CDBC network, i.e. for that country. CPUs as of today can easily add 1 block (20-kilo bits) into the network in 1 second, with bare minimum electricity cost.

Size of the block ∝ Time taken to add the block

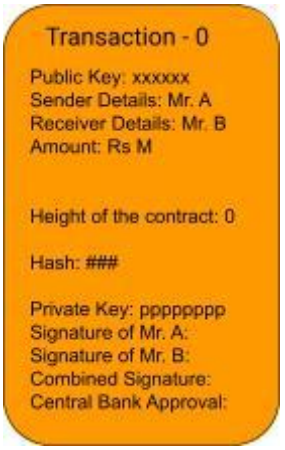


Fig 7: Transaction Contract

A number of such transaction contracts are enclosed within the block. The Banks through which transactions occur, verify the correctness of the transaction and send it to CDBC for approval and block formation. After the CDBC approves the transaction, it (CDBC) forms the block and adds to the network (see Fig 1). This entire process marks the success of 20 transactions under that 1 block. Adding a block takes around 1 second. (this time is determined by the assumption made in the previous paragraph).

The block network is a public network. The block interconnectedness and the security of the chain have been previously explained. Users can check if their transaction has successfully been accomplished. The name is not disclosed in the public network. Instead, the transaction is labeled by Public Key. The User has access to the public key and Private Key. The public key and Private key are provided to the user via SMS or Mail, once their transaction contract is created by the bank. Users can view their transaction contract via their Public Key and Private Key. The private key can serve as a password or a password can be algorithmically generated by the Central Bank. Password Algorithm (a Function)

ISSN: 2349 – 4891

should create the password by plugging in Public Key, Private Key, and Hash as the domain of the function. Password Algorithm (Public Key, Private Key, Hash) = Password.

We can observe that the Central Bank has been centralized with absolute control over the transactions. The Banks only have the responsibility of burning the digital cash (when the money is sent) and mining (when the money is received), and creating clean transaction contracts. The Central Bank has the responsibility of cross verifying the cleanness of the transaction, forming a block, and adding the block to the network. This is done to prevent the monopolization of a few banks. Bank monopoly results in centralization of Banking power among those banks and the Central Bank is left with few options to regulate such monopoly. In such cases, the illegal circulation of money cannot be easily tracked by the Central Bank. Foreign Cash inflow can cause the Nepalese currency to go obsolete. Corruption money cannot be seized easily. Centralized Digital Currency solves these problems. The Central Bank can fully maintain the integrity of transactions and ensure the security of the National Currency.

5. DISCUSSION

This paper has presented how blockchain technology works and how this technology can be used to improve Elections and Money Circulation in Nepal. Creative use of cryptographic hashing, encryption (Symmetric Encryption and Asymmetric Encryption), proof of work consensus, and decentralized features has made Blockchain Technology valuable than ever in the world where cyber-attacks and monopolies are prevalent almost everywhere. As proposed earlier, Centralized Blockchain for Digital Currency and election provides the country with efficient regulatory powers to maintain the integrity of the service. As we have expressed earlier, Nepal cannot afford to enact decentralized currency due to the risks of currency manipulation from unknown sources and the inability of the government to regulate it. Nepal cannot lose the hold of the Blockchain boom as it had missed the Electronics and internet boom. We have to enforce the technology to ensure efficient and secured services over all of the Nation's faculties.

6. CONCLUSION

The overwhelming craze over Blockchain is justifiable. The landmark of scope it provides, the problem it serves, the transparency it offers, and the security it enhances, have been the key behind Blockchain creating headlines in the international community. Blockchain is here to stay like the Internet. Yesterday the Internet created many multinational tech companies and today, Blockchain resembles the exact same trend as the Internet had shown earlier. Although Blockchain is just one of the subordinates of the internet, it has the potential to encapsulate all the other subordinates of the internet ranging from Communication to E-commerce. Nevertheless, we can extrapolate Blockchain's application's increasing curve to experience heights that no boom has ever experienced so far and its deflection/saturation point seems to be far-future stuff.

7. REFERENCES

[1] Catalini, C. & Gans, J., 2016. Some Simple Economics of the Blockchain.

[2] Jung, H. & Jeong, D., 2021. Blockchain Implementation Method for Interoperability between CBDCs. *Future Internet*, 13(5), p.133.

[3] Nakamoto, Satoshi., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

[4] Eyal, I. and Sirer, E.G. (2018). Majority is not enough. *Communications of the ACM*, [online] 61(7), pp.95–102. Available at: https://dl.acm.org/citation.cfm?doid=3234519.3212998.

[5] Study carried out by the Data Science Practice Special thanks to Pierre-Edouard THIERY How to represent a Blockchain through a mathematical model? (n.d.). [online]. Available at: https://canopee-group.com/wp-content/uploads/2020/05/Blockchain-Coperneec.pdf.

[6] Martínez, V.G., Hernández-Álvarez, L. and Encinas, L.H. (2020). Analysis of the Cryptographic Tools for Blockchain and Bitcoin. *Mathematics*, [online] 8(1), p.131.

ISSN: 2349 – 4891

Available at: https://www.mdpi.com/2227-7390/8/1/131

[7] www.federalreserve.gov. (n.d.). *Central Bank Digital Currency: A Literature Review*. [online] Available_at: https://www.federalreserve.gov/econres/notes/feds-notes/central-bank-digital-currency-a-literature-review-20201109.htm.

[8] MIT Digital Currency Initiative. (n.d.). *"Redesigning digital money: What can we learn from a decade of cryptocurrencies?" by Robleh Ali and Neha Narula of the Digital Currency Initiative*. [online] Available_at: https://dci.mit.edu/research/2020/1/22/redesigning-digital-money-what-can-we-learn-from-a-decade-of-cryptocurrencies-by-robleh-ali-and-neha-narula-of-the-digital-currency-inititaive.

[9] Auer, R. and Böhme, R. (2021). *BIS Working Papers No 948 Central bank digital currency: the quest for minimally invasive technology*. [online] . Available at: https://www.bis.org/publ/work948.pdf.

Please cite this article as Reyan Kumar Sapkota St. Xavier's College, Maitighar, Kathmandu (2021). BLOCKCHAIN TECHNOLOGY: THE REVOLUTION THAT THE DIGITAL NEPAL DESERVES. *International Journal of Recent Research and Applied Studies*, 8, 9(3), 12-27

Please cite this article as:

Reyan Kumar Sapkota, St. Xavier's College, Maitighar, Kathmandu (2021). BLOCKCHAIN TECHNOLOGY: THE REVOLUTION THAT THE DIGITAL NEPAL DESERVES *International Journal of Recent Research and Applied Studies*, 8, 9(3), 12-24.