



# BLOCKCHAIN FOR SECURITIES EXCHANGE BOOKING AND REGISTRATION

#1 SYED MEERSUBANALI, Assistant Professor,  
#2 MOHAMMAD ZIAUDDIN, Assistant Professor,  
#3 KOMUROJU ANJALI, Assistant Professor,  
Department of CSE,

TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLI, TELANGANA.

## ABSTRACT:

The Data Trust Portal (DTP) by O'Hara is based on web observatories, as seen in this figure. Data storage is not necessary for the data transfer protocol (DTP). Instead, it is the responsibility of the data owners to ensure the security of their data and to choose and implement a suitable interface method for access. The DTP platform makes it simple to design a secure method of data discovery and transfer. The protocol's metadata details the information's attributes and where it came from. The research conducted by Stalla-Bourdillon et al. offers a methodical strategy for addressing the issue of data efficiency. The authors argue that this framework should include detailed instructions on data governance responsibilities and procedures. Data trust is graphically represented with three levels.

**Keywords:** Securities Exchange, Stock Exchange, Blockchain, Distributed Ledger, FinTech, RegTech,

11430

DOI Number: 10.48047/nq.2022.20.8.nq221183

NeuroQuantology 2022;20(8):11430-11435

## 1. INTRODUCTION

A securities exchange can be defined in a number of ways. Its name alone tells you if it's a digital or physical stock and bond exchange. Stock exchanges provide a number of vital purposes in advancing economic development.

Stock exchanges have used their infrastructure, including data transmission technology, to move cash and securities for the past 50 years. Deep learning has improved algorithmic or "robotic" trading. FinTech, or financial information technology, has always affected the stock market. Given the computerized nature of stock market activities and the sharing and display of ownership data, data security is essential. This is wonderful news for the "Sealed Envelope" project, which uses blockchain technology and "Bit Commitment" to develop cryptocurrencies and smart contracts.

DLT is a blockchain that is an offshoot of Bitcoin. Cryptocurrency's "The Blockchain" has spawned multiple iterations. Blockchain technology is being investigated and possibly implemented by financial, regulatory, and legal technologies to safeguard confidential client data.

One Proof-of-Work (PoW) mathematical challenge that is utilized to protect BC's digital transaction

record is Adam Back's HashCash. BC's dynamic Public Key mechanism protects users from prying eyes. The British Columbia Protocol includes software for distributed systems and networks as well as cryptography algorithms.

Is it possible to settle and clear securities using blockchain technology? You need to understand both the theoretical and practical aspects of blockchain technology in order to respond to this question. First and foremost, I need to comprehend how and why encryption functions, how financial ledgers are made to be impenetrable, and how democratic governance operates. We'll answer the following queries.

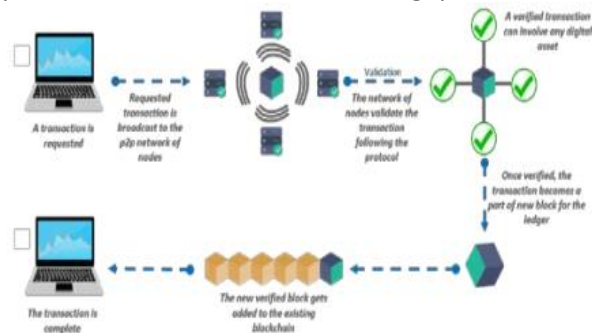


Fig. 1. A Simple Blockchain Transaction

## 2. BLOCKCHAIN: THE WORLD WIDE LEDGER

Blockchain echo systems were first introduced by



Bitcoin, but others have since adopted them. Metal rings are elevated and connected by digital ledgers. We'll examine how Bitcoin BC varies from previous versions here. Blocks, not metal rings, are used in blockchains. Every block had a defined transaction time. As seen in Figure 1, many nodes validate BC p2p transactions. New blocks include validated transactions. After a fresh block has been added and the Proof-of-Work problem has been fixed, the transaction is finished. Before being added to BC, more blocks are sent to other nodes for confirmation. Every node has a legitimate BC. We must first comprehend block internals in order to comprehend this method. Node certification and verification, along with other procedures in the BC ecosystem, are governed by initial block-specific smart contracts. It's possible that transactions using "mined" currencies took place in the beginning of the ecosystem.

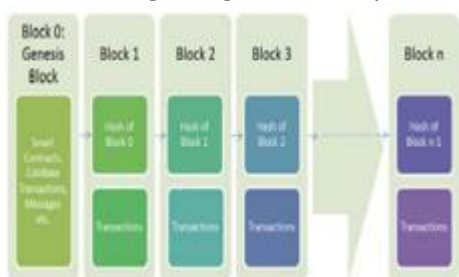


Fig.2. A straightforward Blockchain transaction follows.

By offering a strong basis that forbids centralized control and permits anybody to write, Bitcoin BC removes manipulation.

Proof-of-Work mining is used to create Bitcoin BC blocks. Calculating the block hash is necessary to finish a Proof-of-Work challenge. Miners solve the PoW by using their processing power. Because earlier blocks could be finished in ten minutes or less, this was challenging. In PoW puzzles, the hash of the current block is contained in the block header.

The following details about a block's transactions are displayed in Figure 3: version number (4 bytes), date, once, current difficulty level bits, Markel root hash, and previous block hash (256 bytes).

The Bitcoin BC mining pool or node, which may be operated through smart contracts, is open to anybody with a computer. BC nodes use local databases to access public ledgers. Nodes in a peer-to-peer network work together to create an unchangeable chain. By lowering SPF, nodes improve the fault tolerance of the BC ledger.

If a node has both a public and private cryptographic key, it can complete a transaction. After the first node "digitally" signs the transaction using its private key, all other nodes "verify" it by decrypting it using their

public keys. The entire network will get a broadcast of the public and private keys. By protecting integrity, avoiding nonrepudiation, and abstracting users' identities, asymmetric cryptographic authentication helps network users. Nodes must handle private keys correctly for asymmetric key cryptography to remain secure. Nodes in a BC ecosystem use pre-established protocols to communicate with one another.

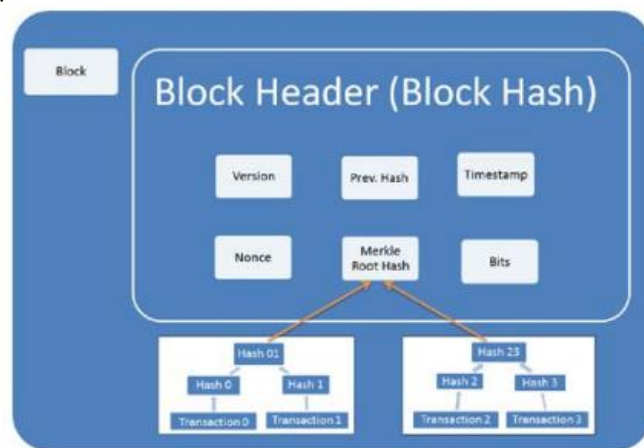


Fig. 3 More compact block diagram.

- Only single values are permitted by hashing.
- A hash computation cannot be used to recover the original input data, even if the algorithm is understood. A fixed-size "hash" can be created from any size of data. The hash is unaffected even if one bit is changed. Improved hash algorithms ensure that no two inputs ever have the same hash result because of the extremely low collision probability. Ethereum BC and Bitcoin BC both use the SHA-256 blockchain technology. 256-bit digests are produced by both methods. If the calculated hash is different from the supplied hash, the recipient rejects the transaction or block. Because hashing detects modifications to blocks, the Blockchain is safe and unchangeable. In the absence of a bank, BC serves as a Trust Machine, guaranteeing that parties to a transaction can have faith in one another.
- Figure 3 shows how BC can use hash functions, like bank account numbers, to identify addresses and transactions. Instead of using transaction hashes, Merkle Tree employs root hashes. BC ecosystem units are identified by their distinct, unchangeable hash values.
- Since each block contains the hash of the previous block, you are unable to change transaction data from earlier blocks. The immutability of BC is due to the Proof-of-Work consensus method, which is very energy and power intensive. The raw transactions of blockchain candidates were verified and examined. By appending the nonce to the anticipated value of the block header hash,



the miner fixes PoW. The process is repeated after increasing the nonce by one if no matches are discovered during the search. The miner who finishes the Proof-of-Work challenge first creates and publishes the block. Every node examines the block it has been allotted. It will be connected to other nodes to create a block once it has been greenlit. All nodes will thus always have access to the most recent version of the blockchain. If malicious nodes are outperformed by honest nodes in terms of processing power, the BC is secure. If a dishonest node's PoW solution does not match their raw transactions, nodes will reject it.

- The hash from the preceding block is included in the current block due to BC's chronological chaining. As a result, the hash of the current block is equal to the sum of the hashes of all earlier blocks. It takes a lot of processing power to solve a Proof-of-Work (PoW) problem, where you have to change one block without changing the others. These illustrations demonstrate how this BC treatment approach renders it unchangeable:

### The Double Spending Problem

- False nodes exploit the process, such as Trudy Double Spend. Trudy not only gives bitcoins to a shop, but also to a trusted friend or herself.
- Trudy tells the store one side of her financial tale while hiding the other. After the payment has been collected and added to the "honest" block, the store will ship. Under the radar, Trudy is replacing little retail payments with larger ones. The "Longest Chain Rule" encourages trustworthy nodes to join Trudy's secretly longer link, which she subsequently leverages to her advantage. When the bit coins are spent, the "honest" block becomes a "orphan," rendering the merchant's payment null and void. A pair is available.
- Problems with the allowance. Because "dishonest" obstacles are more difficult to overcome, PoW decreases double expenditure. To generate the block hash, which is required for building the new block, Trudy must solve the Proof-of-Work at the current level of difficulty. The "honest" miners will continue to work, eventually producing more honest blocks. Trudy requires a lengthier block to pass. Trudy may take longer to solve the PoW than other nodes. Trudy also has to get herself some robust tools. Spending twice is difficult.
- Blockchains, such as Trudy's BC network, are unable to change data because to Proof-of-Work and Longest Chain Rules.

### Deluding an Audit Team

The goal is for Trudy to deceive an auditing team by impersonating the offline chain. Trudy is interested in either growing or concealing offerings. Changes to the transaction block are necessary for transaction hiding. She is unable to add the fraudulent transactions to the final block because they are timestamped consecutively and concatenated. Her role is to identify the transaction's time and date components. A 100-block chain must have block 45 changed. following Trudy makes the appropriate adjustments following the block's hash (#45), the block will fail, rendering all hashes from #46 to #100 invalid. To validate the chain, the auditing team only needs to recalculate the hashes of recent blocks.

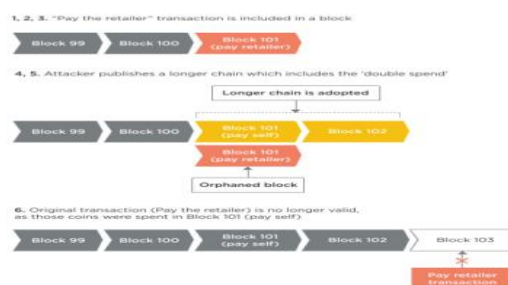


Fig. 4 Consequences of double spending

- By recalculating all subsequent block hashes, Trudy can fool the audit team into believing she has regenerated the block. In blockchain-based (BC) ecosystems such as Bitcoin, every transaction requires the solution of computationally intensive PoW puzzles. Block-adding authority is distributed sequentially and randomly in Multichain and other BC ecosystems. Block adders are represented in digital form as symbols. The private keys of all adders are required to reassemble the jigsaw puzzle parts. Rebuilding the blocks will be challenging in both circumstances.
- Assume Trudy changed or hidden transactions so that we could rebuild the block. The auditing team will not engage in any type of deception. If you know the hash of any recent Trudy's BC block, you can quickly compare it to the block of any unfriendly player. If these two hashes do not match, the audit team will be able to determine whether there has been data corruption throughout the chain.
- The read/write rights distinguish the three versions of the blockchain.

### Public(Permissionless)Blockchain

- Anyone can participate in the ecosystem of public blockchains. Nodes has the capacity to read and write. Bitcoin, Ethereum, Blockstream, and Factom are among the companies that make up this Blockchain ecosystem. Legally Authorized



## Private Blockchain

### Private(Permissioned)Blockchain

- To participate in a private or permissioned blockchain, you must be a "trusted" node with read and write access. Write permissions can be assigned to nodes and locations. Eris Industries, Chain, Multi Chain, and Blockstack are all instances of private blockchain ecosystems. In 2015, Chain and NASDAQ employed blockchain technology to issue and transfer shares of private firms. Chain began issuing and transferring shares using the NASDAQ Private Markets (NPM) private ledger technology. BC reduces the necessity for a mediator by developing mutual confidence between the two people. Private BC has violated the target.

### Hybrid(Consortium)Blockchain

- Blockchain networks can be private or mixed, as long as they allow write access and maintain consensus. Even though fewer nodes can contribute to a hybrid blockchain, consensus is maintained. Unlike private blockchains, hybrid blockchains allow for open read access. Markets prefer hybrid blockchains, which combine the greatest aspects of the two primary varieties.

## 3.EVOLUTION OF SECURITIES EXCHANGE

Stocks can be traded on a securities exchange, which provides numerous benefits, including high liquidity and minimal transaction fees. Typically, brokers and dealers handle stock transactions. Securities exchanges are governed by both internal and external regulations. These characteristics reduce the likelihood of errors, fraud, and bankruptcy.

A country may have multiple securities exchanges, based on considerations such as location and the needs of the financial system. The first stock market opened in Amsterdam in 1602. Some of the most well-known market exchanges are NASDAQ, the New York Stock Exchange, Euronext, the London Stock Exchange Group, the Shanghai Stock Exchange, the Japan Exchange Group, and the Hong Kong Stock Exchange. The entire market value increased by 22.6% in 2017, reaching \$87.1 trillion.

Because of the enormous volume of transactions, stock exchanges have difficulty ensuring accuracy and security. On the Hong Kong Stock Exchange, settlement transfers and order matching are two forms of high-volume stock market operations that generate \$1.24 billion every day. Digital recordkeeping and remote data transfer have made internet trading the standard. Concerns about hacktivism, cyberwarfare, and illicit hacking have

heightened the need of stock market security. Given the rapid advancement of new technology, it is more necessary than ever to have a solid understanding of the stock exchange's history. It appears that private networks are gradually replacing public marketplaces, indicating a shift from corporation to market to business. Institutions have always existed, both official and informal. Despite the effects of legislation and technical improvements, broker-dealers' self-interest has persisted throughout this age. For nearly a millennium, traders of all sizes have participated in the securities market. As a result, direct commerce became increasingly common. From 1800 to 2000, private corporations established what were basically public "exchanges" to facilitate commerce. Private matching venues emerged in the early 2000s, following the development of electronic platforms by well-known brokers using cutting-edge technology.

Initially, stock exchanges were monopolies that only members could join. Legislation established openness, oversight, and governmental dominance. By the end of the century, technological advances and legislative improvements have enabled the largest broker-dealers to develop their own trading matching systems, allowing them to circumvent the exchanges' open egalitarianism.

## 4.APPLICATION OF BLOCKCHAIN INSECURITIES EXCHANGES

The main stock markets have shown their support for BC. BC was initially introduced by NASDAQ. The Australian Securities Exchange (ASX) intends to replace CHESSE with BC in 2020 or 2021. HKEX and ASX have joined forces to reduce costs by leveraging blockchain technology. The London School of Economics is also heavily using BC. The LSE and IBM, the open-source blockchain industry powerhouse, announced their partnership in July 2018.

Our securities exchange operations use a hybrid BC that combines point-of-sale matching and randomized round robin settlement.

Broker-dealer-operated central exchanges can match purchase and sale orders, but clearing and settlement are handled by the central counterparty clearing house. The "closed circle" CCP nodes will manage decentralized "back office" functions.

According to its technical anatomy, the second component of BC could assist stock exchanges.

Compared to stock exchanges, this hybrid distributed BC approach offers ledger holders greater transparency. Nonetheless, transparency may be

lower than in a public Blockchain.

To create a dependable market, BC can use time markers, cumulative hashing, and chronological blocks.

The purchase will be overseen by engineers from the BC system. Traders and merchants will trust the BC if it is fair and the design and operation can be verified.

Long-term transaction costs are lower since BC technology has a lower initial cost and requires less maintenance than previous systems. Because updating an old system requires a financial investment, there are no immediate savings. For years, they will have to pay for the new system before using it.

Schedules for intraday stock market settlements. The majority of exchanges provide settlement on the same day. the initial two or three days of the T+2 phase. At time plus three, the money and asset transfers are complete. To avoid legal issues, brokers and sellers should "allow" numerous share transfers during settlement. China's demand for verifiable cash prior to agreement execution helps to expedite immediate payment. BC can automate post-trade processes. Securities settlement occurs instantly, which increases supply chain efficiency, liquidity, transparency, and trust. How much will it cost firms to provide securities?

According to accounting statements, blockchain technology would encourage more investment in market rearrangement by lowering transaction costs and post-trade inefficiencies.

Because of its numerous benefits, British Columbia is drawing market participants and regulators. Young people in British Columbia present new issues in the fields of law and regulation, which authorities are only now becoming aware of. Legal and regulatory challenges may occur in British Columbia as a result of data localization and scalability in specific countries.

The clearing and settlement processes must be strictly regulated. They started out split. In contrast to British Columbia, current law views them as a single, multi-stage transaction.

Because the terms "dematerializing" and "tracking claims" have different conceptual meanings, legislators and regulators must create separate laws. Use digital DLT transactions instead of physical certificates to keep track of ownership changes. Digital tokens that can be transferred can be considered uncertified securities. Tokens are not yet considered securities, hence they have no monetary value. Because it is an invention, the token is exempt from shareholding limits. Owners have physical possession of their shares since they are registered on

a genuine share registry that does not use the BC ledger or other distributed ledger technology (DLT) to track digital tokens. To function as legitimate share registries, digital ledger technology (DLT), such as BC ledgers, necessitates a new statute.

## 5. CONCLUSION

Implementing private blockchains demands "pressure and budget to build anything connected to blockchains." Instead, we considered whether BC's admission would benefit financial markets. From a regulatory and technical standpoint, how can blockchain technology improve securities registration and settlement on stock exchanges? We investigated the prospect that alternative Blockchain implementations could facilitate stock market transactions. This study establishes a hybrid BC strategy by combining securities exchange operations and the development of BC technology. Further research will be performed into the potential legal repercussions of stock exchanges embracing blockchain technology.

The Han Kong University Centre for Financial Regulation and Economic Development is financing this research.

11434

## REFERENCES

1. David C. Donald, The Hong Kong Stock and Futures Exchanges: Law and Microstructure, 1st ed. London, UK: Sweet & Maxwell, 2012.
2. T. Lunghi et al., "Experimental Bit Commitment Based on Quantum Communication and Special Relativity," *Physical Review Letters*, vol. 111, no. 18, pp. 180504-180508, November 2013. Available: <https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.111.180504>
3. Mahdi H. Mirzazand Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency," *Annals of Emerging Technologies in Computing (AETiC)*, vol. 2, no. 1, pp. 1-6, January 2018. Available: <http://aetic.theiaer.org/archive/v2n1/p1.pdf>
4. Sarah Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15-17, November 2016. Available: <https://doi.org/10.1145/2994581>
5. Mike Sutcliffe, "An overview of Blockchain applications — this is just the beginning!," *Blog 2017*. Available: <https://twitter.com/MikeSutcliffe/status/912382978680082433>
6. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder,



- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, 1sted.New Jersey,USA:Princeton University Press,2016.
7. Ghassan Karame and Elli Audroulaki, Bitcoin and Blockchain Security, 1st ed. Massachusetts, USA: Artech House, Inc., 2016.
  8. Md Mehedi Hassan Onik, Mahdi H. Miraz, and Chul-Soo Kim, "A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0," in Proceeding of Smart Cities Symposium (SCS-2018), Manama, Bahrain, 2018, pp.11-16.
  9. S.Asharaf and S.Adarsh, Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities, 1<sup>st</sup> ed. Pennsylvania, USA: IGI Global, 2017.
  10. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, White Paper 2008. Available: <https://bitcoin.org/bitcoin.pdf>

