Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 12, No. 2, (2021),
ISSN : **1906-9685**

BLOCKCHAIN IN SECURITIES EXCHANGE BOOKING AND REGISTRATION

[#1]**Dr. N. PRABHAKARAN,** Professor, Department of Computer Science and Engineering,
[#2]**BURLA SRINIVAS,** Associate Professor, Department of Computer Science and Engineering
MOTHER THERESA COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TS.

ABSTRACT: When the securities exchange goes online, information and data security become critical concerns. Because Blockchain (BC) technology is distributed and unchangeable, the "Trust Machine" no longer requires third parties. This study looks into how Blockchain can protect stock exchange transactions, with an emphasis on technological and legal aspects. Given the complexities of securities exchange operations, the research suggests designing, developing, and implementing a hybrid BC tailored to each stock exchange. According to the research, such BC has numerous advantages over other techniques. However, when building a BC application, the country's legislation and regulations must be taken into account.

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

1.INTRODUCTION

There are several ways to define a securities exchange. The name implies it is a real or virtual stock and bond trading facility. Stock exchanges play many important functions in economic development.

For 50 years, stock exchanges have used its infrastructure, including data transmission technology, to contract and move securities and cash. Deep learning has improved algorithmic or "robotic" trading. FinTech, or financial information technology, has long affected the stock market. Data security is important because stock exchange transactions and ownership data are exchanged electronically and shown electronically (with certificates or not). This makes the "Sealed Envelope" based on "Bit Commitment" and Blockchain applications like crypto-currencies and smart contracts promising.

Bitcoin spinoff DLT is a Blockchain. Many Blockchain versions have emerged from "The Blockchain" of Bitcoin. Blockchain technology is being studied and applied in FinTech, RegTech, and LegalTech to protect sensitive data and consumer privacy.

BC's digital transaction record is protected by Proof-of-Work (PoW) mathematical conundrums like Adam Back's HashCash. BC's dynamic Public Key ensures user privacy and anonymity. BC includes technology like:

Cryptography Algorithms
Dispersion of Systems and Networks
Program, etc. BC protocol.

Blockchain for securities clearing and settlement? This question requires understanding blockchain technology's theoretical and practical capabilities. The first question is how democratic control of booking ledgers works, how the ledger architecture prevents manipulation, and what encryption is and why it works. Questions will be answered below.

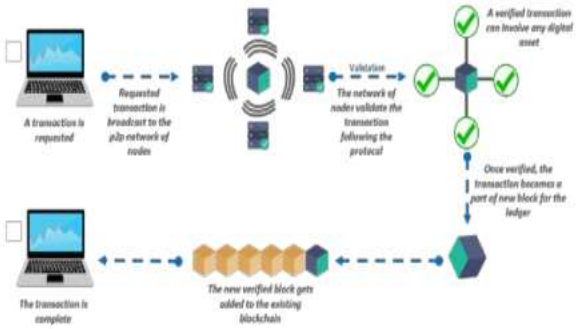

Fig. 1. A Simple Blockchain Transaction

2. BLOCKCHAIN: THE WORLD WIDE LEDGER

Bitcon pioneered blockchain echo systems, but others exist. Blockchains bind and lift metal rings. This section compares Bitcoin BC to older versions. Blockchains use blocks instead of metal rings. Each block had a set transaction time. Multiple nodes verify BC p2p transactions (Figure 1). New blocks contain confirmed transactions. The transaction is complete when the Proof-of-Work difficulty is resolved and the new block is inserted. Other nodes receive new blocks for verification and BC inclusion. Every node has a valid BC. We must grasp block internals to understand this strategy. Initial block-specific smart contracts regulate node validation, verification, and other BC ecosystem processes. When the ecosystem started, coins "mined" may have transactions.

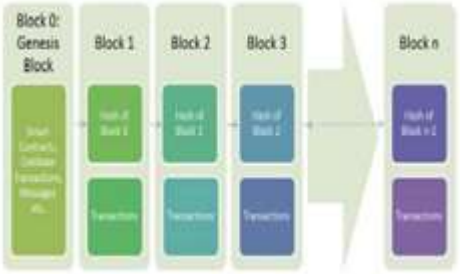

Fig:2. A straightforward Blockchain transaction follows.

To prevent manipulation, Bitcoin BC's solid foundation prohibits centralized control and allows everyone to write.

Proof-of-Work Problem mining generates Bitcoin BC blocks. A Proof-of-Work problem is "completed" by computing the block hash. Miners solve PoW with computing power. It took 10 minutes or less to solve earlier blocks, making this difficult. For PoW puzzles, block headers carry the current block's hash.

Figure 3 shows the version number (4 bytes), prior block hash (256 bytes), date, once, current difficulty level bits, and Markel root hash of a block's transactions.

Bitcoin BC nodes can be smart contract-powered, and anyone with a computer can join the node or mining pool. BC nodes use local databases as public ledgers. P2P network nodes collaborate to immutably chain. Nodes reduce SPF, boosting BC ledger fault tolerance.

Any node with private and public cryptographic keys can transact. The initiating node "digitally" signs the transaction with its private key, and the other nodes "verify" by decrypting it with their public keys. Every public key and private key will be broadcast over the network. Asymmetric cryptographic authentication provides identity abstraction, integrity, and non-repudiation to network users. Nodes must properly handle private keys for asymmetric key cryptography to be secure. BC ecosystem nodes communicate using network protocols.

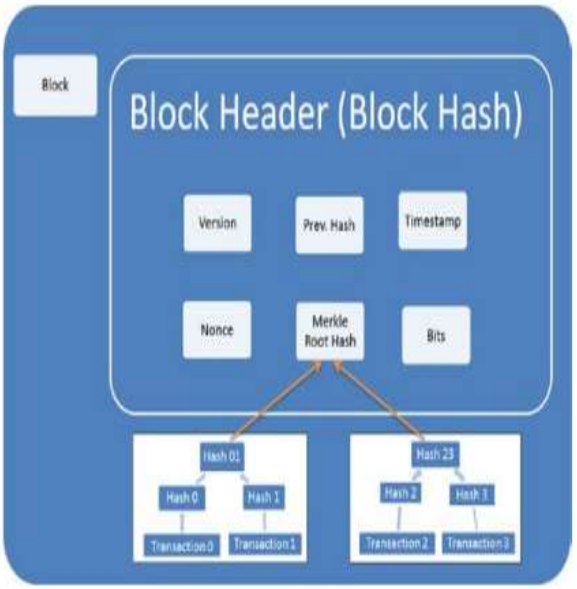

Fig. 3 More compact block diagram.

- Only solitary values are accepted for hashing.
- A hash computation cannot recover the original input data, even if the algorithm is understood. Data of any size can be used to compute a fixed-size "hash." Changing one bit

doesn't affect the hash. Superior hash functions prevent inputs from having identical hash values due to low collision probability. Ethereum BC utilizes Keccak-256, Bitcoin BC SHA-256. Both processes produce 256-bit digests. If calculated hash differs from included hash, recipient rejects transaction or block. Hashing, which detects block changes, makes the Blockchain secure and unchangeable. BC operates as a Trust Machine to ensure transaction parties trust each other without a bank.

- Hash functions help BC identify addresses and transactions (like bank account numbers; Figure 3). Merkle Tree replaces transaction hashes with root hashes. BC ecosystem units can be identified by their immutable hash values.
- Transaction data from older blocks cannot be modified since each block contains the hash of the prior block. BC's immutability comes from the Proof-of-Work consensus protocol, which requires a lot of computational power and electricity to hash. Verified and certified raw transactions are added to blockchain candidate blocks. To fix PoW, the miner adds the nonce to the block header hash value that matches the expected value. When a match is sought but none is discovered, the nonce is raised by one and the procedure is repeated. The first miner to solve the Proof-of-Work challenge creates and broadcasts the block. Nodes check the proposed block. If approved, more nodes will chain it together to form a block. Every node will always have the most recent blockchain thanks to this. If honest nodes outperform malevolent nodes in terms of computing power, the BC is secure. Because it does not match their raw transactions, the other nodes will reject a dishonest node's PoW solution.
- The hash of the previous block is present in the current block due to BC's chronological chaining. The current block's hash is therefore equal to the sum of all previous blocks' hashes. A Proof-of-Work (PoW) puzzle must be solved in order to change a single block without also changing all subsequent blocks, which uses a lot of computer power. These instances show how this method for dealing with BC makes it unchangeable:

The Double Spending Problem

- False nodes take advantage of the system, like Trudy Double Spend. Trudy provides herself or a trusted friend bitcoins in addition to giving a store bitcoins. Trudy tells the shop about one of her finances while keeping the other secret. When a payment is received and added to a "honest" block, the store ships. Trudy is subtly substituting a bigger block for retail payments. The "Longest Chain Rule" tempts dependable nodes to adopt and prosper on it when Trudy advertises her covertly longer chain. When the bit coins are spent, the "honest" block turns into a "orphan," invalidating the payment to the merchant. It's a double,
- Budgeting Problems. Double Spending is eliminated via PoW because "dishonest" blocks are harder to get around. Trudy needs to solve the Proof-of-Work to generate the block hash at the current level of difficulty in order to build the new block. The "honest" miners will keep working and will be able to produce more honest blocks. Trudy needs a longer block to pass. Trudy might not be able to solve the PoW faster than other nodes. Trudy also needs to get some powerful tools. Spending twice is challenging.
- Blockchains like Trudy's BC network are unable to change data because of Proof-of-Work and Longest Chain Rules.

Deluding an Audit Team

To trick an auditing team, Trudy plans to pose as the offline chain. Trudy wants to add or conceal offerings. It is important to change the transaction block in order to hide a transaction. She is unable to add fraudulent transactions to the last block since they are concatenated and timestamped sequentially. She needs to find the transaction's time and date components. A chain of 100 blocks has to be modified at block number 45. The block will fail if Trudy makes the necessary changes since the block's hash (#45), invalidating the

hashes of blocks #46 through #100. The auditing team just needs to recalculate recent block hashes in order to confirm the chain.

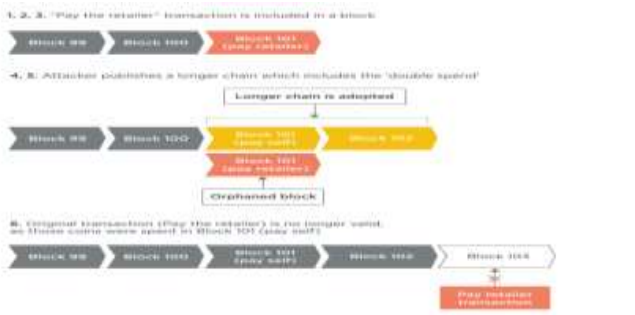

Fig. 4 Consequences of double spending

Trudy can deceive the audit team by recalculating all following block hashes in order to recreate the block. Bitcoin and other blockchain-based (BC) ecosystems demand computationally expensive PoW puzzle solutions for each transaction. The distribution of block-adding authority occurs randomly and sequentially in Multichain and other BC ecosystems. Digital block adders sign. All adders' private keys are needed to put the puzzle pieces back together. Both times, block reconstruction will be difficult.

Assume that Trudy altered or hid transactions to recreate the block. The auditing team won't be misled. Any recent Trudy's BC block hash and the block of any participant who is not cooperating can be easily matched. The audit team can identify whether the chain has been updated without data if these two hashes do not match.

Three different Blockchain variations are defined by write and read permissions.

Public (Permissionless) Blockchain

With public blockchains, everyone can take part in the ecosystem. Nodes have the ability to read and write. Among the components of this Blockchain ecosystem are Factom, Blockstream, Ethereum, and Bitcoin.

Private (Permissioned) Blockchain

Blockchains that are private or have permissions can only accept "trusted" nodes with read/write access. Write permission can be granted to nodes and locations. Private Blockchain ecosystems like Eris Industries, Blockstack, Multi Chain, and Chain all exist. Using blockchain technology, Chain and NASDAQ issued and transferred shares of privately held companies in 2015. Chain initially used the NASDAQ Private Markets (NPM) private ledger technology to issue and transfer shares. By creating complete confidence between the two parties, BC eliminates the need for a third party. Private BC violates the goal.

Hybrid (Consortium) Blockchain

Write access and consensus maintenance are features of both private and hybrid blockchain networks. A hybrid blockchain limits writing to a smaller number of nodes while maintaining consensus. Hybrid Blockchains, as opposed to private Blockchains, allow for open read access. Stock markets prefer the hybrid blockchain because it incorporates the benefits of the other two.

3.EVOLUTION OF SECURITIES EXCHANGE

Investors can trade stocks on a securities exchange that offers low transaction costs, great liquidity, and other advantages. Typically, brokers and dealers manage stock transactions. Exchanges for securities are subject to both internal and external rules. Fraud, insolvency, and inaccuracy are decreased by these factors.

A nation may have several securities exchanges, depending on location and the needs of the financial sector. The first stock market opened in 1602 and its name was Amsterdam Stock market. The top exchanges on the market include the New York Stock Exchange, NASDAQ, London Stock Exchange Group, Euronext, Hong Kong Stock Exchange, Japan Exchange Group, and Shanghai Stock Exchange. The market capitalization of the entire world rose by 22.6% in 2017 to $87.1 trillion.

The volume of transactions makes it challenging for stock exchanges to maintain accuracy and security. Order matching (1.24 billion per day on the Hong Kong Stock Exchange) and settlement transfers are two types of high volume stock market transactions. The majority of business is done online using digital recordkeeping and remote data transfer. The significance of stock market security has increased due to worries about unauthorized hacking, cyberwarfare, and

hacktivism.

Knowledge of the history of the stock exchange is necessary for operations, especially with regard to technological development. It appears that as private networks replace public marketplaces, the transition from company to market to firm is taking place. There have been official and informal institutions in many epochs. Broker-dealer self-interest has been important throughout this history, despite the effects of legislation and technology.

Small and large merchants have traded securities for about a thousand years. Direct trade emerged as a result. Between 1800 and 2000, private companies operated quasi-public "exchanges" for transactions. Private matching venues first appeared in the early 2000s, following the creation of electronic platforms by major brokers using cutting-edge information technology.

Stock exchanges were initially member monopolies. Government control, regulation, and openness were established by law. By the end of the 20th century, advancements in technology and legal changes had made it possible for the biggest broker-dealers to get around the open egalitarianism of the exchanges and create their own trading matching systems.

4.APPLICATION OF BLOCKCHAIN IN SECURITIES EXCHANGES

The major stock markets have embraced BC. The first stock exchange to use BC was NASDAQ. The Australian Securities Exchange (ASX) plans to replace CHESS with BC by 2020 or 2021. To cut costs, HKEX and ASX are working together to use blockchain technology. The LSE is actively implementing BC as well. The LSE announced a collaboration with IBM, the leader in open-source blockchain technology, in July 2018.

We provide a hybrid BC that uses point-of-sale matching and randomized round robin settlement in securities exchange activities. The central counterparty clearing house will handle clearance and settlement, although broker-dealer-led central exchange operations can match transaction buy and sell orders. "Closed circle" CCP nodes will be in charge of managing decentralized "back office" tasks.

The second part of BC's technical anatomy makes a case for stock exchanges possibly benefiting.

Compared to securities exchanges, this hybrid distributed BC approach offers ledger holders more transparency. Nevertheless, there can be less openness than in a public Blockchain.

BC can create a reliable market by using chronological blocks, cumulative hashing, and time markers.

The exchange will be managed by engineers of the BC system. If the BC's architecture and operation are fair, merchants and traders will have faith in it as peers verify and validate transactions.

Long-term transaction costs are decreased thanks to BC technology's lower cost and reduced maintenance requirements compared to earlier systems. Since updating an outdated system involves money, there are no immediate cost savings. Consumers must pay for the new system for years before they can gain from it.

Cycles for intraday settlement in the stock market. The majority of exchanges provide same-day settlement. the T+2 timeframe of two to three days At T+3, delivery of money and securities is complete. Brokers and sellers are protected if they "allow" multiple share transfers at settlement. Prior to the execution of a transaction, China requires verifiable cash; as a result, settlement happens right away. BC has the capacity to automate post-trade tasks. Real-time settlement of securities improves liquidity, supply chain efficiency, transparency, and trust. Will businesses deliver securities, and if so, how much will it cost?

According to accounting, blockchain technology will lower transaction costs and post-trade inefficiencies, luring more investment in market rearrangement.

The advantages of BC draw market players and regulators. The issues that British Columbia's youngsters bring in terms of regulation and the law are now being discovered by the authorities. Data scalability and localization for certain nations may pose legal and regulatory difficulties in British Columbia.

It is crucial to regulate trading, clearing, and settlement. They were initially divided. Modern laws see them as a single, multi-step transaction, in contrast to British Columbia.

Politicians and regulators must create separate policies for "tracking claims" and "dematerialising" because they are legally distinct concepts. Instead of using paper certificates to track ownership changes, use digital DLT transactions. For transfer purposes, digital tokens that are transferable may count as uncertified securities. Since tokens are not securities, they have no current legal value. As an invention, the token is immune from share ownership restrictions. Because the shares are listed in the owners' names on a legally recognized share registry that is devoid of the BC ledger or any other DLT that keeps track of digital tokens, the shares are in their owners' possession. BC ledgers and other DLTs cannot take the role of legitimate share registries without a new law.

5.CONCLUSION

The implementation of private blockchains requires ""pressure and budget to build anything connected to blockchains"". Instead of continuing in this direction, we looked at whether financial markets would be benefited by the introduction of BC. How could Blockchain technology improve stock exchange securities settlement (registration) operations from a legal and technological standpoint? We looked into the potential for stock market transactions to be facilitated by Blockchain versions. By fusing the operations of securities exchanges with BC technology development, this study develops a hybrid BC technique. The legal ramifications of adopting Blockchain in stock exchanges will be the subject of further study.

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. Miraz and 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/MikeSutcliff/status/912382978680082433
6. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, 1st ed. 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, 1st ed. Pennsylvania, USA: IGI Global, 2017.
10. Paper 2008. Available: https://bitcoin.org/bitcoin.pdf