Retraction

Retraction: A Quantum-Based Blockchain Approach to Voting Protocol Using Hyperledger Sawtooth (J. Phys.: Conf. Ser. 1916 012088)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1

Retraction published: 23 February 2022
A Quantum-Based Blockchain Approach to Voting Protocol Using Hyperledger Sawtooth

V Vignesh 1, S Harihara Gopalan 2, M Mohan 3, R S Ramya 4, R Ananthakumar 5
1 Asso. Prof., CSE, KPR Institute of Engineering and Technology, Coimbatore
2 Asso. Prof., CSE, Sri Ramakrishna Engineering College, Coimbatore
3 Asst. Prof., CSE, KPR Institute of Engineering and Technology, Coimbatore
4 Asst. Prof., CSE, Kathir College of Engineering, Coimbatore
5 Deputy Manager, Saipen India Projects Ltd., Chennai
vignesh.v@kpriet.ac.in

Abstract. Protection measures are essential to present-day blockchain innovation ever, since they can exist short of empowered outsider, which implies that there may not be a disclosed trustworthy individual or group responsible for frameworks. Security of the present frameworks depends on estimating the firmness assumptions and large numbers of the benchmark cryptographic functions proven to be powerless for crucial monetary and a variety of applications against the approach of undeniable quantum machines. Upgrading blockchain innovation with the future of quantum states in a shared manner will enhance the degree of protection and security by-laws of physical science, which is never feasible from non-quantum data hypothetical perspectives. In this article, we propose a quantum-built way to deal with harness of security for a democratic application with the execution, utilizing Hyperledger Sawtooth.

Keywords: Quantum computing, Hyperledger, Blockchain, Sawtooth, Cryptography.

1. Introduction
A blockchain is a framework that permits clients to shape a public consensus with no specific third party, such as, government administration and an organization that remained devised by the mysterious creator in 2008 to make the decentralized digital money, called Bitcoin. These days it extends a wide assortment of employments and numerous comparative frameworks getting developed; virtual monetary standards are broadly utilized for various instalments and items can be exchanged or sheared without merchants. In addition, a few nations have considered acquainting blockchain innovation with public administrations. The residents can utilize it for different systems including political decision, charge instalment, bank move, etc. As depicted, a blockchain has a major possible preferred position; consequently, this will profoundly be domineering to guarantee the safety of the frameworks.

Quantum is a kind of blockchain innovation is predominant in vital zones of analysis in upcoming rapid developing area of quantum cryptography [1]. This platform plans utilizing quantum method in their plans and empowers such plans to depend on apparently tough laws of physical science meant for their security. Numerous quantum-based cryptography plans come across securing data hypothetically, implying that, security did not depend on several non-major suspicions. In the plan of blockchain frameworks, data hypothetical security is not demonstrated. Or maybe, old style blockchain
innovation normally depends upon security contentions that produce presumptions about the constraints of invaders assets.

Blockchain and distributed record advances come up with applications in numerous businesses, largely quite in the monetary business. The monetary utilizations of blockchain advancements incorporate cryptographic forms of money, protection, and protections issuance, exchanging, and trading. Non-monetary utilizations of blockchain innovation must be recognized for the harmony business, decentralized IoT, hostile to fake arrangements, Internet applications, and decentralized stockpiling, to give some examples. As of late, blockchain projects have pulled in huge consideration in these businesses [2].

With respect to and protection, the effortlessness of a blockchain's design encourages us to indicate its frail focuses. Extremely close thoughtfulness regarding the accompanying two focuses should be done: the computerized signature plot and the verification of work. Those two viewpoints have various undertones regarding security and protection. To start with, with the safety of computational (digital) signature conspires utilized for blockchain is ensured by calculating the firmness of elliptic curve cryptosystems. But the reality remains not having path shape or form insusceptible from quantum registering, this old-style advanced mark is safe since the existence of supercomputers intended for great execution in taking care of such NP-difficult issues. Also, it remains accepted that breaching elliptic cryptography = past the ability of the mid-21st era quantum innovation. In any case, points of interest of quantum data hypothetical perspectives can be found in various angles, one of which is protection.

In traditional blockchain innovation, there are no approaches to ensure clients' security consummately (this issue was brought up during the first Bitcoin paper is yet a public issue). Thus, the framework encounters weakness. In any case, quantum innovation guarantees security and tackles wellbeing issues by-laws of physical science. For instance, a Quantum Key Dispersion (QKD) convention permits a remitter and a beneficiary to cut off data securely.

Additionally, the traditional advanced mark convention dependent upon the curve which is represented in elliptical manner must be supplanted by a digital signature convention in quantum form hence, just the proprietor can alter. Notwithstanding that visually impaired quantum calculation consummately ensures clients' protection since they can assign their quantum calculation to a worker with a quantum PC so that the worker cannot recuperate any info and yield of the customers.

In this paper, the work is reviewed the work that the innovation of blockchain acquaints quantum cryptographic techniques. The expected outcome is considered and threat related by blockchain innovation and exactly quantum cryptographic strategies is proposed to strive and the various risks is focussed on crucial applications.

2. Background

Conventional methods in blockchain for privacy protection

There are a few issues in the conventional blockchain design separated from quantum points of view. These issues are vital for logical points of view as well as for practical usage and will be useful in a quantum viewpoint also. To say, an essential protection issue of many existing blockchain frameworks is summated up in the accompanying table 1

| Consignee Δ | Connection to private information specified Implicitly, but prediction is possible. |
|-------------|---------------------------------------------------------------------------------|
| Recipient Δ | Connection to private information is Indirectly specified, but result prediction is possible. |
3

| Number of transactions | Blockchain is verified in simple manner |
|-----------------------|----------------------------------------|
| Date and time         | Blockchain is verified in simple manner |

Looking at the table, it very well may be perceived that putting away information in a blockchain is not an awesome path contrasted and the customary brought together ways for exchanges. An outsider cannot have a clue about the individual data of consignees and recipients; notwithstanding, there are yet opportunities to figure after their wallets or addresses. Much more terrible, the quantity of exchanges and exchange time are effortlessly speculated since exchange records are conventionally open to the general population. This is unique in relation to the typical incorporated framework. For example, a bank that puts forth an exceptional attempt to secure data should not accessible of any customers’ data to any spectator in the complete environment.

By what means, an individual who will not believe banks have to disseminate money by hand after a significant slack. Thusly, in each face of data assurance, an innocently planned blockchain would not turn into the best option.

A decent framework, as a rule, should offer different uses in however many fields as clients need. This could concern how to ensure mystery data of proprietors with the goal that anybody insignificant to an exchange ought not realize who is associated with it and how to stay discreet with the number of transactions.

2.1 The ledger
A shared record of a blockchain digital money keeps up the possession and status of every single existing coin. The record is comprised of a group of squares, called chain. This group of chain is made of the squares which refer to each other. Every legitimate square’s header includes the header of the past square in the group of chain is represented by means of hash form. Each square is mentioned regularly to comprises timestamp value, nonce value, and list of exchanges values (Figure 1).

![Blocks Chain representation](image)

**Figure 1.** Blocks Chain representation

At the point once a transaction happens, the present record state is changed by a capacity that holds the first state $S_0$ along with the exchange TX and yields the following transaction state $S_1$ or a blunder $E$. Here, and all through this article, ← addresses a change of a transaction state. The situation here, has the transaction state which is a merely a conventional data structure. Be that as it may, in later segments, a similar documentation will be utilized to indicate advances between quantum states.

$S_1$ or $E ← Apply (S_0, TX)$.

With the advent of Bitcoin, a record’s transaction state is made of all unexpended transaction yields (UT, X O), else basically the bit coins were not spent which is recognized as mined. Each and every coin in the block chain owns upto 20-byte cryptographic public key that holds data concerning its proprietor and its division.

An exchange expects references to every UT X O included and the cryptographic marks delivered by the UT X O proprietors keys is represented privately.
2.2 Resistant of work

The devolution of the record of effort is accomplished, by an agreement framework should be presented. The objective of the agreement framework is to guarantee that everybody concedes to the legitimacy of the exchanges that have prompted the record's state and their request. A few agreement frameworks are being used these days, with verification of-work, confirmation of-risk, evidence of-consume, as well as the sky is the limit from there. The most universal is work on confirmation.

Bitcoin's evidence of-work-based framework necessitates that clients endeavour to distribute deals frequently. These exchanges remain distributed in a fixed range by gathering of bundles (1 MB on account of Bitcoin) called chunks. Notwithstanding rundown is of contracts, a square includes a timestamp, once utilize the id represented in block or time being, along with a value of hash in header of the existing square which added to the record. Henceforth, every chunk keeps note to the chunk that preceded it, in addition to the chunk structure a transaction cable in the same way as they are distributed which reflects the request for their distributions as expected.

Instead, a chunk to be acknowledged, confirmation of work should be substantial. The legitimacy requirement the Bitcoin block remains that of twofold SHA256 hash is not exactly a powerfully changed cut-off when deciphered as a whole number. A SHA256 hash is a totally unusual consequence of a pseudorandom work. Along these lines, to make a legitimate chain of block with the hash work should remain running on a subjective number of instances until a substantial yield arbitrarily happens. In that persists, the ongoing job should create a proof-of-work, and the blowing mind transparent in digital assets that is supported by blockchain is verified by its works verification of-work blockchains.

The instance needed towards creating a legitimate hash is essential to the agreement framework that is utilized. On the off chance that an invader endeavours to transfer cash in a manner that conflicts by the responsibility for because of a transaction contract record previously acknowledged by the record, the incident is just dismissed. In any case, an attacker can attempt to manufacture a square that focuses on a substantial block that ensued distributed prior to the block holding the exchange which improved the responsibility for needed coins. For this situation, the attacker will be needed to create another legitimate confirmed on its work. The different miners are involved in distributing blocks that represent real blockchain which overcome by the attacker. The standard that is used to get rid of these assaults is essentially that the longest substantial chain is brought to be reality. An invader would in this manner want to have further processing power than the remainder of the organization consolidated to dominate the pace of the organization's distributions and get the chain in lengthiest. This is known as a 55% of attack and would hypothetically remain effective.

2.3 Resistant of stake

These plans stayed acquainted with focus on a portion of the concerns related to resistant-of-work [3]. Resistant-of-stake plot is changed to Ethereum. Miner can access mining power with a proof-of-stake plot exists relative near the quantity of coins claimed by the miner. Thus, they stay restricted to mine a few more blocks that are corresponding to their interest in the digital currency eco system. This offloads the miner's utilization of electrical power assets to cash assets that happen more inside towards the blockchain.

A main thrust following the production of proof-of-stake stood vibrant made by miners offering their coins to cover tainted their electric flaps. This development of digital money out of the environment gets prompted reductions in cryptographic wealth esteem.

Resistant-of-stake plans has a risk which is less than resistant-of-work methods. It is obviously shown the result that the verification of-stake form is 52% assault. In a resistant-of-stake in blockchain, an assailant with 55% of the cryptographic currency in the environment to an effective 53% assault. It would create unappealing to damage the environment, since ruining the safety and legitimacy of the framework would hazard negating the invader's simulated wealth. This is a characteristic impediment
that the methods in proof-of-work will not exist, where an assailant with 52% of the organization's processing force can have successful 55% attack paying little attention to their risk in the environment.

There remain disadvantages to any algorithm on consensus. Because of proof-of-stake, any issue is the undeniable relationship of large quantity including the capacity to influence cases. But the scheme enhances resistant-of-work exclusively, it boosts rivalry and, likewise to progressive frameworks, remunerates the "strongest" contestant. For this situation, strongest is quantified by entities of money as opposed to computational capacities.

2.4 Smart contracts
Perhaps the significant commitments to blockchain innovation remains the idea of independent smart contracts. The expansion of smart contracts separates supposed Blockchain 2.0 innovation like Ethereum after "Blockchain 1.0" innovation as Bitcoin [4]. Blockchain 2.0 innovations empower developers to utilize self-ruling specialists, the brilliant agreements, as components of conveyed programming components are referred as Distributed Applications (DApps). Ethereum's, is a high level data structure in recording transaction financial records, as opposed to currencies. The record keeps up every record's public-key location contains 20-byte of data within time being, balance, scam-bundle of source code, and capacity. It contains two sets of records. The first record remotely claimed transaction accounts, which were constrained by private keys. The second record is the account on transaction contract which are constrained by their codes of agreement. Remotely claimed accounts are like individuals utilized Bitcoin and could be utilized in contract transactions as depicted already. Accounts of Contract transaction are substantially above fascinating. The contract accounts go about as independent authorities that perform their agreement code once sent messages. An agreement record could be modified towards logically scrutinize and keep in touch with its build up stocks, send extra messages to more transaction contract accounts, or make transactions. To initiate an agreement, record to implement its code demands a currency related transmitter cost of the first communication, this cost is identified as "smoke" and is corresponding to unpredictability to the agreement cypher. The cash (Ether) gave during first communication is utilized as smoke to "energy" agreement cipher implementations that outcome after the first agreement's initiation.

Agreement cipher is printed in a low level language represented in heap form as machinecentred bytecode instructions referred as Ethereum Virtual Machine (EVM) cipher. The linguistic utilizes heap, straight recollection exhibit, and extended-drag stockpiling. The linguistic is made of little guidance customary that combines application on blockchain with specific guidelines like CALL which makes an impression on an agreement and CREATE which makes another agreement.

The blocks utilized with Ethereum are extremely much like those utilized by the Bitcoin. Ethereum blockchain have all the data that a Bitcoin block does, along with the expansion of a duplicate of the latest record express, the block number, as well as finding difficulty to mine the record for that block. Ethereum does not essentially turn off after the normal proof-of-work agreement scheme.

2.5 Hyperledger Sawtooth
Hyperledger Sawtooth is a private platform for compiling, deploying, and executing distributed records. Distributed records give an electronic record, (for example, resource ownership) that is kept up in absence of a central power or execution. Sawtooth intends to hold given records distributed in addition to make smart agreements alright for big business use. In fitting with this effort building, Sawtooth is exceptionally measured. This empowers schemes and groups to settle on choices about their blockchain applications for themselves.

Sawtooth contains several technical improvements, including

- **Dynamic consensus**— Moving away from compile-time pluggable consensus, this permits a group to change consensus calculations on a running blockchain just by offering a transaction.
• **Transaction groups**— A smart contract reflection that empowers clients to compose contract transaction logic in the language based on their personal preference.

• **Compatibility with Ethereum contracts**—Transaction groups can also incorporate other smart contract actors including Hyperledger Burrow’s Ethereum Virtual Machine. Sawtooth elements like permissions and un-pluggable consensus facilitate Ethereum to be configured suitably for any organization.

• **Parallel transaction execution**—Generally blockchains require transactions to be fulfilled in sequence to assure reliable ordering at each peer. Sawtooth comprises an enhanced parallel scheduler that separates blocks into similar flows. Parallelism permits for quicker block processing address to some extent the execution of shortcoming blockchains compared to traditional databases.

• **Private transactions**— Clusters of Sawtooth nodes could simply deploy with autonomous permissions. This gives privacy and discretion among participants of that diverse chain. No central service disclosure transaction forms or other confidential information. Yet, an arbitrator such as Hyperledger Quilt is essential to link distinct chains.

In the forthcoming, Sawtooth plans to deliver supplementary privacy and discretion features on top of trustworthy accomplishment ecosystems and/or zero-knowledge primitives.

### 3. Problems associated with Quantum Attack

One of the incredible highlights of quantum computers is that they have a likely bit of scope in calculation using the superposition principle of quantum states. Thus, there are for sure a few issues that cannot be addressed by traditional approaches represented in polynomial form on any traditional machine that are feasible in quantum algorithm represented in polynomial period on a quantum machine. To improve insight, a few quantum computations are classified for breaking of code. The main thought depends on the time frame discovering issue expressed below in Equation (1)

Let us consider a function \( f_1 \) on \( S_n = \{0, 1, ..., n\} \), \( n \in S \) (1)

#### 3.1 Interval-Discovery Problematic Function

Let \( f_1 \) be a regular function of period \( t \) which is a divisor of \( n \) expressed below in Equation (2).

\[
\begin{align*}
    f_1(x_1) &= f_1(x_1 + t) , \forall x_1 \in \{0, ..., n - t - 1\} \\
    \text{Then } r \text{ is period.}
\end{align*}
\]

A simple conventional algorithm for this problem is determining \( f_1(0), f_1(1), ... \) and obtaining \( t \) which satisfies \( f_1(0) = f_1(t) \). This approach, takings on the order of \( O(\sqrt{n}) \) time which represented by worst case value. Hence, a faster quantum algorithm is required.

#### Quantum Algorithm for the Interval-discovery problem

(i) Quantum state is represented in the following form expressed below in Equation (3)

\[
\frac{1}{\sqrt{n}} \sum_{a \in S_n} |a|0^n
\]

(ii) Add \( f_1 \) into the second qubit column expressed below in Equation (4)

\[
\frac{1}{\sqrt{n}} \sum_{a \in S_n} |a|f_1(a)
\]

(iii) To measure an output \( s \). This choice gives the state expressed below in Equation (5)

\[
\frac{1}{\sqrt{n}} \sum_{a \in S_n} |a|f_1(s)
\]
Now, the sum of the value is carried over all a such that $f_1(a)=s$.

(iv) The first qubit column from Fourier transformation is used for calculating the value of quantum. One of the divisors of $n/t$ is achieved from the algorithm. (v) Repeat (i) – (iv)

Therefore, a quantum algorithm is strong in solving the interval-discovery problem. The issue is to calculate the Greatest Common Divisor (GCD) of two numbers fits to the session P; still, that of factorisation in prime numbers goes to the session NP.

The better sense to break RSA, which relies on prime factorization, is to transform the problem of prime factorization keen on that of achieving the GCD.

3.2 Factorization Problem to find disintegrated value
Assume $N_1$ be an integer of $n$ bit length and presume $N_p$ can be disintegrated into $N_1 = pq$, where $p$ and $q$ are prime numbers. Subsequently determine the values of such $p$ and $q$.

We are inclined to explain this issue using the quantum algorithm for the period/interval-finding problem. The trick is to use the function of the form $f_1(s) = e^{s \mod{N_1}}$. This $f_1$ has a certain period $s$. For instance, take $N=12=4.3$ and $x=2$. Then is satisfies $f_1(0) = f_1(2) = f_1(6) = .. = 1$ and its period is 2. We express the GCD $(a, b)$. The subsequent algorithm developed by Shor [5] uses $f_1$ and resolves prime factorization in polynomial period on a quantum machine. Shor’s Algorithm

(i) Pick up a random value $x_1 \in \{1, \ldots, N_1 - 1\}$.
(ii) We presume $GCD(x_1, N_1) = 1$ since otherwise $GCD(x_1, N_1)$ is a nontrivial divisor on $N_1$ and we can achieve prime factorization $N_1$ by the Euclidean algorithm.
(iii) Find the minimum $t_1$ such that $x_1^{t_1} = 1 \mod{N_1}$
(iv) If $t$ is even and $x_1^{t_1/2} \neq 1 \mod{N_1}$ check whether $GCD(x_1^{t_1/2} + 1, N_1)$ or $GCD(x_1^{t_1/2} - 1, N_1)$ divides $N_1$. If so, output them otherwise start over from (i).

Shore’s algorithm makes sense and is efficient to solve the factorization problem. In this way, we finally obtained an approach to break RSA using a quantum machine. Correspondingly, for experimental understanding of the algorithm [6].

4. A quantum computation voting protocol based on blockchain.
Blockchain Technology is an appropriate application used to develop voting application as it makes difficult for participants to fabricate claims. To design a self-tallying voting protocol Sun, Xin, et al. proposed the concept using quantum approach.

4.1 Voting using binding trust.
It is modest kind of protocol. The protocol help for voting encompasses two phases. “Ballot Commitment/trust” and “Ballot Counting” phases are the two phases. The ballot commitment phase carry out the following steps.
1. For each $i_1 \in \{1, \ldots, n_1\}$ voter $V_{i_1}$ creates the $i_1$th row of an $n_1 \times n_1$ matrix of integers $r_{i_1,1}, \ldots, r_{i_1,n_1}$ such that $\sum_{j=1}^{n_1} r_{i_1,j} = 0 \mod{n_1 + 1}$.
2. For each $i_1, j_1$ voter $V_{i_1}$ sends $r_{i_1,j_1}$ to voter $V_{j_1}$ via a quantum secure transmission.
3. Then, each voter $V_{i_1}$ knows the $i_1$th column $r_{1,i_1}, \ldots, r_{n_1,i_1}$. $V_{i_1}$ computes his/her hidden ballot $V_{i_1} = v_{i_1} + \sum_{j=1}^{n_1} r_{i_1,j_1}$. $V_{i_1}$ binds $v_{i_1}$ to every counting of the blockchain via a quantum commitment protocol.

Ballots are counted by the following de-commitment procedure. $v_{i_1} = 0$ is considered as a dispute with the proposal being voted on and $v_{i_1} = 1$ is considered an agreement.
1. Each voter $V_{i_1}$ shows $v_{i_1}$ to every count of the blockchain by opening his/her commitment.
2. The counters individually run the Quantum reliable winner Byzantine Agreement Protocol to reach a consensus on the value of the hidden ballot \( v_1, \ldots, v_n \).

3. The result of the vote is \( \sum_j jv_{i1} = \sum_l 1v_{l1} (\mod n1+1) \).

### 4.2 Duplicitous ballot counters Behavior.
A Byzantine Agreement Protocol (QHBA) is got successes by means of quantum trust, implied in the voting scheme to recognize illegal ballot counters. An authentic success QHBA includes \( n \) agents. One of the agents is sender \( S1 \) and holds an input value \( x_s \in Bf \) where \( Bf \) is a set of finite domain. A protocol accomplishes straightforward QHBA success if the protocol guarantees the following:

1. If the sender is active, then all true agents on the same output value is approved \( y_1 = x_{1s} \).

2. If the sender is duplicate, then either the value becomes true and receivers terminate the protocol legally, or all honest receivers determine on the same output value \( y \in D \).

The QHBA is \( n-2 \) resilient. \( n \) is the number of receivers and is further effective than a traditional HBA protocol after there are many illegal receivers [7-10].

### 4.3 System Flow
The system flow as depicted in the Figure 2, works as mentioned in steps.

1. The values are read from the fields and passed in through the SendData function by specifying the action.
2. The payload is set with the passed values which are encoded.
3. The Address is set for voter according to the voter id.
4. The Address is set for the candidate according to the area of the candidate.
5. Then the address is sent to TransactionHeader which includes the family name, family version, batcher Publickey, signer public key, Inputs, Outputs, Dependancies, Nonce and payloadsha512 string.
6. Then the Transaction is signed with Transaction headerbyte.
7. Then it is sent into the RestAPI.

![Figure 2. System Flow](Retracted)
5. Conclusion
This work focussed on easy voting protocol in simple form of Blockchain based on Quantum. Moreover, being modest, our protocol bids secret, necessary, non-reusable, provable, qualified, reasonable, and self-evaluating voting. Besides Quantum in Blockchain, Quantum Secure Communication and Quantum Bit Commitment are other quantum approaches included in our protocol. Completely, the above set of practices are realizable with the current knowledge. We have tried deploying using Hyperledger sawtooth and the task of voting in an electronic manner is simplified and in a significant manner. In forthcoming year, Quantum Blockchain simplify and secure many applications from the machines that make attacks using quantum theory.

References

[1] Fehr, S.:2010, Quantum cryptography. Found. Phys. 40(5), 494–531. doi.org/10.1007/s10701-010-9408-4
[2] Nofer, M., et al.:2017, Blockchain. Bus. Inf. Syst. Eng. 59(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3
[3] King, S., Nadal, S.:2012, PPCoin: Peer-to-peer crypto-currency with proof-of-stake .https://blockchainlab.com/pdf/peercoin-paper.pdf.
[4] Editor.:2019, Blockchain 2.0—What is Ethereum [Part 9]. OSTechNix. https://www.ostechx.com/blockchain-2-0-what-is-ethereum/
[5] P.W. Shor,1997, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) 303–332.
[6] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio networks, Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020. doi:10.1016/j.compeleceng.2020.106784
[7] https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf
[8] Wiesner, S.1983, Conjugate coding. ACM SIGACT News 15(1), 78–88
[9] Bennett, C.H., Brassard, G.1983, Quantum public-key distribution reinvented. ACM SIGACT News 18(4), 51–53