ISSN: 0975-833X

*Available online at http://www.journalcra.com*

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

*International Journal of Current Research*
*Vol. 13, Issue, 06, pp.18011-18020, June, 2021*

*DOI: https://doi.org/10.24941/ijcr.41554.06.2021*

RESEARCH ARTICLE OPEN ACCESS

# HYBRID PRIVATE-PUBLIC BLOCKCHAIN FOR ENHANCED DATA PRIVACY USING NETWORK VIRTUALIZATION

*Anfal Alruwaili and Saloua Hendaoui

Jouf University, College of College of Computer and Information Sciences

**ARTICLE INFO**

*Article History:*
Received 29th March, 2021
Received in revised form
17th April, 2021
Accepted 24th May, 2021
Published online 30th June, 2021

*Key Words:*

Privacy, Security, Blockchain,
Private, Public,
Complexity, Virtualization.

## ABSTRACT

Data privacy has to be guaranteed for enhanced system security especially in some sensitive domains such as in banking systems. Blockchain is frequently used in these systems due to its high security level. however, public blockchainhas a major concern about privacy which is the ability to discover addresses of nodes in the blockchain.Thus, private blockchain is preferred since they guarantee full privacy since the blockchain is not open. In addition, they guarantee easier deployment and faster computation. However, the security level lower than the public blockchain. Our contribution in this paper is to enhance the privacy of banking transactions (so use the private blockchain), reduce the cost of complexity (use the private blockchain),guarantee enhanced security level (use the public blockchain via network virtualization). Our proposal is a hybrid private-public blockchain solution for enhanced data privacy and guaranteed security. We propose a hybrid blockchain structure that applies the special properties of the blockchain physically and increases the general blockchain characteristics by default. Currently, all the advanced systems do not need physical devices and use virtual devices that have the same functions but with higher capabilities than them. We propose the use of a virtual network because of its advantages as it is cost-effective, reduces the business burden, better operating time, faster resource deployment, and economic and efficient use of energy

***Citation: Anfal Alruwaili and Saloua Hendaoui.*** "Hybrid private-public blockchain for enhanced data privacy using network virtualization*", 2021. International Journal of Current Research, 13, (06), 18011-18020.*

# INTRODUCTION

Security is a state of protection and no exposure to risk which allows a defence against any enemy or opponent who may, intentionally or unintentionally, inflict damage. Security is crucial and indispensable in all domains and in particular in information systems. Despite that information security is often seen as computer security, however, it is more than that. Information security is something that includes computer security among many things and has been defined as "the field of study that discusses data and information security against unauthorized access, use, piracy and leakage if used over the Internet" (El-kenawy et al., 2019) . Information security has many goals that organizations need to understand the value of information, taken from the features that they have.

Evaluation of information security can be achieved via various criteria among them, three key factors are considered very important and are with the highest significance. These factors are the main objectives of the CIA triad, and also called the CIA triangle. C stands for Confidentiality, I for Integrity, and A for Availability.There are many techniques used to achieve the CIA triangle features. Authentication techniques, which rely heavily on passwords are not enough safe, as the ability to theft is very high(Gahan and Devanagavi, 2019). To overcome this vulnerability,several methods were included in addition to the password for identity protection, such as biometrics techniques like fingerprintscanning, eye print, etc (Gahan and Devanagavi, 2019). When itcomes to security, the main imperative is to hide data from public or bad attackers. One of the techniques circulating in confidentiality is encryption. Encryption includes many types and basics that guarantee the safety of information from unauthorized access, including encryption, asymmetric and symmetric, as well as message authentication codes (Gahan andDevanagavi, 2019).

***Corresponding author:** *Anfal Alruwaili,*
Jouf University, College of College of Computer and Information Sciences.

Symmetric cryptography works by exchanging the attacker's hidden key between the receiver and the sender. The Advanced Encryption Standard (AES) is gaining popularity among different types of algorithms that are similar due to its efficiency, protection, and outperforming its predecessors. Steganography is a coded writing mechanism so that no one knows the existence of a message inside it other than the recipient and the sender (Gahan and Devanagavi, 2019); Mukund et al., 2015). What distinguishes steganography is that the encrypted message does not attract the audience (Gahan andDevanagavi, 2019; Mukund et al., 2015). The advantage of data privacy is that it is related to the privileges of authorized access, who determines the data, and who can access it, in contrast to data security that relates to securing data from unauthorized access (Namasudra et al., 2018) . Despite the power of these techniques in protecting information systems, with the advancement of information technology, several challenges occur regarding systems privacy. Privacy is one of the legal problems, knowing that it is often a technical problem, but it includes some policies through which data privacy protection can be managed in the information system in two ways: (Namasudra et al., 2018)

- Communication policy is implemented based on communication, activation of privacy policies, and the application of legitimacy in exchange for what individuals desire.
- Policy application refers to the security procedures applied within security systems to protect data privacy during storage and transmission

Consequently, data privacy has to be guaranteed for enhanced system security especially in some sensitive domains such as in banking systems. Blockchain is frequently used in these systems due to its high security level. however, public blockchain has a major concern about privacy which is the ability to discover addresses of nodes in the blockchain. Thus private blockchain is preferred since they guarantee full privacy since the blockchain is not open. In addition, they guarantee easier deployment and faster computation. However, the security level lower than the publicblockchain.

**Our contribution in this paper is the following**

- Enhance the privacy of banking transaction (so use the private blockchain)
- Reduce the cost of complexity (use the private blockchain)
- Guarantee enhanced security level (use the public blockchain via network virtualization)

So, our proposal is a hybrid private-public blockchain solution for enhanced data privacy and guaranteed security. This paper is organized as follows: Section 2 gives the Literature review; Section 3 describes the proposed methodology, mainly Blockchain structure in banking systems. Section 4 discusses the results followed by the conclusion and future work in section 5.

**LITERATURE REVIEW:** The use of digital currency by the Central Bank is becoming a major policy priority for the country. The CBDC (Central Bank Digital Currency) model should benefit from oversight, payment, and consumption. Decentralization, tamper resistance, and traceability are all characteristics of blockchain. (Sun et al., 2017) attempted to create CBDC's fundamental technologies the blockchain. Conversely, barriers like consumer privacy rights, oversight, and transaction speed must be addressed. They suggested the Multi-Blockchain bank digital currency model (MBDC-CBDC), which is based on authorization blockchain technology and is based on the CBDC model. To boost scalability and process payments more efficiently, the model employs multi-blockchain technology and Chain ID. They developed their blockchain framework, to validate the MBDC model. The simulated transfers are generated using the transaction format and execution process. First, the transaction execution system's time constitution was investigated. Then theycalculated the time it took to conduct a transaction, such as the Tb and Tu. The study showed that Tb's transaction execution time is approximately four times greater than that of Tu's. The outcome is consistent with the blockchain traffic that has been studied. The blockchain traffic between the two branches was substantially reduced when they used the bank reserves protocol to build the account and test the transaction execution time. Finally, they experimented with a growing number of blockchains to see how much bandwidth they could get in terms of transactions per second. For instance, research is required into the parallel technologies used for transaction execution and the implementation of block and consensus protocols to increase throughput. In addition, the allocation method for transactions isa crucial issue to address.

For the banking sector, (Wang et al., 2020) introduced a new data privacy protection system focused on blockchain technology. The system had three parts: a data privacy classification method based on financial data characteristics, a modern collaborative-filtering-based model, and a data disclosure validation scheme for consumer strategies based on Nudge Theory. They created a prototype for this system and suggested a collection of algorithms for it. Field and laboratory tests were used to test the structure. The Nudge principle was used to create the data disclosure programs, which decreases the amount of manual work and device transformation. Experimentsshow that the proposed system is accurate in terms of managing banking data privacy. Through a study of the current typical cryptocurrency and the prototype of the CBDC system, (Han, Yuan, and Wang ., 2019)provided the role and security requirements of Central Bank Digital Currency (CBDC). On this foundation, they introduced a three-layer blockchain-based architecture for CBDC, such as a supervisory layer, a network layer, and a user layer, as well as a detailed description of the main business processes of the CBDC's entire lifecycle of issuance-circulation-withdrawal. After that, they used cross-border payment as an instance to describe the CBDC transaction mechanism as well as to providetheoretical guidelines for CBDC design.

(Dai, Gu, and Teng 2020) proposed a CBDC supervised anonymous issuance (SAI) scheme based on the blockchain that uses a "special" anonymous multi-receiver certificates signcryption scheme and zero-knowledge proofs to ensure the privacy of commercial banks and the secrecy of amounts under central bank supervision. Transactions are around 2 KB in size and take less than 6 milliseconds to check in the SAI scheme's realistic implementation. A special type of Succinct Non-interactive Argument of Information (SNARK) and certificate-less-based multi-receiver signcryption schemes were used as thekey cryptographic primitives. They then briefly discussed a publicly verifiable preprocessing zero-knowledge SNARK (zk-SNARK) and the anonymous multi-receiver certificate-less signcryption framework model (AMCLS).

The proposed scheme is designed to solve the financial information leakage problem in the indirect CBDC model, which can provide better privacy for the banking sector under central bank supervision. They realized anonymity and amount confidentiality for the banking sector by using a special AMCLS scheme they devised, as well as public verifiability through zk-SNARKs. The unique AMCLS is adaptable enough to function in a variety of situations. Construction of an inverse method of the Issue and Transfer algorithms of CBDCs, respectively, can be used to reach anonymous redemption and resolution. Under certain cryptographic assumptions, their scheme is stable, according to the security analysis. SAI performs similarly to Zcash in terms of total efficiency, suggesting that the proposed scheme is deployable.

# METHODOLOGY

In various modern areas, digital information is flowing through unreliable communication channels, hence, the big issue here is confidentiality and privacy. Blockchain technology is currentlyone of the most in-demand areas of science in various applications and data privacy particularly. In the following section, we start by presenting blockchain, and then we will present the data privacy management framework. Blockchain is very popular and as its name indicates it is a seriesof blocks that contain information, as indicated in Fig.1. This technology was defined in 1991 by a group of researchers and was originally intended to put a time stamp as it is not possible to create a backdate for it or tamper with it. However, many years have passed it has not been used until Setouchi Nakamoto in 2009 adapted it to work with digital currencies and created Bitcoin. The data in the blockchain is difficult to change because each block contains data and a hash of the previous block. Blockchain is a peer-to-peer technology that guarantees the protection of digital information. It was originally invented for Bitcoin electronic currency and is also used for other electronic currencies, digital signature services, and voting systems. Blockchain is used to guarantee power security in various systems, in particular in banking.

**Blockchain structure in banking systems:** As its name indicates, a blockchain is composed of a set of blocs. In Fig. 2, we present the structure of a bullock in banking systems.

- **Block size**: On average, the block size is 1 megabyte for allblocks in the blockchain
- **Transactions Counter**: it refers to the number of transactions in a block, and approximately one block contains about 500 transactions
- **Transactions**: means all transactions stored in masses correctly
- **Block header**: contains 5 elements
- **version**: for every block in the network, it has a copy in the head of the block
- **Previous block segmentation**: a group of a blocklinked to each other by a hash
- **Merkle Root hash**: the segmentation of all transactionsin a block
- **Time Stamp**: The current time for each block
- **Nonce**: each block has special bits of data

The characteristics of blockchain lead us to many benefits in structuring, such as verification of the transaction, integrity, and transparency of the process, and thus its durability (Abeyratne and Monfared, 2016). Also, there are privacy requirements in the blockchain (Feng et al., 2019):

The links between transactions must be invisible or discoverable. The content of the transactions is only known to the participants and is activated by setting policies on it.

**The privacy requirements of the blockchain are subject to two main factors (Feng et al., 2019):**

- Identity privacy: it means the intractability of the treatment texts and the true identity of their posts
- Transaction privacy: it means that no one can access the content of transactions except by specific and known users of the public blockchain network.

The transaction in the blockchain contains the identifier of the transaction that precedes it, the commercial value, the addresses of the participants in it, the signature of the one who sent it, and the timestamp for it (Nakamoto , Bitcoin 2008). However, due to the general nature of blockchain networks, it is possible to track the flow of transactions to extract identities for users or any information (Nakamoto , Bitcoin 2008).

**Characteristics of financial statements and framework** Blockchain works by dividing bank clients into corporate and individual clients (Wang et al., 2020). The banks work by collecting data from customers while doing financial business, and then use it for a product recommendations, marketing, and anti-fraud control (Wang et al., 2020). the banking bodies used, and how and where the data is handled. Therefore, managing data privacy in the financial blockchain has three main aspects (Wang et al., 2020). Use "Privacy by Design" to enforce data privacy management first and foremost. Banks should ensure that the minimumrequired financial business data is processed and access to employee personal data. Classification management for different dimensions of customer information should be implemented and given to customers and fast monitoring via the data retention function of the blockchain. Second, to quickly create customer data disclosure schemes among broad groups of customers and reduce artificial contract signatures, and apply successful techniques and algorithms. Third, understand the complex data behavior that will be positioned with the in-chain and off-chain blockchain, allowingfrequent changes, additions, and removal of customer information.

**Blockchain categories:** Blockchain is a database that is only appended to maintain the nodes of a peer-to-peer (P2P) networkwhich on its responsibility has to ensure the connection betweenthe blockchain nodes (Feng et al., 2019). As nodes are geographically distributed in different regions there is no centralserver for them. Each node is consuming information as well asis working to provide information, so all nodes share the routing operations of the entire network (Feng et al., 2019). Also, P2P network has to discover and maintain communications with neighboring peers, as well as synchronizing with private data blocks (Feng et al., 2019). The blockchain has been categorized into public and private types (Feng et al., 2019). Most of the projects focus on the public blockchain because it gives them access to large numbers of markets, users, and network nodes, but also there are still those who prefer the private sector and consortia between a trusted and known group of participants (Feng et al., 2019).

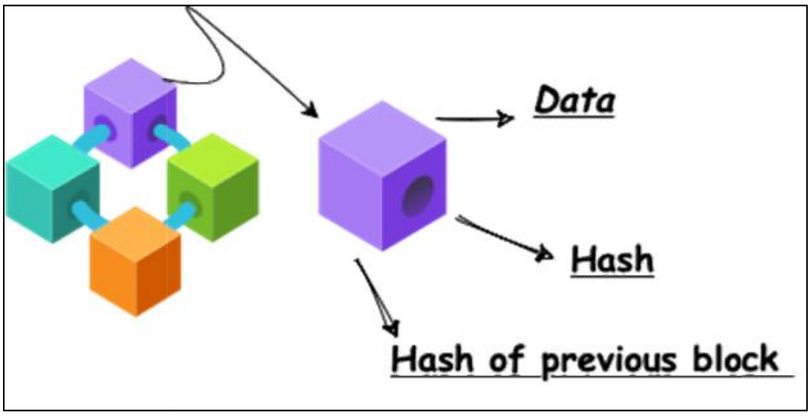


**Figure 1. Blockchain structure**

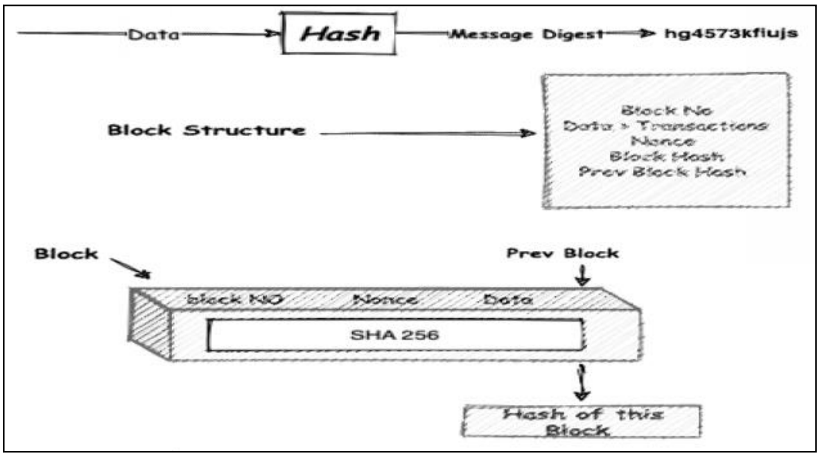
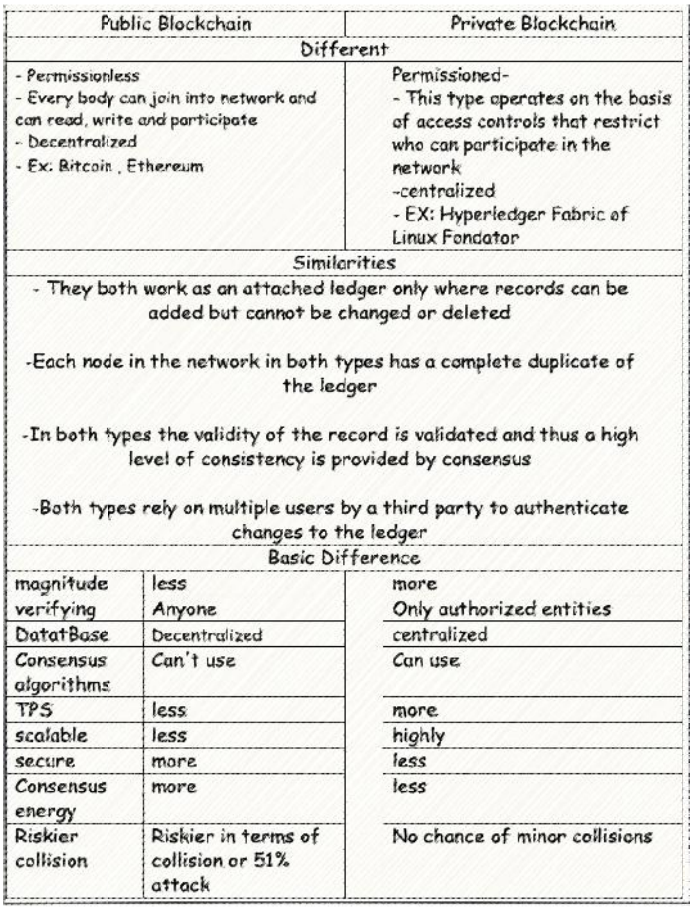


**Figure 2. General block structure in banking system**



| Public Blockchain | | Private Blockchain |
|---|---|---|
| Different | | |
| - Permissionless<br>- Every body can join into network and can read, write and participate<br>- Decentralized<br>- Ex: Bitcoin , Ethereum | | Permissioned-<br>- This type operates on the basis of access controls that restrict who can participate in the network<br>-centralized<br>- EX: Hyperledger Fabric of Linux Fondator |
| Similarities | | |
| - They both work as an attached ledger only where records can be added but cannot be changed or deleted<br>-Each node in the network in both types has a complete duplicate of the ledger<br>-In both types the validity of the record is validated and thus a high level of consistency is provided by consensus<br>-Both types rely on multiple users by a third party to authenticate changes to the ledger | | |
| Basic Difference | | |
| magnitude | less | more |
| verifying | Anyone | Only authorized entities |
| DatatBase | Decentralized | centralized |
| Consensus algorithms | Can't use | Can use |
| TPS | less | more |
| scalable | less | highly |
| secure | more | less |
| Consensus energy | more | less |
| Riskier collision | Riskier in terms of collision or 51% attack | No chance of minor collisions |

**Figure 3. comparison between private and public blockchain**

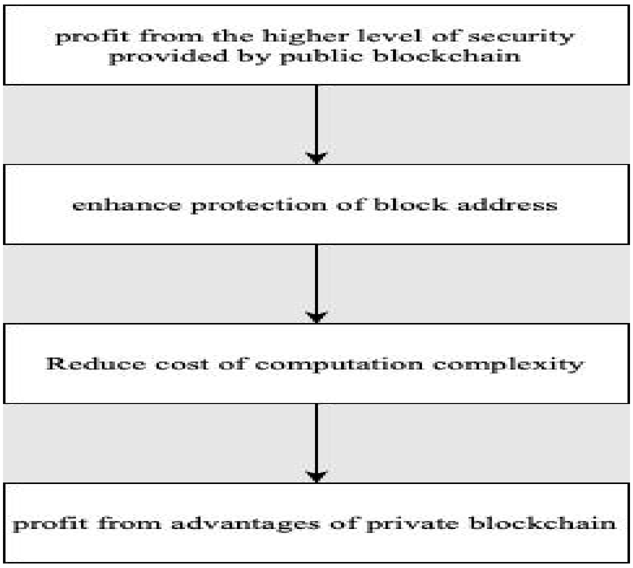

profit from the higher level of security provided by public blockchain
enhance protection of block address
Reduce cost of computation complexity
profit from advantages of private blockchain

**Figure 4. Contribution objectives**

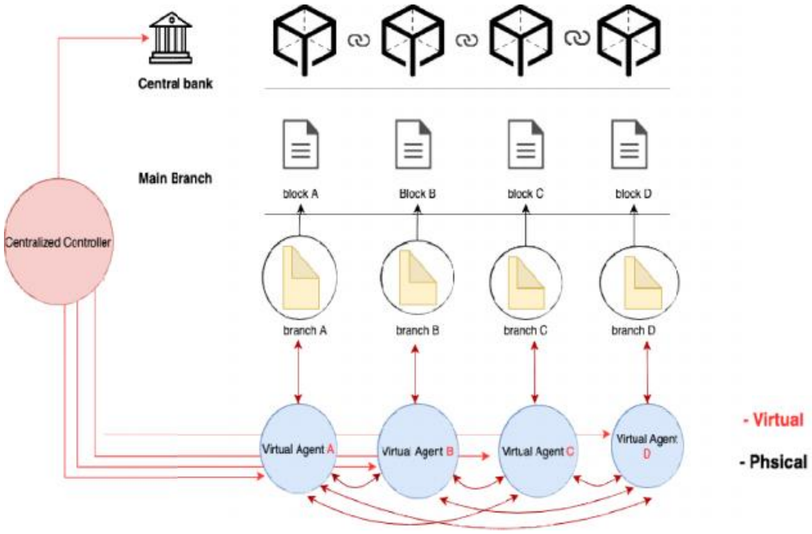


**Figure 5. Proposed system architecture**

Therefore, it is necessary to clarify these patterns and explain the differences between them (we give a comparison between private and public blockchain in Fig. 3).

- **Public Blockchain:** It is a chain of blockchain with whichany participant can read and present his transactions as well as ensure their validity, so participate in the reconciliation process between all parties (Feng et al., 2019). A public blockchain has a decentralized database of transactions on open networks (Feng et al., 2019). Public blockchain has the advantage of giving the system high confidentiality and integrity due to a large number of nodes and decentralization in it, but in return for that it has many problems, including the high cost of accounts and deployment, which leads to complexity in transactions
- **Private Blockchain:** It is often considered as the opposite of the public with all its basic characteristics, as it works to preserve the write permissions, for one institution, also the reading permissions are restricted or public (Feng et al., 2019). This pattern includes any non-public domain (Feng et al., 2019). This type has better flexibility in managementas well as many features and advantages. Independence (Autonomous): There is no single entity controlling transactions or the network.

**Distribution:** The blockchain system is built on the P2P network in the sense that every transaction of any private site is transmitted through the node that issued it to its peers,from the first point and then to the rest of its neighboring peers. Sustainability (Immutability): All transactions and validblocks that are recorded in the general ledger are completely non-modifiable. In addition, the global ledger will be fully synchronized between all nodes in the blockchain after the compatibility mechanisms, thus providing high degrees of trust to users that ensure the data in the blockchain is not modified in a very high and very short time. Contractual: The blockchain relies on a consensus process (such as voting) on data cases, whereby consensus is reached by implementing some of the rules from the blockchain without central permission. These rules, which were previously defined by the code, are included so that any procedure is executed and applied in the appropriate form and at the right time and to ensure that it is correct and without human intervention. Table 1. presents a comparison between public and private blockchain `regarding security and deployment.

## PROPOSED METHODOLOGY

Our main contribution is the combination of both private and public blockchain. We merge both of the previous two types to take advantage of each of them (the main objectives of the contribution are summarized in Fig. 4).

**Network Virtualization:** Software Defined Networking (SDN) is a network architecture that injects automation and programmability into the network by decoupling network control and forwarding functions. Network Function Virtualization (NFV) applies to the virtualization of network elements, while SDN is a network architecture that injects automation and programmability into the network by decoupling network control and forwarding functions. To put it another way, NFV virtualizes network infrastructure while SDN centralizes network management. SDN and NFV work together to build a network that is designed, controlled, and managed entirely by software [14]. Network virtualization is deployed in our contribution due to its various advantages among of them:

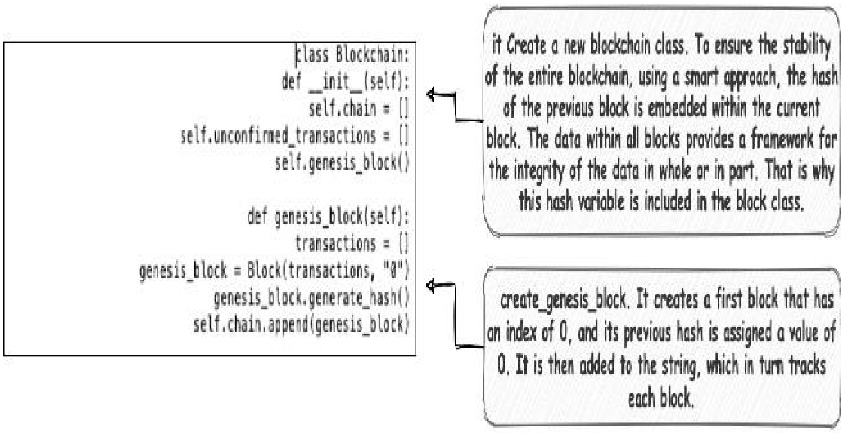
- Virtualizing a network allows network operators to save money, reduce time-to-market for new or upgraded products, and better scale and adapt the resources available to applications and services [15].
- Less Vendor Lock-In: Using COTS hardware to run VNFs ensures that companies aren't tied to proprietary, fixed-function boxes that require truck rolls and a lot of time and effort to deploy and conFigure [15].
- Greater Resource Efficiency: Since more can be achieved with less in a virtualized data center or other infrastructure, it is more economical to run. With increased workload capability, data center footprint, power usage, and cooling requirements can all be reduced or kept the same. Since a single server can run multiple VNFs at the same time, fewer servers are required to complete the same amount of work [15].
- Flexibility: NFV's versatility allows businesses to rapidly respond to evolving customer needs and emerging market opportunities [15].

**SDN networks have several benefits that can be used [14]:**

- The ability to manage the network more efficiently is enhanced by centralized control
- BOX without a control plane simplifies the process and reduces CAPEX
- Since the interfaces are "Open," they allow for automationand programmability
- A network virtualization enabler Virtual network (overlay)over a physical file
- A network is independent of the physical network

**Hybrid Public-Private Blockchain Schema:** Blockchain is classified for its private and public types, where the public blockchain was classified as more secure than private blockchain. Because its database is distributed, it is not easy to modify it, and if one block is modified, the entire blockchain changes, with knowledge of all of its participants. However, it iseasy to access block addresses and this matter may affect the privacy of data in the applications used for this technology as well as this type needs powerful and huge capabilities for computation and processing. In banks, the transaction must be characterized by two important characteristics, (protection and security), so it is not logical that the amount of processing time of transactions is long, and this matter is not desirable for banks at all because it disrupts transactions and reduces the quality of service. The private blockchain is considered less secure than its counterpart, but it is easy to change the chain because the database is centralized, however, the data in this type is more protected. It has many advantages such that its high privacy, efficiency, and ease of computation. Its scalability is excellentsince the entry into it is controlled where no person can read and write private data, so the data in this type is strongly protected because blockchain is not open. Banking systems require enhanced privacy by protecting blocks, reducing of " Infrastructure Costs "required to perform different computations. We propose a hybrid blockchain structure that applies the special properties of the blockchain physically and increases the general blockchain characteristics by default. Currently, all the advanced systems do not need physical devices and use virtual devices that have the same functions but with higher capabilities than them. We propose the use of a virtual network because of its advantages as it is cost-effective, reduces the business burden, better operating time, faster resource deployment, and economic and efficient use of energy (Rashid , Chaturvedi 2019). In the proposed architecture, there are many bank branches, andeach branch is linked to a special block, all the blocks are gathered in the central bank in the form of a blockchain, where the database is centralized. Physically, our blockchain is private. So to allow a new branch to add data into the blockchain, it must be approved by the central bank. However, as mentioned above, private blockchain has a lower security level than public blockchain. So, we propose to use a public blockchain but using network function virtualization. For each bank branch, we design a virtual agent that has a continuous link with the physical branch.

Whenever a new transaction is generated, it is added to the private blockchain and simultaneously it is sent to the virtual agent to add it in the public blockchain, virtually. We assume that Branch A sends and receives a transaction. Thistransaction will be sent to the central bank and added to the blockchain after verification at the same time. Branch A will send it to its ion, and this hypothetical entity is working to distribute it through a peer-to-peer network by default. It in turnperforms the accounts on the way of the public blockchain. (If Branch A performs the transaction, it has to send it to the centralbank in blockchain account at the same time the transaction hasto to be sent to the virtual agent to make computation through the private-public blockchain. The information is published to all other virtual agents in the proposed system. As Fig. 5 presents, agents A,B,C and D are virtual entities that communicate easily through the peer-to-peer network. The function of a virtual device is to receive transactions, add them to the blockchain, and compare it to the blockchain of others agents. For example, Agent A sends and receives a transaction to and from the central bank and the bank must calculate the private blockchain. At the same time, the transaction has to be sent to the virtual agent A which has to make computation in a public blockchain manner. A centralized controller has to compare between public and private blockchains, generated by both physical and virtual branches. The centralized controller confirms and verifies the blockchains, their accuracy, and their integrity and can save them in separate entities in the cloud. Once it detects that there is no match, the controller can retrieve the fault chain and rejectthe transaction that caused the problem and send an alarm to thecentral bank and tell it about the block that may be the cause of the problem.



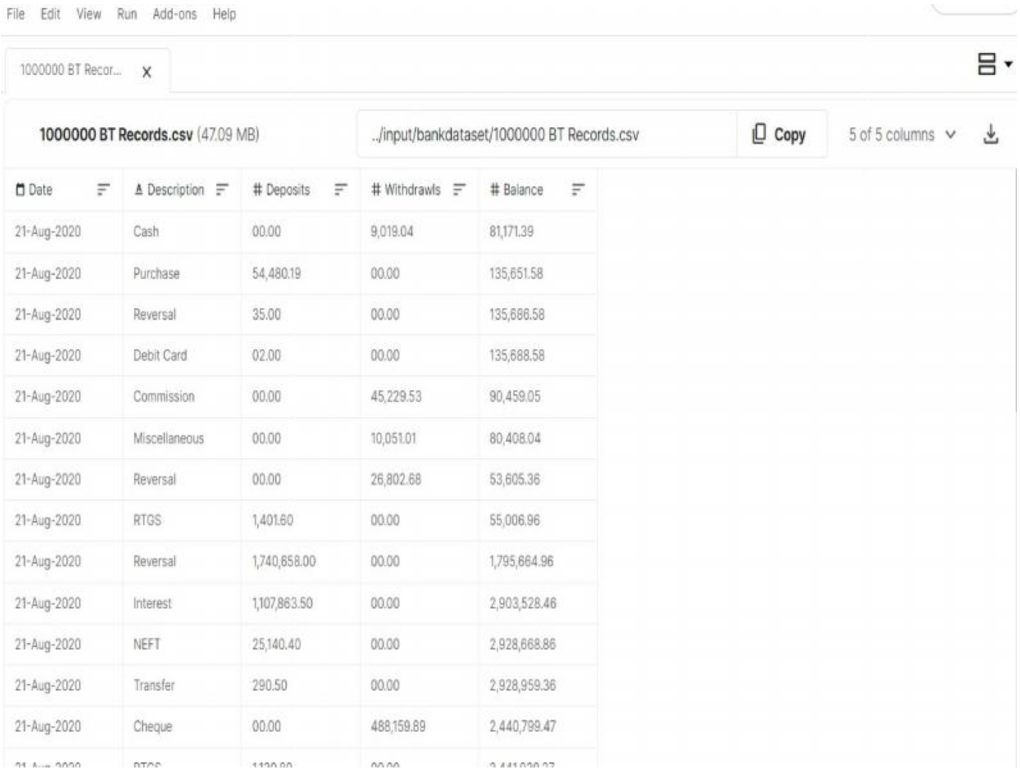
```
class Blockchain:
    def __init__(self):
        self.chain = []
        self.unconfirmed_transactions = []
        self.genesis_block()

    def genesis_block(self):
        transactions = []
        genesis_block = Block(transactions, "0")
        genesis_block.generate_hash()
        self.chain.append(genesis_block)
```

it Create a new blockchain class. To ensure the stability of the entire blockchain, using a smart approach, the hash of the previous block is embedded within the current block. The data within all blocks provides a framework for the integrity of the data in whole or in part. That is why this hash variable is included in the block class.

create_genesis_block. It creates a first block that has an index of 0, and its previous hash is assigned a value of 0. It is then added to the string, which in turn tracks each block.

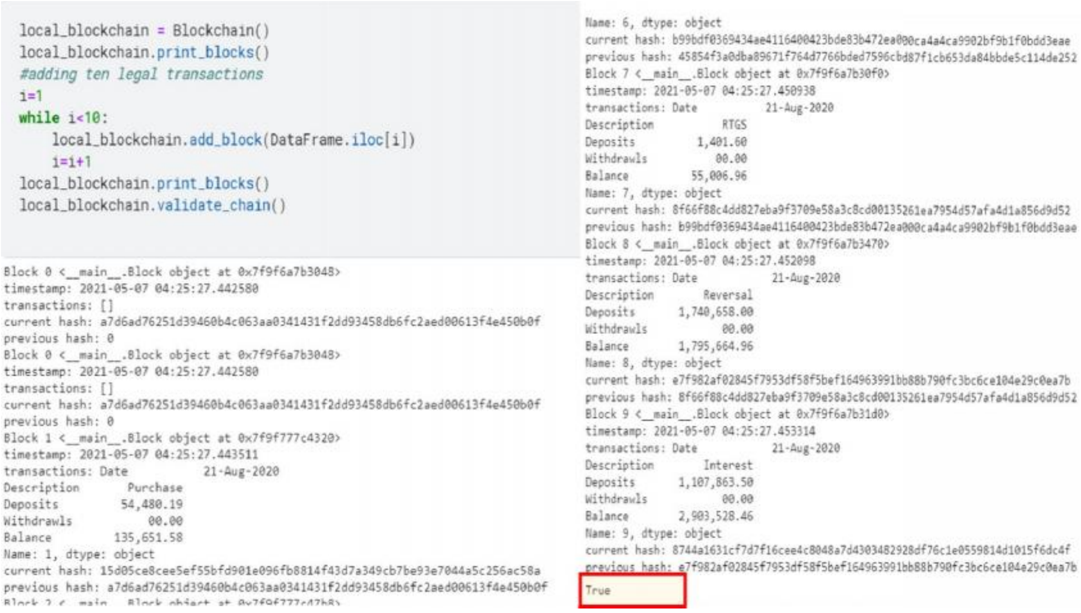
**Figure 6. Blockchain class**



1000000 BT Records.csv (47.09 MB) ../input/bankdataset/1000000 BT Records.csv

| Date | Description | # Deposits | # Withdrawls | # Balance |
|---|---|---|---|---|
| 21-Aug-2020 | Cash | 00.00 | 9,019.04 | 81,171.39 |
| 21-Aug-2020 | Purchase | 54,480.19 | 00.00 | 135,651.58 |
| 21-Aug-2020 | Reversal | 35.00 | 00.00 | 135,686.58 |
| 21-Aug-2020 | Debit Card | 02.00 | 00.00 | 135,688.58 |
| 21-Aug-2020 | Commission | 00.00 | 45,229.53 | 90,459.05 |
| 21-Aug-2020 | Miscellaneous | 00.00 | 10,051.01 | 80,408.04 |
| 21-Aug-2020 | Reversal | 00.00 | 26,802.68 | 53,605.36 |
| 21-Aug-2020 | RTGS | 1,401.60 | 00.00 | 55,006.96 |
| 21-Aug-2020 | Reversal | 1,740,658.00 | 00.00 | 1,795,664.96 |
| 21-Aug-2020 | Interest | 1,107,863.50 | 00.00 | 2,903,528.46 |
| 21-Aug-2020 | NEFT | 25,140.40 | 00.00 | 2,928,668.86 |
| 21-Aug-2020 | Transfer | 290.50 | 00.00 | 2,928,959.36 |
| 21-Aug-2020 | Cheque | 00.00 | 488,159.89 | 2,440,799.47 |
| 21-Aug-2020 | RTGS | 1120.80 | 00.00 | 2,441,920.27 |

**Figure 7. Bank data set**

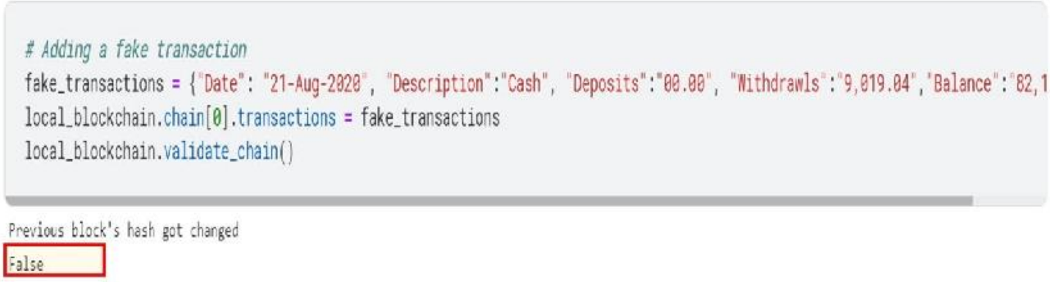


```
local_blockchain = Blockchain()
local_blockchain.print_blocks()
#adding ten legal transactions
i=1
while i<10:
    local_blockchain.add_block(DataFrame.iloc[i])
    i=i+1
local_blockchain.print_blocks()
local_blockchain.validate_chain()
```

```
Block 0 <__main__.Block object at 0x7f9f6a7b3048>
timestamp: 2021-05-07 04:25:27.442580
transactions: []
current hash: a7d6ad76251d39460b4c063aa0341431f2dd93458db6fc2aed00613f4e450b0f
previous hash: 0
Block 0 <__main__.Block object at 0x7f9f6a7b3048>
timestamp: 2021-05-07 04:25:27.442580
transactions: []
current hash: a7d6ad76251d39460b4c063aa0341431f2dd93458db6fc2aed00613f4e450b0f
previous hash: 0
Block 1 <__main__.Block object at 0x7f9f777c4320>
timestamp: 2021-05-07 04:25:27.443511
transactions: Date            21-Aug-2020
Description       Purchase
Deposits         54,480.19
Withdrawls           00.00
Balance         135,651.58
Name: 1, dtype: object
current hash: 15d05ce8cee5ef55bfd901e096fb8814f43d7a349cb7be93e7044a5c256ac58a
previous hash: a7d6ad76251d39460b4c063aa0341431f2dd93458db6fc2aed00613f4e450b0f
Block 2 <__main__.Block object at 0x7f9f777c47b8>
```

```
Name: 6, dtype: object
current hash: b99bdf0369434ae4116400423bde83b472ea000ca4a4ca9902bf9b1f0bdd3eae
previous hash: 45854f3a0dba89671f764d7766bded7596cbd87f1cb653da84bbde5c114de252
Block 7 <__main__.Block object at 0x7f9f6a7b30f0>
timestamp: 2021-05-07 04:25:27.450938
transactions: Date           21-Aug-2020
Description           RTGS
Deposits          1,401.60
Withdrawls           00.00
Balance          55,006.96
Name: 7, dtype: object
current hash: 8f66f88c4dd827eba9f3709e58a3c8cd00135261ea7954d57afa4d1a856d9d52
previous hash: b99bdf0369434ae4116400423bde83b472ea000ca4a4ca9902bf9b1f0bdd3eae
Block 8 <__main__.Block object at 0x7f9f6a7b3470>
timestamp: 2021-05-07 04:25:27.452098
transactions: Date            21-Aug-2020
Description        Reversal
Deposits       1,740,658.00
Withdrawls            00.00
Balance        1,795,664.96
Name: 8, dtype: object
current hash: e7f982af02845f7953df58f5bef164963991bb88b790fc3bc6ce104e29c0ea7b
previous hash: 8f66f88c4dd827eba9f3709e58a3c8cd00135261ea7954d57afa4d1a856d9d52
Block 9 <__main__.Block object at 0x7f9f6a7b31d0>
timestamp: 2021-05-07 04:25:27.453314
transactions: Date            21-Aug-2020
Description        Interest
Deposits       1,107,863.50
Withdrawls            00.00
Balance        2,903,528.46
Name: 9, dtype: object
current hash: 8744a1631cf7d7f16cee4c8048a7d4303482928df76c1e0559814d1015f6dc4f
previous hash: e7f982af02845f7953df58f5bef164963991bb88b790fc3bc6ce104e29c0ea7b
True
```

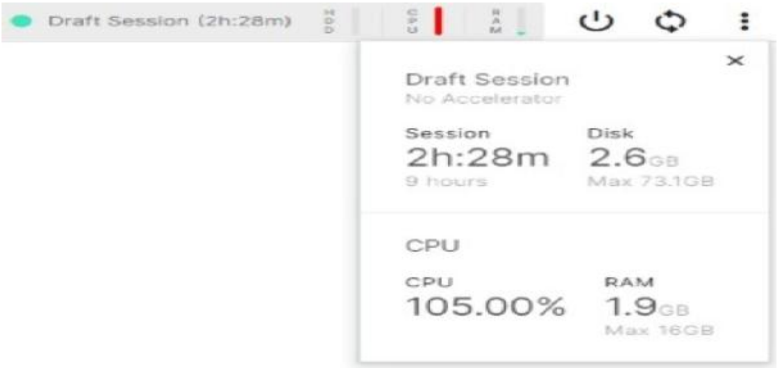
**Figure 8. Adding legal transactions**



```
# Adding a fake transaction
fake_transactions = {"Date": "21-Aug-2020", "Description":"Cash", "Deposits":"00.00", "Withdrawls":"9,019.04","Balance":"82,1
local_blockchain.chain[0].transactions = fake_transactions
local_blockchain.validate_chain()
```

```
Previous block's hash got changed
False
```

**Figure 9. Adding fake transactions and blockchain validation**



Draft Session
No Accelerator

Session 2h:28m
9 hours

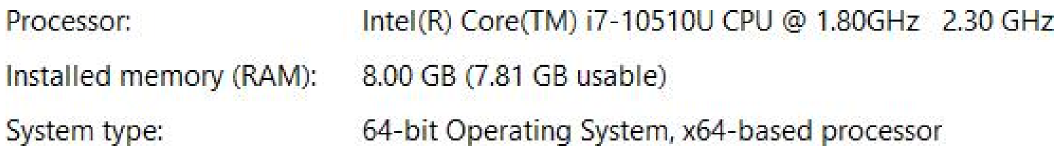
Disk 2.6GB
Max 73.1GB

CPU

CPU 105.00%

RAM 1.9GB
Max 16GB

**Figure 10. Computation complexity of public blockchain**



| | |
|---|---|
| Processor: | Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz |
| Installed memory (RAM): | 8.00 GB (7.81 GB usable) |
| System type: | 64-bit Operating System, x64-based processor |

**Figure 11. Processor capabilities**

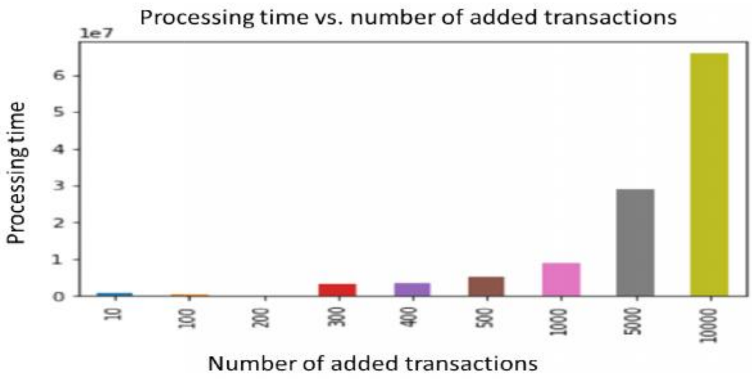


**Figure 12. processing time vs. number of added transactions**

**Table 1. Private vs. private blockchain: security efficiency and ease of deployment**

| | Stronger security | Easier on deployment | HigherCost of deployment | Better confidentiality |
|---|---|---|---|---|
| public | ✓\| | \| | ✓\| | ✓\| |
| Private | \| | ✓\| | \| | \| |

**Table 2. response time for adding various number of transactions**

| Task | year | month | date | hours | minutes | second | μs |
|---|---|---|---|---|---|---|---|
| Initially | 2021 | 5 | 7 | 3 | 1 | 59 | 88295 |
| Adding 10 transaction | 2021 | 5 | 7 | 3 | 2 | 0 | 7843 |
| Adding 100 transaction | 2021 | 5 | 7 | 3 | 2 | 0 | 399634 |
| Adding 200 transaction | 2021 | 5 | 7 | 3 | 2 | 0 | 551841 |
| Adding 300 transaction | 2021 | 5 | 7 | 3 | 2 | 3 | 710061 |
| Adding 400 transaction | 2021 | 5 | 7 | 3 | 2 | 7 | 247961 |
| Adding 500 transaction | 2021 | 5 | 7 | 3 | 2 | 12 | 469351 |
| Adding 1000 transaction | 2021 | 5 | 7 | 3 | 2 | 21 | 646576 |
| Adding 5000 transaction | 2021 | 5 | 7 | 3 | 2 | 50 | 735018 |
| Adding 10000 transaction | 2021 | 5 | 7 | 3 | 3 | 56 | 528668 |

**Table 3. processing time**

| Transaction Performed | Time |
|---|---|
| 10 | 919548 |
| 100 | 391791 |
| 200 | 152207 |
| 300 | 3158220 |
| 400 | 3537900 |
| 500 | 5221390 |
| 1000 | 9177225 |
| 5000 | 29088442 |
| 10000 | 65793650 |

The data protection rests on the responsibility of the physical part that it uses the private blockchain, so no one can enter or change the blockchain, and there is parallel computing with the virtual part to the blockchain to reduce the complexity. This system and this comparison guarantee the integrity of the blockchain with the protection of addresses of the blocks through the private blockchain, as well as reduce the complexity of computation through the public blockchain. The centralized controller has functions such as comparison between the public blockchain generated by virtual agents and the private blockchain generated by physical entities, make a copy and keep it on the default system in the cloud. These copies are used whenever we need them in case of an emergency. Network optimization for data transfer speeds, scalability, reliability, resilience, and security are all possible with architecture virtualization. It also automates a lot of network management activities.

# RESULTS AND DISCUSSION

This section discusses the results and discussion which are obtained from the implementation. To validate our proposal, we will build a blockchain using python programming languages, library sha256 from hashlib for keys encryptions, and pandas for data set interpretation, Fig. 6 presents the blockchain class. For the dataset, we downloaded a bank data set with 5 columns and 1000000 rows (Fig. 7 gives a print of the used data set). Transactions that are added to the blockchain are based on data of this data set.

**Adding legal transactions:** In the first stage, and to verify the validity of our proposal, we added 10 valid legal transactions. We started by experimenting with ten blocks, then we found out that the verification is validand that the blockchain is 100% correct as shown in Fig. 8.

**Adding a Fake Transaction:** in the second stage, as shown in Fig 9, we tried to change one of the blocks. Then, after verifying the blockchain, this modification was identified as illegal. After the recalculation of the transaction, the proposed system did notaccept this modification and showed an "error" due to a change in the original hash of the transaction. In this case, the virtual centralized controller has to notify the central bank with this error to reject the modified transaction and recover the original transaction, that was already saved in the cloud.

**Processing time evaluation:** To evaluate the cost of computation of the public blockchain, performed by the virtual agents, we tested the system response time in case of adding various numbers of a transaction, as shown in table 2. Then we computed the processing time in table 3. As reported in Fig. 10, the central processing unit of the computeris at 105% working, due to the complexity of computation (processor capabilities are summarized in Fig. 11). We draw in Fig. 11 the processing time vs. the number of added transactions into the public blockchain. We can easily see that the processing time grows proportionally with the number of transactions. Of course, this complexity is computed inside only one node. In a public blockchain, each node has to perform the computation so the cost will be increased by the number of connected nodes (branches in the banking system). However, ourmain idea is to use the virtualization of functions. This may resolve this problem since physically, the branches will compute the blockchain using a private concept which is too much easier and faster. In addition, branches are not asked to waste time validating the public blockchain since this is the function of the virtual central controller which will send an alert to the central bank, in which the central database is saved, in case of detection of modificationor fault transaction.

# CONCLUSION

In this paper, we propose a hybrid blockchain architecture that combines private and public blockchain in banking transaction validation. The proposed system is physically private however virtually public. Private blockchain guarantees the ease of deployment as well asthe rapidity and scalability of computation. Networkvirtualization is adapted since its cost of deployment is reduced and easy to use and guarantee a robust and secure system since no node will be able to alter transaction because all the agents in the blockchain will perform verification after each transaction modification

# REFERENCES

El-kenawy, E. S. M. T., Saber, M., & Arnous, R. (2019). An Integrated Framework to Ensure Information Security Over the Internet. International Journal of Computer Applications, 975, 8887.

Gahan, A., & Devanagavi, G. (2019). A empirical study of security issues in encryption techniques. Int J Appl Eng Res,14.

Mukund R. Joshi, Renuka Avinash Karkade "Network Security with Cryptography" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 1, pp.201 – 204 January 2015.

Namasudra, S., Devi, D., Choudhary, S., Patan, R., & Kallam, S. (2018). Security, privacy, trust, and anonymity. Advances ofDNA Computing in Cryptography, 1, 138-150.

Sun, H., Mao, H., Bai, X., Chen, Z., Hu, K., & Yu, W. (2017).

Multi-blockchain model for central bank digital currency. In 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT) (pp. 360-367). IEEE.

Wang, H., Ma, S., Dai, H. N., Imran, M., & Wang, T. (2020).

Blockchain-based data privacy management with nudge theory in open banking. Future Generation Computer Systems, 110, 812-823.

Han, X., Yuan, Y., & Wang, F. Y. (2019, November). A blockchain-based framework for central bank digital currency. In 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) (pp. 263-268). IEEE.

Dai W., Gu X., Teng Y. (2020) A Supervised Anonymous Issuance Scheme of Central Bank Digital Currency Based on Blockchain. In: Qiu M. (eds) *Algorithms and Architectures for Parallel Processing. ICA3PP 2020. Lecture Notes in Computer Science, vol 12454. Springer, Cham. https://doi.org/10.1007/978-3-030-60248-2_32*

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed

ledger. International Journal of Research in Engineering and Technology, 5(9), 1-10.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45-58.

Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, *4*.

https://telcocloudbridge.com/blog/ultimate-guide-to-role-of-sdn- in-nfv/ https://www.sdxcentral.com/ networking/ nfv/definitions/whats- network-functions-virtualization-nfv/

Rashid, A., & Chaturvedi, A. (2019). Virtualization and its role in Cloud Computing environment. *International Journal of Computer Sciences and Engineering*, *7*(4).

*******