# Integration Of Consortium Blockchain Model In The Nigerian Banking Sector

Oluwaseun, A. Ojerinde
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
o.ojerinde@futminna.edu.ng

Jonathan, Salawu
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
salawu.jonathan@st.futminna.edu.ng

Opeyemi, A. Abisoye
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
o.abisoye@futminna.edu.ng

Andrew, A. Uduimoh
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
a.uduimoh@futminna.edu.ng

## ABSTRACT

Conventionally, Nigerian banks rely on a less secure and time-consuming centralized clearinghouse where transactions are sorted out and balances are made. This paper presents a model for integrating permission DLT into the Nigerian banking sector. The proposed model has utilized Corda – permissioned DLT, to log transactions between parties on the chain such that those transactions are only visible to the participants of the transaction, thus, combatting fraudulent claims. Participants' details are also verified upon provision of their National Identification Number (NIN) and Bank Verification Number (BVN) as stipulated in the smart contract. This work has also avoided the problems inherent in the public blockchain that requires miners to spend gigantic computer resources and time validating and verifying blocks before being added to the chain. The result obtained is a developed DLT model for logging real-time transactions between banks and their clients.

**ACM Reference Format:**
Oluwaseun, A. Ojerinde, Jonathan, Salawu, Opeyemi, A. Abisoye, and Andrew, A. Uduimoh. 2021. Integration Of Consortium Blockchain Model In The Nigerian Banking Sector. In *The 5th International Conference on Future Networks & Distributed Systems (ICFNDS 2021), December 15, 16, 2021, Dubai, United Arab Emirates.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3508072.3508110

## 1 INTRODUCTION

Distributed ledger technologies, sometimes known as blockchains or blockchain-based platforms, have risen from the outskirts of public consciousness to be hailed as paradigm-shifting innovations. Blockchain and distributed ledger technology (DLT) are new methods for digitally managing data in a decentralized way, revolutionizing how people, businesses, and organizations exchange and trade with one another.

In the commercial and academic worlds, blockchain is one of the most talked-about subjects [1]. It was initially introduced with Bitcoin in 2008 as a peer-to-peer payment system for electronic transactions that enabled diverse financial actors to transmit payments to one another without the need for a central agency (such as a central bank), thereby avoiding the issue of double-spending [2].

Large corporations and governments are becoming more interested in learning more about the benefits of blockchain and distributed ledger technology. In contrast to bitcoin's open design, the banking industry and other economic sectors have concentrated on permissioned networks while developing enterprise-grade blockchains. In financial services and other sectors, federated blockchain models hold the greatest promise as future enterprise-grade platforms [3].

Banks and other financial organizations only need a few nodes to create consensus, they do not need nearly as much computing power to protect the network, which allows for more scalability. Validators — those responsible for validating transactions inside a blockchain – are not needed to compete with hashing power for cryptocurrency rewards, unlike public blockchain since sustaining the network is a common interest. It indicates that, rather than decentralization, the financial industry is favoring blockchain models that can provide security and scalability [4].

The development of public and private key systems predates the advent of the blockchain [5]. Asymmetric cryptography was invented by Diffie and Hellman in 1976, marking the beginning of the key system's evolution [6]. Two parties can create a secure connection using a public key system and transfer information over a public network. It operates by encrypting data and sending it to the other party using their public keys. The counterparty will use its private deciphering key to decode the communication.

The main focus of this work is to address the security issues and disjointedness of banks and their clients. The consortium blockchain model for banks provided in this work would help log transactions on an irreversible and decentralized ledger thereby enabling parties to verify transactions in which they are actively involved. This model also addresses the non-atomic nature of the conventional banks' databases, in the case of an incomplete money transfer operation, for instance.

*ICFNDS 2021, December 15, 16, 2021, Dubai, United Arab Emirates*
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8734-7/21/12…$15.00
https://doi.org/10.1145/3508072.3508110

## 1.1 Bank and FinTech

Financial technology, also known as ‘FinTech’, denotes the use of computer programs or other technology to assist the financial industry and banking institutions [8]. The term was used for the first time at the beginning of the 1990s [9] and what started as a word related solely to the financial industry, soon expanded into other very diverse sectors. Since early 2014, the sector has started attracting the attention of regulators, industry members, customers, and academics [10]. Blockchain in FinTech appeared for the first time as the distributed ledgers of Bitcoin but has recently attracted consideration from practitioners and researchers [11]. Today, financial institutions and other market participants, mainly due to the development of blockchain technology, are approving the nature of FinTech and the necessity for research in the academic world given the implications of this technology. Financial innovation is not something new, as it has an extensive history. The development of FinTech throughout history can be divided into three main eras [10]. Table 1 shows the three types of blockchain systems.

- FinTech 1.0 (1866–1967): Finance began to develop in agricultural states during this period. Money was first used to facilitate financial transactions because of its main advantage of transferring its value. Railroad advancements and the invention of sustainability in the nineteenth century. The telegraph allowed for cross-border communication. Following WWI, technological advancements accelerated, laying the groundwork for the next FinTech era.
- FinTech 2.0 (1967–2008): In this period, electronic payment methods have grown rapidly. British banks began using what is now known as BACS (Bankers’ Automated Clearing Services) in 1968 when they established the Inter-Bank Computer Bureau. Regulations in the financial technology industry began to take effect as a result of the failure of Herstatt Bank in 1974. It was confirmed that worldwide markets were technologically linked after the stock market crash of 1987 (also known as Black Monday). There were technological advancements in risk management systems and online consumer banking throughout the 1990s. Due to the hazards presented by digital banking, regulators paid extra attention to it when it first emerged (banks were the only legal monetary organizations at the time) [12].
- FinTech 3.0 (2008–present): The beginning of this era was characterized by the financial turmoil of the years 2007–2008. Trust in the banking system started deteriorating, and technology firms started to operate through peer-to-peer networks outside the regulatory framework (in China alone over 2000 platforms were developed). Today, these technological firms and many start-ups are displacing banks at a pace never seen before. Flexible regulations that stimulate entrepreneurship [13] are beginning to be adopted by some countries.

## 1.2 Smart Contracts

A smart contract is a digital contract that allows terms dependent on a decentralized consensus that is tamperproof and often self-enforcing through automated execution [14]

Nick Szabo first proposed the idea of smart contracts in 1994. Essentially, smart contracts are automated transaction procedures that carry out the conditions of an agreement. Thus, all contract clauses are stored electronically on the computers of those who transact business [15]. There’s no need for a central authority or third-party support because these contracts are automatically performed when certain conditions are met.

# 2 BLOCKCHAIN IN NIGERIAN BANKS

## 2.1 Transaction speed

If a Nigerian banking payment involves crosses borders and exchanges, it could take days or weeks for clearing and settlement to occur because of inefficiencies in reconciling records on separate ledgers from intermediaries. Blockchain technology removes all these loopholes and allows instant transactions across border trade for better commerce.

## 2.2 Dispute settlement

Even though digital payment solutions are already popular, money transfers between individuals (especially when dealing for the first time) have always had trust and transaction fee issues if the money was sent or not.

That is the reason why a third-party monetary escrow like banks and other financial services came into play. Banks can integrate blockchain technology into their systems and have all banking transactions send tokens including the transaction details to tackle the problem. This is then recorded on the blockchain network of the bank as evidence of payment.

When there are payment disputes between two peer users, this will reduce the stress and process required for one to undergo in getting out payment/transaction verification details from banks. They can simply view their transaction on the blockchain network to see it was recorded.

## 2.3 Reducing Friction in Global Markets Caused by Banks

Friction in global market transactions makes getting financing and completing trades a lengthy and complex process for anyone.

Nigerian banking activities such as lending, issuing letters of credit, factoring, all involve paper documents in the traditional banking system; sent to and fro to be validated and reconciled by different third parties and senders/receivers. In the interim, capital gets tied up and business slows down leading to loss on the receiver as he/she pays extra charges while waiting for days/weeks to have transactions confirmed. All these problems can be mitigated by integrating blockchain technology into the Nigeria Banking system.

## 2.4 Payment security

Blockchain will help Nigerian banks with banking security as transactions done on the blockchain are secured and cannot be hacked. Every monetary transaction carried out on the blockchain cannot be forged and as such, there is a higher level of trust than banking traditionally where there are always disputes of misplaced funds and manipulated transactions.

**Table 1: Three types of blockchain systems**

| | Public blockchain | Consortium blockchain | Private blockchain |
|---|---|---|---|
| Managing entity | All participants (decentralization) | Participants in the consortium | One central institution holds all the authority |
| Governance | It is very difficult to change the rule that has been made | Rules can be changed easily through the agreement among consortium members | Rules could be changed easily according to the decision made by the central institution |
| Transaction speed | Difficult to expand the network, and transaction speed is slow | Easy to expand the network and transaction speed is fast | Very easy to expand the network and transaction speed is fast |
| Data access | Everyone can access it | Only authorized users can access it | Only authorized users may access it |
| Identifiability | Pseudo-anonymous | Identifiable | Identifiable |
| Transaction Proof | Proof of transaction is decided by algorithms such as PoW and PoS, and cannot be known in advance | Proof of transaction is known through authentication, and transaction verification and block generation are made according to the rules agreed in advance | Proof of transaction is made by a central institution |
| Examples | Bitcoin | R3, Hyperledger Fabric, Quorum, Ethereum | Linq, a stock exchange platform for Nasdaq unlisted companies |

Financial sector favours permission-based consortium model Source: Financial Services Commission (2016)

# 3 METHODOLOGY

The proposed solution is to integrate Distributed Ledger Technology - blockchain into the Nigerian banking sector to provide for a fast and secure distributed ledger management across parties. The architecture of the system is illustrated in Figure 1.

## 3.1 System Design

System design comprises the entities of this project and the individual modules that form the overall system.

The system architecture is shown in Figure 2. It comprises transacting BANKS registered as members in the network of the consortium blockchain. Banks are linked to each other via a consortium ledger and they are connected to those ledgers via an authenticated link. The authenticated link shows a vital part of Corda's DLT – privacy and scalability. It means that BANKS can only view transactions on the ledger of which it partook. On the blockchain's smart contract are a BVN and NIN verification and lookup engine that ensures that transacting customers on any BANK is duly registered. As transactions are carried out, they are logged real-time into the ledger and updated on the recipient node instead of waiting to be added to a block before being added to the chain (in the case of a "Blockchain"). Every transaction on the ledger is assigned a unique key and transaction hash based on some cryptographic function. Say, a public key is defined as (pubKey, n) and a private key is defined as (priKey) then

$$transaction^{pubKey} \equiv encTranction\ mod\ n \tag{1}$$

$$encMessge^{\ priKey} \equiv transaction\ mod\ n \tag{2}$$

$$transaction = \left(\sum N + AN + RN + A + BA + BB + BVN + NIN\right) \tag{3}$$

Where: $N$, $AN, RN, A, BA, BB, BVN, NIN$ corresponds to Name, accountNumber, receiverNumber, amount, BankA, BankB, BVN and NIN respectively.

With banks performing transactions every day and logging such transactions in their ledger before a clearinghouse sits, those transaction data form the major input into the DLT system. Upon integrating, such data for every customer whose NIN and BVN have been verified are logged into the blockchain and the effect becomes binding on the other responder or node. Because the idea of miners and Proof of Work is no more, (for a consortium DLT) time taken and computing resources expended for registering transactions are greatly reduced. The architecture treats every transaction as a private chain where participants are nodes, for instance, BANK_A, BANK_B, and so on, and transactions they commit are only visible to them on the chain.

## 3.2 Technology and Implementation

Corda is a financial blockchain solution developed by R3 to serve as a secured decentralized ledger technology for banking and FinTech needs. CordApps can be developed using any JVM-supported languages like JAVA and KOTLIN.

The goal of this project is to utilize Corda to build a DLT for the banking sector. SPRING BOOT will serve as the backend enterprise language for robust functionality and high interoperability between banks.

The following modules form the whole architectural design of the system

**Smart contracts:** Smart contracts for the DLT serve as automated, tamper-proof, and self-enforcing rules that guide transactions in the consortium blockchain. They are written in Java into the blockchain network.

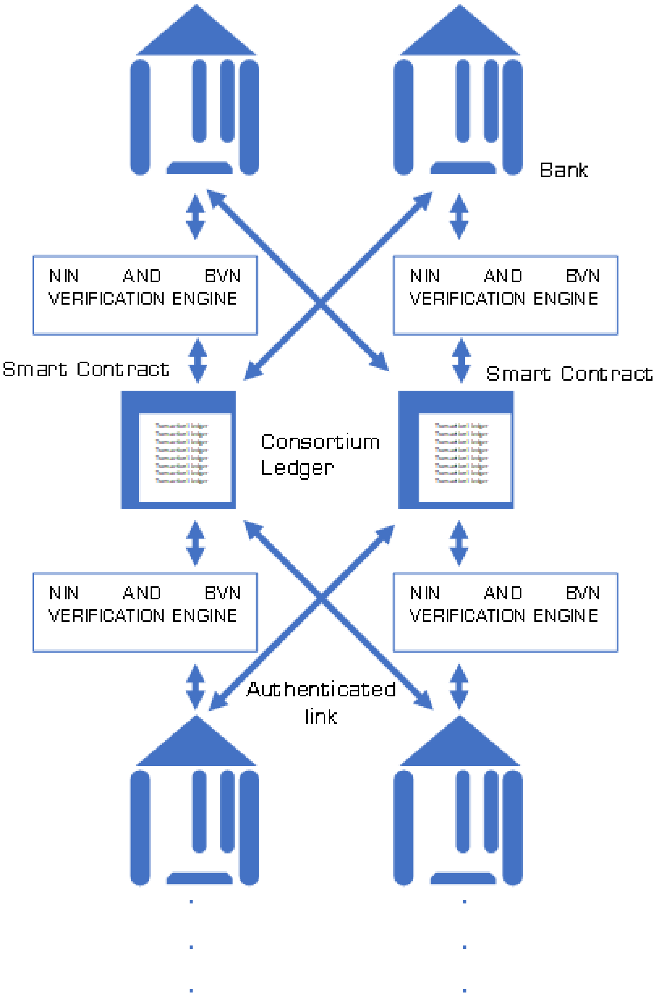

Bank
NIN AND BVN VERIFICATION ENGINE
NIN AND BVN VERIFICATION ENGINE
Smart Contract
Smart Contract
Consortium Ledger
NIN AND BVN VERIFICATION ENGINE
NIN AND BVN VERIFICATION ENGINE
Authenticated link

**Figure 1: Architecture of the system**

**Parties:** Parties refer to the banks and clients whose transactions are added to the chain.

**NIN and BVN engine**: This engine is built into the smart contract that provides NIN and BVN authentication for every entity in the network.

**Notaries**: These help to prevent double-spending and maintain the sanity of data in the blockchain.

# 4 RESULTS AND DISCUSSION

## 4.1 Transaction Per Second (TPS)

A key criterion in scaling up any blockchain platform is the number of transactions per second the system can process. In the early stages of evaluating this metric, however, care must be taken to ensure the comparison is done in a like-for-like manner. Corda offers the following standard for consideration on comparing Corda's Consortium DLT performance to an alternate platform. The following has been adhered to when measuring a transaction

- **Start** should commence from the point at which the party that is building the transaction (contract or other terms) does its verification and submits the transaction to the Notary Pool for a uniqueness check.
- **The finish** should be regarded as the point at which the transaction has been acknowledged as being added to the record which is used for the prevention of double-spending.
- All variables such as the transactions, hardware, and network properties should be consistent.

Table 2 compares the transaction per second of the developed DLT on Corda and other blockchain implementation schemes.

## 4.2 Experimental Setup

Corda's consortium architecture forms the underlying process of this project. Since Corda architecture does not support proof of work consensus algorithm like in Blockchain, nodes that do not partake in a transaction need not be involved in the computational

**Table 2: TPS comparison between Corda and other Blockchain implementation**

| Corda (DLT) | 1678 TPS |
|---|---|
| Bitcoin | 7 TPS |
| Ethereum | 15 TPS |

Source: Corda Docs

process of validating the ledger. To develop the banking solution DLT, three parties have been considered, BANK_A and BANK_B and Notary.

### 4.2.1 *Implementation.*

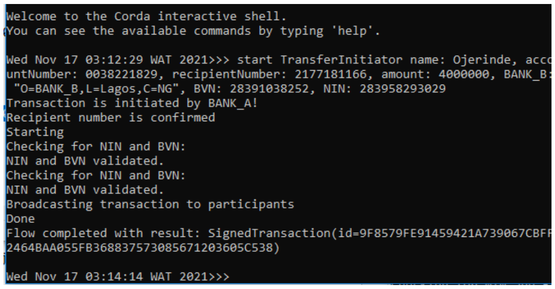
- **NODES**: Three nodes labeled BANK_A, BANK_B and Notary are created to mimic inter-bank transactions. Either bank can serve as the initiator or receiver of a transaction. The Notary is a concept in Corda that keeps track of inputs and outputs of transactions to identify double-spending attempts. This ensures that transactions between BANK_A and BANK_B are free from double-spending i.e BANK_A or BANK_B cannot consume a particular token more than once.
- Initially, to gain membership in a private network, a KYC (Know your client) process is manually done. Upon successful completion of a KYC process, a digital certificate would be issued to the bank (say BANK_A) of which they exclusively hold the private key. Therefore, transactions signed by that particular node can only have originated from BANK_A. Secondly, given a Bank's name (say BANK_A,) – plus, for Corda, the company's city and country – these technologies themselves allow a lookup of that company's associated node on the private network. Thus, it is reassuring to know who you are doing business with.
- **SPRING BOOT:** The spring boot server (with Tomcat server) has been used to expose the Nodes through Remote Procedure Call (RPC). The flow functions provided by the DLT can be initiated through API calls to the Spring Boot server. The Spring Boot server is deployed on an Intel Core i5 CPU @2.50 GHz with 8GB RAM running Windows 10 OS.
- **SMART CONTRACT:** The smart contract for the transaction is built into the transaction flow and they are checked before a transaction is validated.
- NIN and BVN constraints: These constraints are validated before a transaction flow is established.
- Sender Signature: An initiating bank must sign a transaction before it is processed by the Notary and subsequently added to the ledger.
- **TRANSACTION FLOW:** The nodes are deployed using the command on Windows:

We then proceed to start up the three nodes namely BANK_A, BANK_B, and Notary.

After the three nodes start-up, we proceed to run a sample transaction from BANK_A to BANK_B with the following code:

```
start TransferInitiator name: Ojerinde, accountNumber: 0038221829, recipientNumber: 2177181166, amount: 4000000,BANK\_B: "O=BAN
```

The transaction is shown in Figure 2

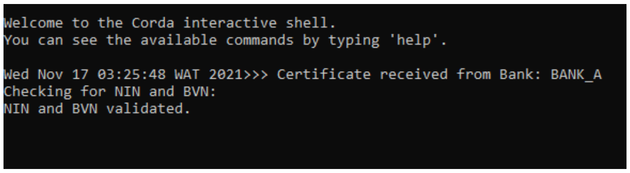


```
Welcome to the Corda interactive shell.
You can see the available commands by typing 'help'.

Wed Nov 17 03:12:29 WAT 2021>>> start TransferInitiator name: Ojerinde, acco
untNumber: 0038221829, recipientNumber: 2177181166, amount: 4000000, BANK_B:
 "O=BANK_B,L=Lagos,C=NG", BVN: 28391038252, NIN: 283958293029
Transaction is initiated by BANK_A!
Recipient number is confirmed
Starting
Checking for NIN and BVN:
NIN and BVN validated.
Checking for NIN and BVN:
NIN and BVN validated.
Broadcasting transaction to participants
Done
Flow completed with result: SignedTransaction(id=9F8579FE91459421A739067CBFF
2464BAA055FB3688375730856712036O5C538)

Wed Nov 17 03:14:14 WAT 2021>>>
```

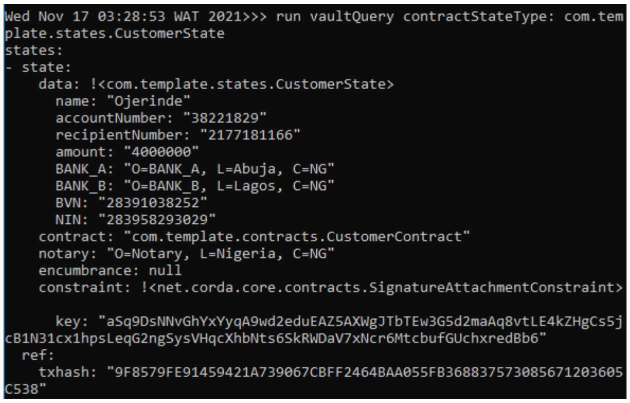
**Figure 2: Initiating a transaction flow**



```
Welcome to the Corda interactive shell.
You can see the available commands by typing 'help'.

Wed Nov 17 03:25:48 WAT 2021>>> Certificate received from Bank: BANK_A
Checking for NIN and BVN:
NIN and BVN validated.
```

**Figure 3: Transaction reception**



```
Wed Nov 17 03:28:53 WAT 2021>>> run vaultQuery contractStateType: com.tem
plate.states.CustomerState
states:
- state:
    data: !<com.template.states.CustomerState>
      name: "Ojerinde"
      accountNumber: "38221829"
      recipientNumber: "2177181166"
      amount: "4000000"
      BANK_A: "O=BANK_A, L=Abuja, C=NG"
      BANK_B: "O=BANK_B, L=Lagos, C=NG"
      BVN: "28391038252"
      NIN: "283958293029"
    contract: "com.template.contracts.CustomerContract"
    notary: "O=Notary, L=Nigeria, C=NG"
    encumbrance: null
    constraint: !<net.corda.core.contracts.SignatureAttachmentConstraint>

      key: "aSq9DsNNvGhYxYyqA9wd2eduEAZ5AXWgJTbTEw3G5d2maAq8vtLE4kZHgCs5j
cB1N31cx1hpsLeqG2ngSysVHqcXhbNts6SkRWDaV7xNcr6MtcbufGUchxredBb6"
  ref:
    txhash: "9F8579FE91459421A739067CBFF2464BAA055FB368837573085671203605
C538"
```

**Figure 4: vaultQuery of the distributed ledger**

Node BANK_B is updated in real-time with the output in its console shown in Figure 3

On running vaultQuery command to check the state of the ledger, the output shown in Figure 4. For each transaction, Corda generates a unique key and transaction hash that can be used to trace any transaction on the ledger.

If another node is added to the network, BANK_C for example, if BANK_C queries the ledger using the vaultQuery command, it will be unable to see those transactions between BANK_A and BANK_B since it is not actively involved.

## 5 CONCLUSION

Banks and FinTech form the major players of a country's finance. Individuals, groups, organizations, and even the government rely on the seamless operations of banks to meet their transactional needs. Conventionally, various banks and financial institutions maintain incoherent ledgers that are synchronized by a clearinghouse from time to time. This approach to transaction management opens a window for security flaws, drags in processing transactions, and high risks of non-atomicity in transactions. The implementation of blockchain in the clearinghouse for banking transactions has proven swift, secured, and instant settlement of payment between financial houses is obtainable.

## ACKNOWLEDGMENTS

This paper is supported by the Royal Academy of Engineering UK Grant under the Higher Education Partnership in Sub-Sahara Africa (HEP-SSA) Programme with project ID HEPSSA1921 3 88

## REFERENCES

[1] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, Dec. 2018, doi: 10.1186/s40561-017-0050-x.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: www.bitcoin.org

[3] F. Huibers, "Distributed Ledger Technology and the Future of Money and Banking: Banking is Necessary, Banks Are Not. Bill Gates 1994," *Accounting, Economics and Law: A Convivium*, 2021, doi: 10.1515/ael-2019-0095.

[4] K. Zhang and H.-A. Jacobsen, "Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains (Technical Report)," 2017.

[5] T. M. Damico, "A Brief History of Cryptography," 2009. [Online]. Available: www.inquiriesjournal.com/print?id=1698http://www.inquiriesjournal.com/a?id=1698

[6] W. Diffie and M. E. Hellman, "New Directions in Cryptography Invited Paper."

[7] O. Konashevych and M. Poblet, "Is Blockchain Hashing an Effective Method for Electronic Governance?"

[8] K. Julia, "Financial Technology – Fintech," Aug. 27, 2020. https://www.investopedia.com/terms/f/fintech.asp (accessed Nov. 18, 2021).

[9] M. Hochstein, "FinTech (the word, that is) Evolves," 2015.

[10] D. Arner, J. Barberis, R. Buckley, U. Law, D. W. Arner, and R. P. Buckley, "THE EVOLUTION OF FINTECH: A NEW POST-CRISIS PARADIGM?"

[11] W. (Derek) Du, S. L. Pan, D. E. Leidner, and W. Ying, "Affordances, experimentation and actualization of FinTech: A blockchain implementation study," *The Journal of Strategic Information Systems*, vol. 28, no. 1, pp. 50–65, Mar. 2019, doi: 10.1016/J.JSIS.2018.10.002.

[12] F. Zabala Aguayo and B. Ślusarczyk, "Risks of banking services' digitalization: The practice of diversification and sustainable development goals," *Sustainability (Switzerland)*, vol. 12, no. 10, May 2020, doi: 10.3390/SU12104040.

[13] R. Ramanathan, U. Ramanathan, and Y. Bentley, "The debate on flexibility of environmental regulations, innovation capabilities and financial performance – A novel use of DEA," *Omega*, vol. 75, pp. 131–138, Mar. 2018, doi: 10.1016/J.OMEGA.2017.02.006.

[14] L. William Cong *et al.*, "Blockchain Disruption and Smart Contracts *," 2017.

[15] N. Szabo, "Smart Contracts," 1994. http://www.fon.hum.5uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed Nov. 18, 2021).

[16] U. Agrawal, I. Koshy, and P. P. Churi, "A Role of Blockchain in IoT and Financial Applications," Mar. 2019. doi: 10.1109/ViTECoN.2019.8899446.