Central Bank Digital Currencies, Internet of Things, and Islamic Finance: Blockchain Prospects and Challenges

Al-Ansari, Khalid Ahmed and Aysan, Ahmet Faruk

Hamad Bin Khalifa University

19 April 2022

Central Bank Digital Currencies, Internet of Things, and Islamic Finance: Blockchain Prospects and Challenges

Abstract

This paper introduces the need for blockchain technology integration for Islamic financial institutions. The paper presents three main applications of blockchain technology. It explains how such technology can be used in the banking and financial sectors by providing examples for each application. Given its relevancy, the paper expands on Central Bank Digital Currencies (CBDCs) as one of the blockchain applications. The paper then discusses salient points on how the banking sector would be affected by what is described as the future of money. Subsequently, an analysis of the use of blockchain in financial services and, in particular, the use for Islamic financial services is provided by examining examples of past successful implementations. The paper then introduces the Internet of Things (IoT) and illustrates the possible technology implementation in financial institutions. The inherent security weakness of IoT is summarized with the potential elimination of that weakness if combined with blockchain (BIoT). The paper concludes by providing a handful of suggestions and recommendations on the urgency of considering CBDCs for future daily operations, integrating Distributed Ledger technology, and using BIoT to safeguard the financial and clients' transaction records.

Keywords: Blockchain, CBDCs, Internet of Things, IoT

JEL Codes: G23, F30, L17, O31

Ahmet Faruk Aysan

Hamad Bin Khalifa University,

Professor & Program Coordinator Ph.D. in Islamic Finance and Economy

College of Islamic Studies, Qatar Foundation

aaysan@hbku.edu.qa

orcid.org/0000-0001-7363-0116

Khalid Ahmed Al-Ansari

Hamad Bin Khalifa University,

College of Islamic Studies, Qatar Foundation,

BSc, MBA, LLM, and Doctor of Law

khaalansari@hbku.edu.qa

orcid.org/0000-0003-2483-6972

Central Bank Digital Currencies, Internet of Things, and Islamic Finance: Blockchain Prospects and Challenges

I. Introduction

Blockchain technology is here and has been in existence for more than a decade. Slowly but surely, innovations using this technology are springing in different fields that touch our lives to make them more accessible and comfortable. We saw that several banks have mobile applications that enabled their customers to access the bank's services without physically visiting any branches. These innovations in the blockchain technology impacting Financial Technology, known as FinTech, are being developed to make the financial institutes more cost-efficient and give better services leading to more satisfied customers.

This paper addresses different technologies operating hand in hand with blockchain technology as part of the blockchain ecosystem. In particular, this paper explores those technologies related to or could be used in the financial sector to increase efficiency, lower operational costs, and provide more transparencies to combat financial crimes.

The rest of the paper is organized as follows. Section II introduces blockchain, its types, and areas of operations. Section III presents general applications of blockchain in the financial sector, such as cryptocurrencies; and smart contracts. A particular focus is lent to Central Bank Digital Currencies (CBDCs), their advantages, and their impact. This section also presents examples of issued CBDCs. Section IV investigates blockchain applications in Islamic financial services and lists a few successful examples. Section V focuses on the use of distributed ledger technology (DLT) in governance and introduces decentralized autonomous organizations (DAOs) and Decentralized Finance (DeFi). Section VI introduces the Internet of Things (IoT) and gives examples of its present and potential use in financial institutions. Section VII analyzes the IoT weakness and the possible technical solution to address that weakness by combining it with blockchain (BIoT). The final section concludes with the recommendations of the authors.

II. Blockchain: Myth or Reality

Ledgers have been at the heart of economic transactions with the purpose of recording contracts, payments, buy-sell deals, or moving assets or property (Majaski, 2021). A centralized ledger is more prone to cyber-attacks and fraud as it has a single point of failure (Majaski, 2021). A distributed ledger stands in contrast to a centralized ledger, which is the type of ledger that most companies use (Majaski, 2021). Blockchain is a distributed ledger type that has been used by the famous cryptocurrency called bitcoin.

Many definitions for the blockchain exist with different explanations of how it works from different perspectives. The definition that the authors find most encompassing is Gartner's definition (Gartner, 2022), which defines it as:

> "*A blockchain is an expanding list of cryptographically signed, irrevocable transactional records shared by all participants in a network. Each record contains a timestamp and reference links to previous transactions. With this information, anyone with access rights can trace back a transactional event belonging to any participant at any*

point in its history. A blockchain is one architectural design of the broader concept of distributed ledgers. "

The primary advantage of blockchain is its ability to resolve trust issues without a central third party. Therefore, blockchain technology has the potential to reinstitute trust by facilitating the protection of data, simplification of service delivery, clarification of outcome measures, and accountability (Aysan, Bergigui, and Disli, 2021).

2.1 Types of Blockchain

The blockchain is classified based on who can read or write back on the chain according to the assigned authority, that is, whether it is permissioned or permissionless (or public, i.e., where permission is not required) to connect to the chain (Alam, Gupta, and Zameni, 2019). While there is a split in the literature on whether there are two types of three types, the authors of this paper argue that there are four types for clarity with variants of the original two (i.e., public and private).

(1) **Public blockchain**: the general characteristic of this type is that it is open and transparent for all participants to participate in reading, writing, and auditing the blocks (Alam et al., 2019). An example of this type is the blockchain used for cryptocurrencies such as Bitcoin and Ether (Alam et al., 2019).

(2) **Private blockchain**: the general characteristic of this type is that it is not open to all and is owned by a single organization, which has the write permissions restricted to itself due to data sensitivity. The reading of the block, though, could be accessible to the public (Alam et al., 2019). An example of this type is database management and auditing, which is required by a single conglomerate to consolidate the internal data for internal purposes where public access is not required for it (Alam et al., 2019). Examples of this type are blockchains used for voting, supply chain management, digital identity, and asset ownership (Types of Blockchains, 2018)

(3) **Hybrid blockchain**: this type contains the best part of both public and private blockchain, and the architecture is entirely customizable (Geroni, 2021). The hybrid blockchain members can decide who can participate in the blockchain or which transactions are made public (Geroni, 2021). Examples of this type are the blockchain used in banking, supply chain, or government blockchain (Geroni, 2021).

(4) **Consortium blockchain:** this type is owned and operated by a group of individuals or institutions where only the consortium members will have access to add, view, and audit the blocks (Alam et al., 2019). An example of this type is the Ripple network.

It is noteworthy to mention that not all private blockchains are necessarily permissioned, as an organization, for instance, can deploy a private blockchain based on Ethereum, which is a permissionless type (Fernández-Caramés and Fraga-Lamas 2018). Examples of permissioned blockchains are the ones used by Hyperledger-Fabric or Ripple (Fernández et al., 2018).

2.2 How does it work?

The blocks in blockchain store information of all transactions that are all cryptographically interrelated in chronological order, forming, therefore, the form of a chain; hence its name "blockchain" (Chong, 2021). The records on a blockchain block can be any type of information, and blocks are formed by bundling records (Aysan and Bergigui, 2021). Chains are made by linking blocks together (Aysan and Bergigui, 2021). When a blockchain-based transaction occurs, two operational levels must be considered, the first is the transaction itself, and the second is the decentralized validation of that transaction (Chong, 2021). Once both the user and the transaction have been verified by the nodes, the transaction is combined with other transactions in a block of the ledger (PricewaterhouseCoopers, 2022). Once this block is filled with verified information/transactions, it will be added to the existing blockchain. In this stage, the information/transactions become permanent and not possible to alter (PricewaterhouseCoopers, 2022). This step marks the point of completion of the transaction. The whole process is illustrated in the infographic below in Figure 1.

2.3 Myth or reality?

Until March 2021, there were 506 peer-reviewed journal articles written in the English language by 1278 authors distributed across 79 countries, specifically on finance, economics, and social sciences subject areas regarding the utilization of blockchain (Al-Ansari and Aysan, 2021). The above finding is primary evidence that blockchain is a ubiquitous reality, impacting Islamic finance (Unal and Aysa,n 2021). It is essential to mention that this new reality is forecasted to disrupt the banking sector's normal operations (if it has not already done so). Depending on how the banking sector regards this technology, blockchain can be either an opportunity or a threat. In this paper, the authors mainly treat the blockchain as an opportunity for the financial sector.

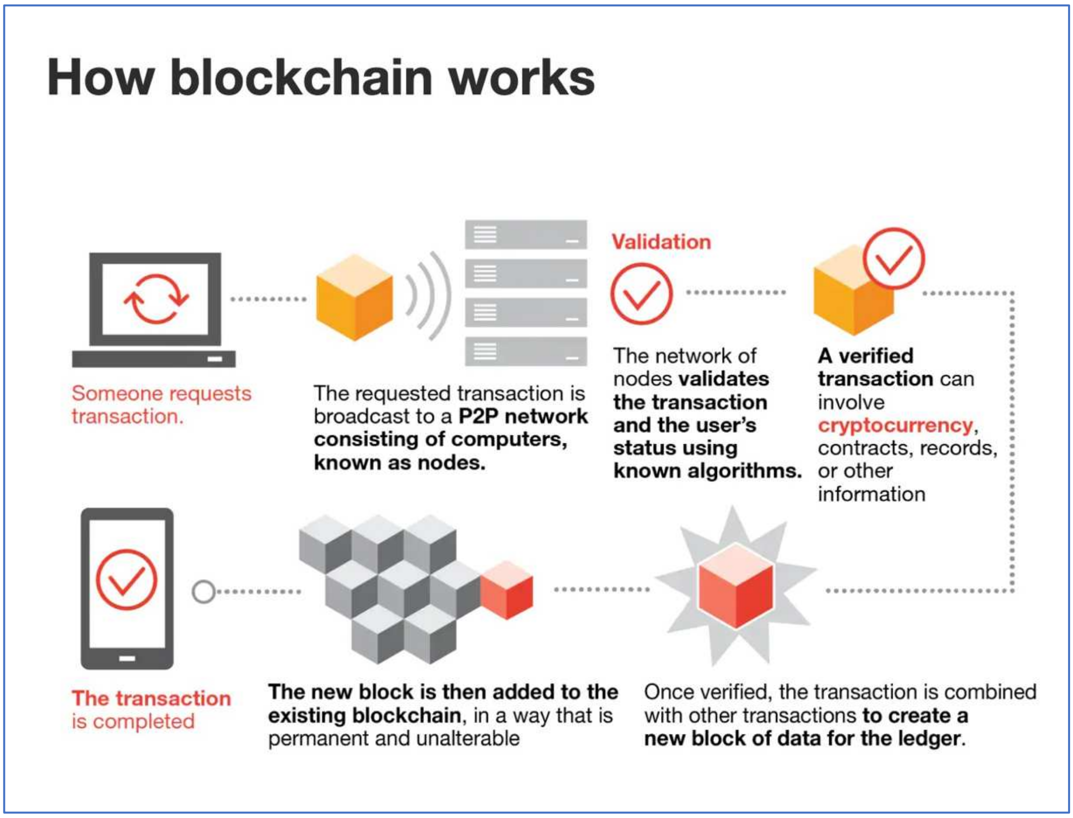


Figure 1. How blockchain works (Source: PwC, 2022)

III. Applications of the blockchain technology (Cryptocurrencies – Smart Contracts – and Central Bank Digital Currency)

Blockchain technology establishes trust and harmony in any given direct communication between two parties without the involvement of a third party. Therefore, using this technology, participants can confirm transactions without the intervention of a central clearing authority (Ahamad et al., 2021). Blockchain technology has various applications. In this paper, the authors will briefly introduce the first two. As for the third application, the authors will expand on it due to its importance.

3.1 Cryptocurrencies

Cryptocurrency, also known as digital currency, virtual currency, or crypto assets, refers to digital entries in a distributed ledger (i.e., blockchain) maintained by a network of computers (nodes) where the record of all transactions is identically distributed on all the peer nodes (Kulkarni et al., 2019). Cryptocurrencies are not issued by central authorities; therefore, their value mostly comes from the scale of participation within the market (Aysan, Demirtaş, and Saraç, 2021).

As of February 3rd, 2022, there were nearly over 10,000 currencies, a severe increase from just a handful of digital coins in 2013 (de Best, 2022). According to Statistica, it is believed that the top 20 cryptocurrencies make up nearly 90 percent of the total market (de Best, 2022). Examples of cryptocurrencies include, but are not limited to: Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH), Bitcoin Cash (BCH), Cardano (ADA), Stellar (XLM), Dogecoin (DOGE), and Tether (USDT). All cryptocurrencies are held in an electronic wallet (e-wallet), and it must be signed by a private key for the cryptocurrency wallet holder to initiate any transfer (Alam et al., 2019).

Stablecoins

A Stablecoin is a type of cryptocurrency that derives its value from some underlying external asset, like the USA dollar or the price of gold, which is different from cryptocurrencies like Bitcoin or Ethereum that are tied to primarily being "mined" by computers (Hou, 2021). Therefore, while Bitcoin and other cryptocurrencies are volatile, Stablecoins are popular among investors and companies because of their supposed price stability (Hou, 2021). They are also attractive to beginners because many exchanges (between Stablecoins and the USA dollars) do not charge extra trading fees, unlike other cryptocurrencies, such as Bitcoin, where there is a trading fee charge between USA dollars and those cryptocurrencies (Hou, 2021). Some of the Stablecoins are Tether (USDT), Dia (DAI), Binance USD (BUSD), TrueUSD (TUSD), USD Coin (USDC), Terra USD (UST), and Digix Gold Token (DGX).

3.2 Smart Contract

Unlike conventional contracts established through speech, written words, or actions, smart contracts are algorithmic, self-executing, and self-enforcing computer programs (Lauslahti, Mattila, and Seppala, 2017). Smart contracts are agreements between two parties recorded as computer codes on the blockchain, which are automatically activated when the conditions agreed upon in the agreements are met (Aysan and Bergigui, 2021). Smart contracts can allow people from around the globe to transact with one another without needing an intermediary, thus reducing the costs of intermediaries and brokers since there is no third party involved.

Moreover, smart contracts can reduce administration, thus saving time and offering complete autonomy (CoreLedger, 2019). Since everything is backed up onto the blockchain, smart contracts are considered entirely safe against loss of data (CoreLedger, 2019). In its simplest form, a smart contract is a machine-readable program written in a code that will execute itself once a set of pre-determined terms are met (CoreLedger, 2019). It is noteworthy that smart contracts do not need artificial intelligence for them to work, regardless of what their name may suggest, and it is in most cases, smart contracts create a set of rights and obligations and thus become legally binding contracts (Lauslahti, Mattila, and Seppala, 2017).

3.3 Central Bank Digital Currency (CBDC)

A Central Bank Digital Currency (CBDC) is considered by many economists as the future of money. It is the digital form of a country's fiat currency that is also a claim on the central bank, where instead of printing money, the central bank issues electronic coins or accounts that are backed by the full faith and credit of the government (Atlantic Council Geoeconomics Center, 2022). Since a country's central bank issues CBDC, people and businesses can use it for retail payments, much like cash but in digital form (CBDC Whitepaper, 2020). This would mean that CBDCs would also be controlled by that country's central bank, which would be able to know about the details of all of the transactions involving those CBDCs. Given this intervention may introduce an objection from privacy-concerned groups.

A CBDC, which a country's central bank issues, is different from cryptocurrencies in that the latter are privately issued digital currencies (i.e., Bitcoin, Ether), and their value can move up and down very quickly, which is the reason for them being a risky investment (U.K. Central Bank Digital Currency, 2022).

When it comes to popularity and implementation, a 2020 white paper by Ripple on CBDCs, showed that 80% of central banks were actively exploring CBDCs, as shown in Figure 2. Currently, nine countries issued their CBDCs. These countries are The Bahamas, Nigeria, and the seven Eastern Caribbean countries, namely; Saint Kitts & Nevis, Montserrat, Antigua & Barbuda, Dominica, Saint Lucia, Saint Vincent & The Grenadines, and Grenada (Atlantic Council Geoeconomics Center, 2022). Moreover, fifteen countries are in the pilot stage; sixteen countries are in the development stage, while forty are in the research stage (Atlantic Council Geoeconomics Center, 2022), as shown in Figure 3.

To address the research area of cross-border payment using CBDCs, there is an initiative run in partnership with the Bank of International Settlement (BIS), the Hong Kong Monetary Authority, and the Bank of Thailand to create a Multiple CBDC (m-CBDC) Bridge, which aims to develop a proof-of-concept prototype to facilitate real-time cross-border foreign exchange payments on distributed ledger technology (BIS-Press Release, 2021). In February 2021, the central bank of the United Arab Emirates (UAE) and China's central bank joined a digital project for cross-border payment using the CBDCs of the two countries (BIS-Press Release, 2021).

Figure 2. Central banks around the world and CBDCs development
(Source: CBDC Whitepaper, 2020)

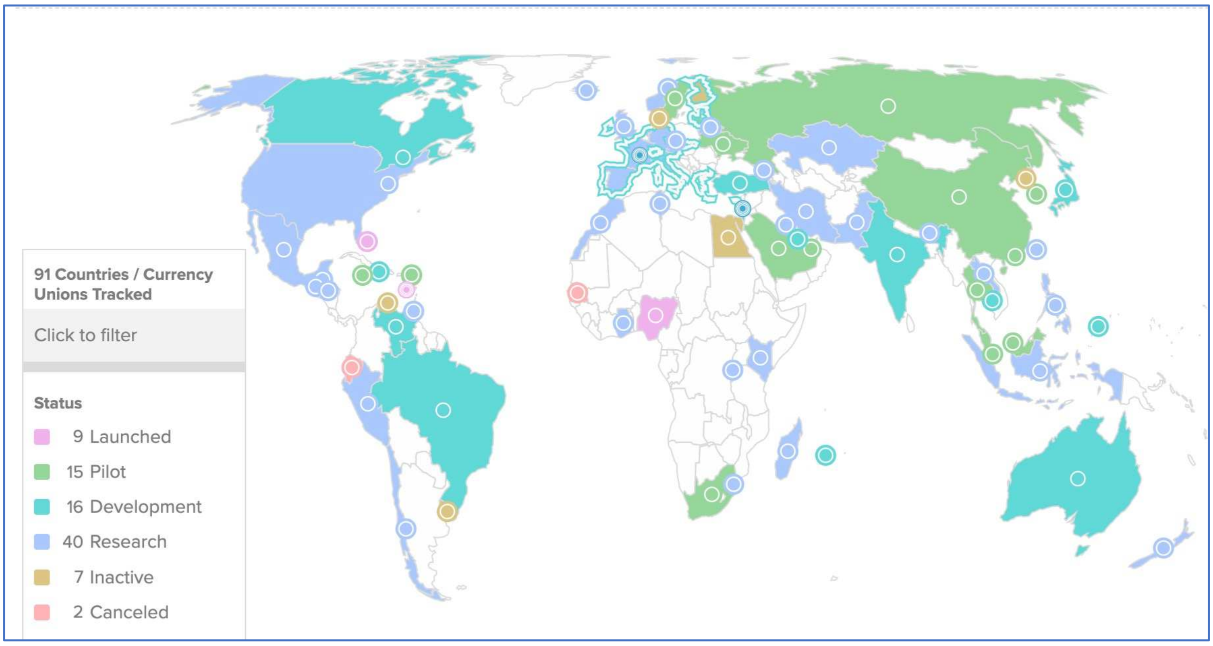


Figure 3. Status of 91 countries and stages of CBDCs
(Source: Atlantic Council Research, Bank of International Settlements, International Monetary Fund, John Kiff Database)

Advantages and drivers of CBDCs

A 2021 report issued by Deloitte has identified four main drivers that have pushed central banks to explore CBDCs, which we view as perceived advantages to promote the use of the CBDCs.

a. Supporting digitization of economies: CBDCs could help maintain and streamline central banks' function of providing legal tender and ensuring continued access in a purely digital economy, as well as offering access to digital payments at minimum or zero cost via a new general-purpose electronic payment medium.

b. Streamlining current payment systems: CBDCs could improve payment contestability by reducing operational costs and risks associated with managing physical currency. It would help improve the efficiency of payment systems, both at point of sale and peer-to-peer transactions. It would finally help improve interbank payments through faster settlements and open or extend settlement hours.

c. Enhancing monetary and fiscal policy: CBDCs could be used to improve monetary policy for central banks, simplifying the distribution of government benefits to individuals and improving control over transactions for tax controls. They could also enhance financial stability by managing liquidity squeezes and offering public alternatives to private digital currencies.

d. Improving financial inclusion: CBDCs could provide a tool to improve the competitiveness of local currency as a means of payment in regions that are attempting to reduce U.S. dollar dependency.

CBDCs Impact

CBDCs are expected to have various impacts on the financial sector of the country where they are deployed (Deloitte, 2021). Additionally, once a central bank introduces CBDC in a country, it will add significant complexity for local commercial banks and may imply a drastic change across the banking sector organization to keep up with the need to innovate compatible products (Deloitte, 2021).

It is anticipated that CBDCs would reduce specific negative characteristics of the fiat currency features, such as anonymity and the lack of an audit trail, which make fiat currency more attractive for illicit transactions, including but not limited to; tax evasion, money laundering, and terrorist financing (Soderberg et al., 2022).

Moreover, CBDCs might be potentially a policy tool to offer digital forms of payments that are cheaper to operate in countries where fiat currency and check use are high, which would elevate the operational costs (Soderberg et al., 2022).

The literature discusses the potential risk that the introduction of CBDC could create, including crowding out banks and facilitating bank runs (Kumhof and Noone 2018, Juks 2018, and Bindseil 2019, as cited by Soderberg et al., 2022). In addition, the literature discusses different ways to mitigate these risks by either restricting CBDC balances or taxing the use or balances of CBDC above a threshold (Bindseil 2020, as cited by Soderberg et al., 2022). All CBDCs currently circulating as official currencies are designed with two restrictions limiting the competitiveness of CBDC versus bank deposits (Soderberg et al., 2022). Those are restrictions on the remuneration of CBDC and quantitative restrictions on holdings and transactions of CBDC (Soderberg et al., 2022).

Examples of CBDCs

In the Bahamas, the *Sand Dollar*—the local CBDC—has been in circulation for more than a year, while in China, the digital renminbi (called e-CNY) continues to progress with more than a hundred million individual users and billions of yuan in transactions (Georgieva, 2022). The most recent and first CBDC in Africa is the launch of e-Naira by the Central Bank of Nigeria in October 2021, where 500 million e-Naira (=$1.21 million) had already been minted, which only the bank account holders can access by signing up with Nigeria's BVN bank identity (Atlantic Council Geoeconomics Center 2022).

IV. Applications of blockchain in Islamic Financial Services: Digital Banks, Sukuks, Payment-Remittance, and Smart Contracts

4.1 Blockchain-based Customer Authentication

Security and privacy are top concerns among consumers, regardless of their age. To address such concerns, upgrading the Internet of Things (IoT) technology (as will be detailed in section VI) has enabled banks to adopt blockchain technology for better customer authentication (Intelligence 2022). According to Business Insider Intelligence, given that the identity credential has already been logged, the benefit of using blockchain for identity authentication is that it cannot be changed or altered.

Blockchain can ease the cost of cross-border payments and increase the efficiency of trade finance processes (Intelligence, 2022). Accordingly, financial institutions are investing about $1.7 billion annually in blockchain technology (Intelligence, 2022).

From the market's perspective, it is necessary for the micro and macro levels of the Islamic finance industry to adopt Fintech, specifically blockchain technology, to necessarily grow and remain competitive in the marketplace (Chong, 2021). To remain competitive with conventional banking, Islamic financial institutions may initiate and implement projects in digital banking (Nanaeva, Aysan, and Shirazi 2021), Sukuk on the blockchain, payment-remittance, and smart contracts. An example of each will be given below to give the incentives for Islamic financial institutions to visualize how their operations will be in the near future.

4.2 Digital Banks

One example of a digital Islamic bank is HADA DBank (HDB), whose headquarters are located in London, England. It is the first Islamic digital bank running on blockchain technology to create an ethical and responsible banking ecosystem (Alam, 2019). HDB employs a private blockchain which is stored on every node in the network, and by default, the nodes are all controlled by HDB. Some nodes only store a copy of the blockchain and do not take part in the transaction confirmation process (Alam, 2019). HDB utilizes blockchain technology, which provides unique advantages such as speedy transaction processing, low fees, and robust security. Being available online round the clock, HDB offers a multitude of services to its users, including free e-wallets and accounts, Shariah-compliant financing, and artificial intelligence-based financial advisory (Alam, 2019).

4.3 Sukuks (Islamic Bonds)

One example of smart contracts and Islamic Finance is the recent development of Smart Sukuk, which are Islamic bonds with values tied to real projects, representing only productive economic activities (Chong, 2021). Abu Dhabi's Al Hilal Bank in the UAE (AHB) concluded in November 2018 World's first blockchain-enabled Sukuk transaction in a deal worth $1 million sold to a private investor via a Swiss-based FinTech company called Jibrel Network (Alam, 2019). The Al Hilal Bank Smart Sukuk transaction was executed to leverage the blockchain for the secondary market Sukuk deal (Chong, 2021).

4.4 Payment & Remittance

Alam (2019) explained that using cryptocurrency for remittance is becoming a competitive option compared to fiat-to-fiat money transfer. He explained that the remittance backed by blockchain technology instead of the traditional model based on a centralized network is called a ReBittance. He further explained that:

a. blockchain makes the remittance transaction cheaper by cutting out intermediary banking costs, thus enabling the transfer can be completed in minutes;
b. the beneficiary can either retain the digital currency or convert it into fiat currency.

Nowadays, clients expect instant, mobile-friendly, and multi-currency payment options linked with cross-border payments. Using blockchain will facilitate these operations if the financial institutions undertake the necessary research and development steps to implement the available technology. The Islamic financial institutions can use the available technology in distributed ledger technology and cryptocurrencies such as stablecoins—wherever it is legally permitted—to make the technology work (see Dosso and Aysan 2022).

4.5 Smart Contracts

As explained in section 3.2, smart contracts are digital legal contracts that are self-executing when the pre-set conditions have been met. These contracts are legally binding to all parties involved. Through smart contracts, Islamic commerce and finance receive inspiration for developing intelligent agents to help execute and ensure Shari'ah compliance, mainly through basic conceptual innovations with blockchain-smart contract applications (Chong, 2021). The example given earlier about Al Hilal Bank Smart Sukuk is a perfect example of combining a smart contract with Islamic finance. A second example is the Smart Sukuk issuance by Blossom Finance, a microfinancing start-up that provides what is perceived as an innovative Islamic FinTech platform through Smart Sukuk operating on the Ethereum blockchain protocol encrypts all rules and Shari'ah codes automatically into the smart contracts (Chong 2021). Although Chong (2021) had given a detailed description of the process of Blossom Finance Smart Sukuk, one of the shortcomings of this process is its lack of applicability in countries where the local laws do not allow dealing with cryptocurrencies. However, from the literature, Chong (2021) has succinctly identified two challenges based on the process of the smart Sukuk that she presented. The first challenge she identified was the extent to which Shari'ah principles can be computationally encoded into a smart contract code. The second challenge was related to the algorithmic protocol used to validate smart contracts when it comes to Smart Sukuk.

The following are two examples of using blockchain in trade. The first example is the Halal certification industry, which, given its vulnerability to fraud, is experimenting with blockchain-backed solutions (Aysan and Bergigui, 2021). K.T., a telecom company, and partners are working to establish a Halal Certification Platform that will issue certificates on the blockchain while allowing customers to use Q.R. codes on their products to verify their status (Wood, 2019, as cited in Aysan and Bergigui, 2021). The second example is OneAgrix, a trading marketplace that provides a business-to-business (B2B) platform using a blockchain ledger to trace halal ingredients and authenticate halal certificates (Whitehead, 2019).

V. DLT For Governance / DAOs / DeFi

Distributed ledger technology (DLT) refers to the protocols and supporting infrastructure that allows computers in different locations to propose and validate transactions and update records in a synchronized way across a network (Bech and Garratt, 2017). The idea of a distributed ledger, which is a common record of activity that is shared across computers in different locations, is not new (Bech and Garratt, 2017). However, in a traditional distributed database, a system administrator typically performs the key functions necessary to maintain consistency across the multiple copies of the ledger (Bech and Garratt, 2017).

5.1 DLT for Governance

Using DLT for finance would mean that ledgers have two main characteristics. First, those ledgers would be distributed on all the nodes on the blockchain chosen, so a single point of failure will not happen if the local server has the ledger's information crash. Many nodes have the same information that was on the crashed server. The second characteristic of that ledger is immutable, so the transactional data on the ledger cannot be changed or modified. In the case of Islamic finance, such tools as Mudarabah (trust financing) or Murabaha (cost plus trade financing) need the use of an agent, which introduces two possible problems, namely, agency cost and moral hazard part of the transaction cost. With the information of Mudarabah or Murabaha placed on DLT, the second character would ensure the reduction of agency cost and moral hazard.

5.2 Decentralized Autonomous Organizations (DAOs)

The DAO is an organization designed to be automated and decentralized (Reiff 2021). It acted as a venture capital fund, based on open-source code and without a typical management structure or board of directors (Reiff 2021). To be fully decentralized, the DAO was unaffiliated with any particular nation-state, though it made use of the Ethereum network (Reiff 2021).

The developers of the DAO believed they could eliminate human error or manipulation of investor funds by placing decision-making power into the hands of an automated system and a crowdsourced process (Reiff 2021). Fueled by Ether (ETH), the DAO was designed to allow investors to anonymously send money from anywhere in the world (Reiff 2021). The DAO would then provide those owners with tokens, allowing them voting rights on possible projects (Reiff 2021). For example, the DAO launched in late April 2016 a crowd-sale of tokens that raised more than $150 million in funds, which was considered—at the time—the largest crowdfunding fundraising campaign of all time (Reiff 2021).

5.3 Decentralized Finance (DeFi)

Decentralized finance (DeFi) is a type of alternative finance that uses public blockchain technology to conduct various financial transactions (Kumar 2022). With DeFi, you can do most of the things that banks support, for instance: earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, and more. Unlike a regular bank, though, DeFi is faster and does not require paperwork or a third party (Coinbase 2022).

As with crypto generally, DeFi is global, peer-to-peer (meaning directly between two people, not routed through a centralized system), pseudonymous (i.e., you do not need to provide your name, email address, or any personal information), and open to all (Coinbase 2022). Common usage incorporates one or more elements of (i) decentralization; (ii) distributed ledger technology and blockchain; (iii) smart contracts; (iv) disintermediation; and (v) open banking (Zetzsche, Arner, and Buckley 2020).

VI. The Internet of Things (IoT)

6.1 Background

In today's technological era, the Internet of Things (IoT) is an ever-increasingly popular technology that has evolved with ubiquitous computing (Ahamad et al., 2021). Smart homes, smart cities, and smart transportation are examples of IoT applications that have improved people's lives (Ahamad et al., 2021). The Global Standards Initiative in 2013 analyzed the possibility of integrating information sharing among several functions and activities and came up with the concept of the IoT, with a clarification that "thing" is an object of either the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks (Kiran 2019).

In short, the IoT refers to the rapidly growing network of connected objects that can collect and exchange data in real-time using embedded sensors, such as thermostats, cars, lights, refrigerators, and more appliances that can be connected to the IoT (Meola 2022). It is estimated that by 2025, there will be 64 billion IoT devices worldwide. McKinsey & Company (McKinsey), a management consulting company, reports that 127 new tools worldwide are attached to the web each second (Adams 2020).

Using human language as an analogy, electronic devices (computers, smartphones, alarm systems, game consoles, T.V.s, tablets, cameras, etc.) can all speak to each other, too (Kiran 2019). They speak a different language—their own computer language (i.e., IoT), which enables objects to be sensed or controlled remotely across existing network infrastructure and creates opportunities for more direct integration of the physical world into computer-based systems (Kiran 2019). Currently, most IoT solutions rely on the centralized server-client paradigm, connecting to cloud servers through the Internet (Fernández-Caramés and Fraga-Lamas 2018).

The IoT then allows virtual and physical items to link and communicate with one another, resulting in the creation of new digitized services (Ahamad et al., 2021). However, this data is not encrypted and does not provide privacy (Ahamad et al., 2021). IoT devices are frequently vulnerable to security flaws, making them a prime target for Distributed Denial of Service (DDoS) attacks (Ahamad et al., 2021). In this regard, blockchain technology might give massive benefits because it can quickly secure the anonymity of the obtained data (Ahamad et al., 2021). Blockchain can assist in solving most of the security vulnerabilities and traceability concerns in financial transactions by keeping track of how devices interact (Ahamad et al., 2021).

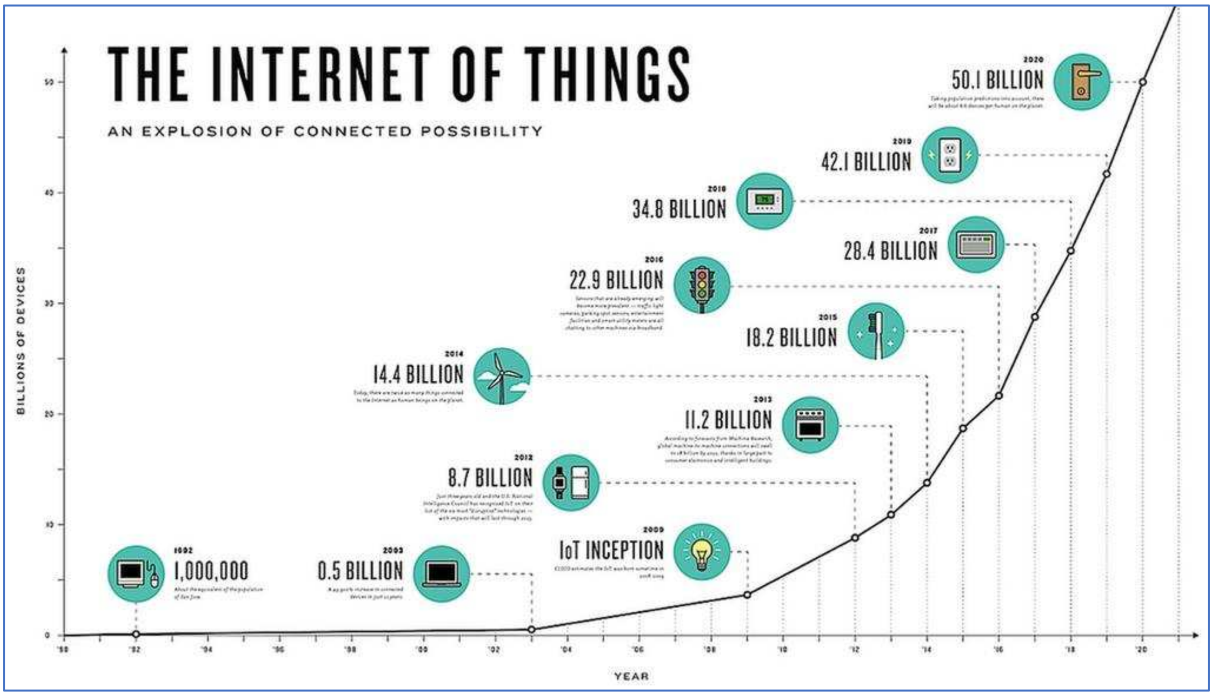


Figure 4. An explosion of Connected Possibility of IoT (Source: IoT Basics, 2015)

Insider Intelligence forecasts 3.74 billion IoT mobile connections worldwide by 2025 and more than 64 billion IoT devices installed by 2026 (Meola 2022).

6.2 Current Utilization of IoT

Retail banking has been using an early prototype of an IoT device for decades: the automated teller machine (ATM), which has been one of the top IoT devices that make banks far more efficient by allowing real-time transactions rather than waiting to see a teller at a brick-and-mortar bank (Intelligence 2022).

Banks operating model improvements have soared with the introduction of IoT in retail banking (Intelligence 2022). For example, in Q3 2019, Chase Manhattan Bank announced that it improved on digital account opening, cutting down the time it takes to just 3-5 minutes on average (Intelligence 2022).

Despite such widespread use of IoT, most individuals might not be aware of such omnipresence of this technology. These days, access to mobile devices (e.g., laptops, tablets, or smartphones) is secured by scanning the user's finger via a fingerprint scanner installed on those devices. Access is also given via facial recognition using the front camera on mobile devices. This boosts security and access to only those who own the devices. Not far from this, the first example of the current use of IoT is the use of facial recognition and fingerprint scan in banking applications on mobile phones to allow access of the bank's customers to various digital services offered by the bank, such as funds transfer, utility bills settlement, as well as access to finance. By using the sensors of the authentication protocol made by the phone's camera to recognize the face of the owner or the fingerprint scanner to identify the scan of the owner's finger, whose credentials had already been registered digitally on the mobile device, access authentication is triggered to grant access to his/her bank account and associated services. Most IoT protocols are created by using the sensors in the smartphone. The authentication of the digital credentials from the bankside utilizing the internet makes this process fast and within less than a minute in most banking services.

Another example is what is called Smartwatch Banking. By using smartwatches to give information such as currencies rate, account transactions, credit card balances, and access to other banking services, the identity of the bank's customer can be authenticated in seconds ("Time Is Money-FINANTEQ" 2021). Moreover, IoT wearables are replacing traditional credit cards in making wireless payments and cash withdrawals (Adams 2020).

A final example is Banking via smart speakers, which provide customers with the convenience of issuing voice instructions rather than having to physically look at a mobile device (Intelligence 2022). In 2019, National Westminster Bank (NatWest) piloted a voice banking feature with Google Assistant (Intelligence 2022). The feature was compatible with the Google Home smart speaker and allowed customers to inquire about account balances' latest and pending transactions (Intelligence 2022).

6.3 Potential Use of IoT in Financial Institutions

The potential use of IoT in financial institutions would impact customer service experience and improve the security of the transactions. We list below the possible utilization of IoT.

a. **Prompt Customer Assistance:** combining industrial IoT with Artificial Intelligence (A.I.) for financial institutions to offer immediate support to customers, using a smartphone application that will notify account supervisors when a consumer arrives at their branch, to respond promptly while saving customers time (Adams 2020).

b. **Self-Checkout Services:** IoT can use smart gadgets to provide wireless self-checkout services on numerous domains, and the prime example of applying this concept is Amazon.com and all of its self-checkout stores (Adams 2020).

c. **Authentication and Safety:** IoT wearables are used to boost safety and security in the workplace, and a good example is the Nymi smart wristband, which utilizes an individual's heart rate for biometric authentication (Adams 2020).

d. **Lowering Purchases Fees:** IoT can directly link the retailer with a bank; therefore, there is no requirement to utilize credit cards such as Visa or MasterCard; both are understood for high handling charges varying from 1.9% to 2.5% per deal (Adams 2020).

The authors acknowledge that the above potential use would constitute investments that would translate to more efficient use of employees' time and save time for the customers who might change their bank to utilize such services. According to a Microsoft report, 96% of consumers worldwide suggest that client service is a necessary factor in their brand name selection (Adams 2020).

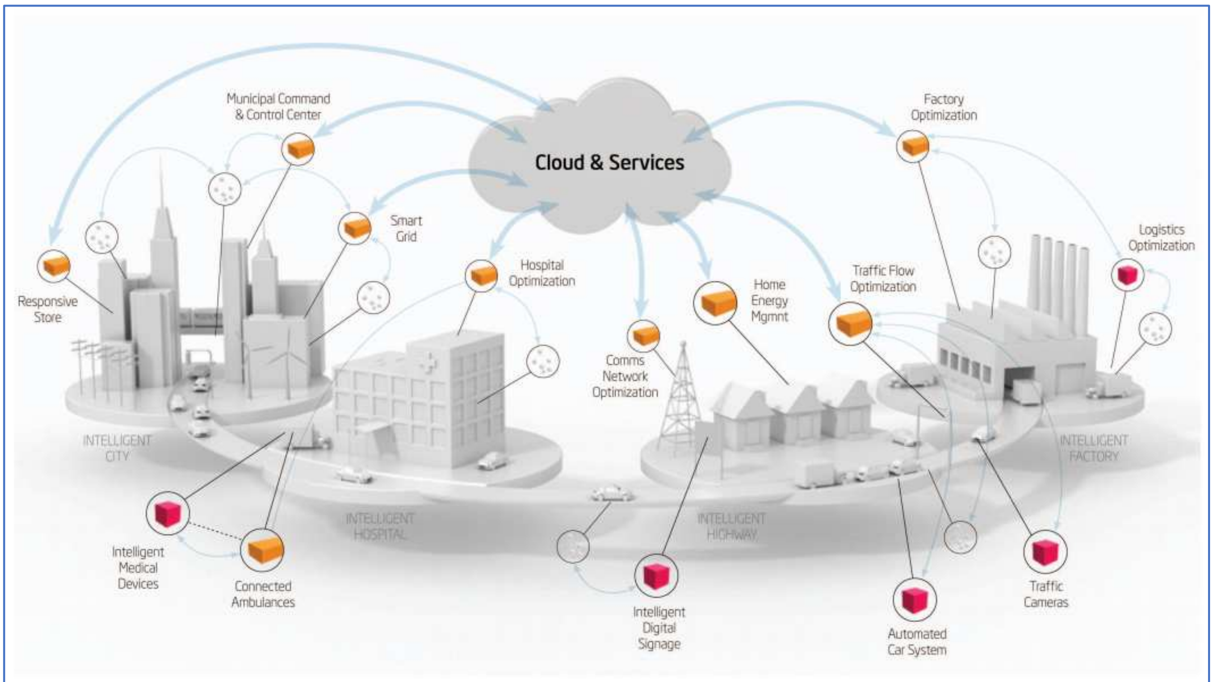
VII. Internet of Things (IoT) and the blockchain

As stated earlier that most existing IoT solutions rely on the centralized server-client paradigm, connecting to cloud servers through the internet, which is a possible data privacy leak (see Figure 5). The cloud servers' operators may give access to the cloud servers to certain authorities such as governments, manufacturers, or service providers, allowing them to collect and analyze user data, as it had occurred in the Edward Snowden leak case (Fernández-Caramés and Fraga-Lamas 2018). Snowden was an employee and a contractor of the American Government National Security Agency (NSA), and he blew the whistle on what the NSA was doing on numerous global surveillance programs with the cooperation of telecommunication companies and European governments, collecting metadata from the Internet communications (Landau 2013).

Edward Snowden's case concludes that it is relatively easy to access the cloud servers' contents by forcing the servers' owners to give servers direct access to security agencies and manufacturers of hardware, for example. Subsequently, all the data stored on those servers can be exposed, copied, or mirrored to other sites, compromising data privacy. This is more dangerous in the case of financial institutions as the financial claims can be catastrophic, not to mention the institution's reputation damage.

When it comes to IoT, this technology at this time connects to cloud servers. This represents its weakest link. As discussed earlier, one layer of security can be compromised if the cloud server operator is forced to give access to those servers. This is why future and potential IoT for financial applications should be moved to a real trusted environment other than cloud servers. This move uses the blockchain's characteristics as a real trust environment.

Figure 5. IoT Reliance on centralized servers



(Source: IoT Basics, 2015)

Therefore, the future potential uses of IoT in the blockchain will enhance IoT security, as discussed earlier. IoT with blockchain can bring real trust to captured data as the underlying idea is to give devices, at the time of their creation, an identity that can be validated and verified throughout their lifecycle with blockchain (Cuomo 2020). There is great potential for IoT systems in blockchain technology capabilities that rely on device identity protocols and reputation systems, as each device has its own identity protocol, which will make it easier for it to have its own blockchain public key and send encrypted challenges and response messages to other devices, thereby, ensuring a device remains in control of its identity (Cuomo 2020) In addition, a device with an identity can develop a reputation or history that is tracked by a blockchain (Cuomo 2020).

Blockchain technology can be applied in different areas of IoT utilization (the most relevant are shown in Figure 6) where IoT applications are involved (i.e., BIoT) (Fernández-Caramés and Fraga-Lamas 2018). Applications include sensing, data storage, identity management, timestamping services, smart living applications, intelligent transportation systems, wearables, supply chain management, mobile crowd sensing, cyber law, and security in mission-critical scenarios (Fernández-Caramés and Fraga-Lamas 2018).

Out of the possible applications that can use blockchain in IoT are the Financial Transactions, which can increase the safety of financial transactions and prevent private information leaks or hacks. As a result of this promising feature, it should become the focus of Islamic Financial Institutions to make them more resilient against digital information leaks or hacks.

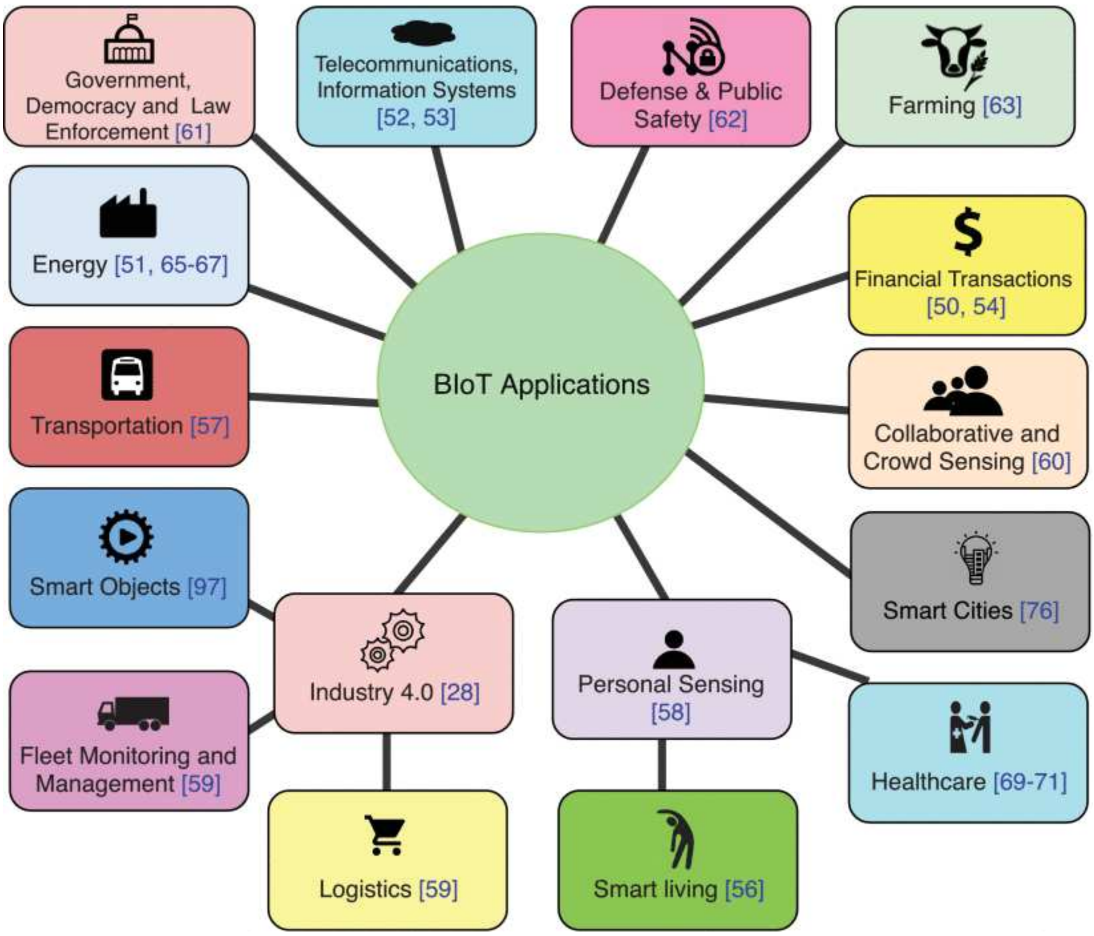


Figure 6. Possible use of blockchain in IoT (BIoT)
(Source: Fernández-Caramés and Fraga-Lamas, 2018)

VIII. Conclusions and Recommendatory Remarks

When it comes to technology, this paper shows that Islamic financial institutions have pioneered digital banking and used smart contracts in issuing smart Sukuks. The technology is getting smarter, and so is the threat of cyberattacks. Therefore, it would be advantageous for the Islamic financial institutions to move to DLT on the blockchain and connect their daily operations with clients' identifications and authentications with the records each institute have on its permissioned (i.e., private) blockchain for speedy identifications.

The CBDCs implementation worldwide has reached nine countries that have launched their digital currencies, while fourteen countries are in the pilot stage in preparation for full launch. The paper showed the drivers of central banks to issue their digital currencies. Additional complexity for commercial banks, reduction of tax evasion, money laundering, and terrorist financing were identified as some of the impact factors of introducing CBDC. The initiative to have real-time international cross-border foreign exchange payments is in the work by BIS, the Hong Kong Monetary Authority, and the Bank of Thailand.

The bulk of the paper was geared toward introducing the internet of things (IoT) and how the concept of connecting something physical with another thing that is virtual was exemplified in the regular AutoTeller Machine (ATM). Other current financial sector's uses of IoT were explained as well as future potential benefits of IoT in the same sector. However, IoT can be used in many other areas, as illustrated and depicted in Figure 5. In addition, with the inherent technology of the IoT relying on servers and clouds, which poses a security weakness, the technology of blockchain came to the rescue when the information would be decrypted on the blockchain such that private information would not be subject to hacking or servers-leak. The case of Edward Snowden was presented to show the vulnerability of stored data (metadata) on cloud-based servers as those servers can be exploited to reach personal and private data.

The Islamic finance tools of Mudarabah or Murabaha generally need the use of agents, which introduce two possible problems: agency cost and moral hazard as part of the transaction cost. With the information of Mudarabah or Murabaha placed on DLT, the immutability of the DLT would ensure the reduction of agency cost, and the transparency of the DLT would reduce—if not eliminate—the moral hazard dilemma. The further use of IoT on the blockchain (BIoT) would help with the authentication process of the customers and agents and allow for faster recognition of the credentials of the parties involved in the Mudarabah or Murabaha. The BIoT would be an effective agent for the customer to stay with the financial institutes.

The paper has two main contributions and further secondary recommendations to boost the competitive edge of Islamic financial institutions. The first main contribution is for the present time. It is the evaluation of one of the available stablecoins -in jurisdictions where it is legally allowed- to be used for real-time payments and remittance. The second main recommendation is for the near future. It is summarized in the actual evaluation of creating an Islamic stablecoin (ISC) as a cryptocurrency, which would have its value based on the available reserve of gold and other more stable assets. This new Islamic stablecoin should have an electronic wallet (same as all other cryptocurrencies) but differs in the interaction with the owner. The difference would be that the private key communicates through BIoT with the owner to double verify the owner's identity before any transaction is broadcasted to the network of nodes to be verified and added to the blockchain. Certainly, there are many potential blockchain applications that Islamic finance and the economy may benefit from. The bottom line is as conventional finance is changing with the recent advancement in technology, Islamic finance institutions and the instruments in Islamic finance cannot stay intact and need to cater to the needs in the market to stay relevant for the customers.

The secondary recommendations to boost the competitiveness of the Islamic financial institutions with the conventional types are as follows:

1. Most central banks are investigating the use of CBDCs. Therefore, financial institutions should be aware that clients will withdraw some of their deposits to buy CBDCs, which offer instant payments. Moreover, financial institutions should seek other alternative means to avoid bank runs and depletion of the clients' deposits.

2. The use of CBDCs for cross-border international payments is coming as the next stage after the rolling out of CBDC. Hence, the financial institutions are encouraged to become part of the multiple CBDCs (m-CBDCs) movement initiatives.

3. Investigate distributed ledger technology (DLT) in the institution's daily financial operations. If that investigation shows positive results and improvement in efficiency and security, plan a phasing program to implement the process.

4. Investment in profitable products using DLT for clients should be on the agenda for Islamic financial institutions to compete with conventional ones.

5. The use of IoT at this time is not fully developed for the financial sector other than mobile banking applications. Innovation of using customers' information to ease the clients' access to their accounts and services should be moved to blockchain IoT (BIoT) to avoid privacy-data leaks.

6. Clients' concerns about their data and future use of that data should become a priority in any financial institution's daily operation. This concern should be addressed transparently to the clients and the financial regulators and in line with the outlines of the General Data Protection Regulation (GDPR) implemented in the European Union countries.

7. Artificial Intelligence and Big Data are exploding in multiple sectors. The financial sector should plan projects to use those technologies to ease the clients'/institutions financial transactions and emphasize the security of the clients' data.

8. Financial institutions should work diligently with the regulators and central banks to prevent payment fraud via innovative solutions anchored in blockchain technology.

References

Adams, Allen. 2020. "Eight Advantages of IoT in Banking." *TechNative* (blog). December 3, 2020. https://technative.io/8-advantages-of-iot-in-banking/.

Ahamad, Shahanawaj, Priti Gupta, Purnendu Bikash Acharjee, K. Padma Kiran, Zarrarahmed Khan, and Mohammed Faez Hasan. 2021. "The Role of Block Chain Technology and Internet of Things (IoT) to Protect Financial Transactions in Crypto Currency Market." *Materials Today: Proceedings*, December. https://doi.org/10.1016/j.matpr.2021.11.405.

Alam, Nafis, Lokesh Gupta, and Abdolhossein Zameni. 2019. "Digitalization and Disruption in the Financial Sector." In *Fintech and Islamic Finance: Digitalization, Development and Disruption*, edited by Nafis Alam, Lokesh Gupta, and Abdolhossein Zameni, 1–9. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-24666-2_1.

Al-Ansari, Khalid Ahmed, and Ahmet Faruk Aysan. 2021. "More than Ten Years of Blockchain Creation: How Did We Use the Technology and Which Direction Is the Research Heading?" SSRN Scholarly Paper ID 3922722. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3922722.

Atlantic Council Geoeconomics Center. 2022. "Central Bank Digital Currency Tracker." *Atlantic Council* (blog). 2022. https://www.atlanticcouncil.org/cbdctracker/.

Aysan, Ahmet Faruk, and Fouad Bergigui. 2021. "Sustainability, Trust, and Blockchain Applications in Islamic Finance and Circular Economy: Best Practices and Fintech Prospects." In *Islamic Finance and Circular Economy*, edited by Syed Nazim Ali and Zul Hakim Jumat, 1st ed., 5:141–48. Gulf Studies. Springer, Singapore. https://www.springerprofessional.de/en/islamic-finance-and-circular-economy/19933126.

Aysan, Ahmet Faruk, Fouad Bergigui, and Mustafa Disli. 2021. "Blockchain-Based Solutions in Achieving SDGs after COVID-19." *Journal of Open Innovation: Technology, Market, and Complexity* 7 (2): 151. https://doi.org/10.3390/joitmc7020151.

Aysan, Ahmet Faruk, Hüseyin Bedir Demirtaş, and Mustafa Saraç. 2021. "The Ascent of Bitcoin: Bibliometric Analysis of Bitcoin Research." *Journal of Risk and Financial Management* 14 (9): 427. https://doi.org/10.3390/jrfm14090427.

Aysan, Ahmet, and Ibrahim Musa Unal. 2021. "Fintech And Blockchain in Islamic Finance: A Bibliometric Analysis." SSRN Scholarly Paper 3921538. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3921538.

Bech, Morten Linnemann, and Rodney Garratt. 2017. "Central Bank Cryptocurrencies," September. https://www.bis.org/publ/qtrpdf/r_qt1709f.htm.

Best, Raynor de. 2022. "Number of Crypto Coins 2013-2022." Statista. February 8, 2022. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.

"BIS-Press Release." 2021. February 23, 2021. https://www.bis.org/press/p210223.htm.

"CBDC Whitepaper." 2020. *Ripple* (blog). 2020. https://ripple.com/lp/cbdc-whitepaper/.

Chong, F.H.L. 2021. "Enhancing Trust through Digital Islamic Finance and Blockchain Technology." *Qualitative Research in Financial Markets* 13 (3): 328–41. https://doi.org/10.1108/QRFM-05-2020-0076.

Coinbase. 2022. "What Is DeFi?" Coinbase. 2022. https://www.coinbase.com/learn/crypto-basics/what-is-defi.

CoreLedger. 2019. "What Are Smart Contracts? A Breakdown for Beginners." *CoreLedger* (blog). October 9, 2019. https://medium.com/coreledger/what-are-smart-contracts-a-breakdown-for-beginners-92ac68ebdbeb.

Cuomo, Jerry. 2020. “How Blockchain Adds Trust to AI and IoT IBM Supply Chain and Blockchain Blog.” IBM Supply Chain and Blockchain Blog. August 5, 2020. https://www.ibm.com/blogs/blockchain/2020/08/how-blockchain-adds-trust-to-ai-and-iot/.

Deloitte. 2021. “CBDC: The next Disruptor.” https://www2.deloitte.com/us/en/pages/financial-services/articles/cbdc-central-bank-digital-currency.html.

Dosso, Mamadou, and Ahmet Faruk Aysan. 2022. “The Technological Impact in Finance: A Bibliometric Study of Fintech Research.” In *Eurasian Business and Economics Perspectives*, edited by Mehmet Huseyin Bilgin, Hakan Danis, Ender Demir, and Ghulam Mustafa, 193–209. Eurasian Studies in Business and Economics. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-94672-2_12.

Fernández-Caramés, Tiago M., and Paula Fraga-Lamas. 2018. “A Review on the Use of Blockchain for the Internet of Things.” *IEEE Access* 6: 32979–1. https://doi.org/10.1109/ACCESS.2018.2842685.

Gartner. 2022. “Definition of Blockchain - Gartner Information Technology Glossary.” Gartner. 2022. https://www.gartner.com/en/information-technology/glossary/blockchain.

Georgieva, Kristalina. 2022. “The Future of Money: Gearing up for Central Bank Digital Currency.” IMF. February 9, 2022. https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency.

Geroni, Diego. 2021. “Hybrid Blockchain: The Best of Both Worlds.” *101 Blockchains* (blog). January 28, 2021. https://101blockchains.com/hybrid-blockchain/.

Hou, Felicia. 2021. “Stablecoins Are Taking over the Crypto World and They’re a Hot Topic for Congress—Here’s What They Are and the Fastest-Rising Ones to Keep an Eye On.” Fortune. December 8, 2021. https://fortune.com/2021/12/08/stablecoins-cryptocurrency-congress/.

Intelligence, Insider. 2022. “IoT in Banking: Examples of IoT Technology Used in Financial Services.” Business Insider. January 11, 2022. https://www.businessinsider.com/iot-banking.

“IoT Basics.” 2015. Opentechdiary. July 24, 2015. https://opentechdiary.wordpress.com/category/iot-basics/.

Kiran, D. R. 2019. “Chapter 35 - Internet of Things.” In *Production Planning and Control*, edited by D. R. Kiran, 495–513. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-818364-9.00035-4.

Kulkarni, Rajendra, Laurie Schintler, Naoru Koizumi, Jim Olds, and Roger R. Stough. 2019. “Cryptocurrency, Stablecoins and Blockchain: Exploring Digital Money Solutions for Remittances and Inclusive Economies.” SSRN Scholarly Paper ID 3511139. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3511139.

Kumar, Povun. 2022. “Top 10 Decentralized Finance (DeFi) Use Cases.” Finextra Research. March 9, 2022. https://www.finextra.com/blogposting/21958/top-10-decentralized-finance-defi-use-cases.

Landau, Susan. 2013. “Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations.” *IEEE Security Privacy* 11 (4): 54–63. https://doi.org/10.1109/MSP.2013.90.

Lauslahti, Kristian, Juri Mattila, and Timo Seppala. 2017. “Smart Contracts How Will Blockchain Technology Affect Contractual Practices?” *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3154043.

Majaski, Christina. 2021. "Distributed Ledgers." Investopedia. October 9, 2021. https://www.investopedia.com/terms/d/distributed-ledgers.asp.

Meola, Andrew. 2022. "A Look at Examples of IoT Devices and Their Business Applications in 2022." Business Insider. January 11, 2022. https://www.businessinsider.com/internet-of-things-devices-examples.

Nanaeva, Zhamal, Ahmet Faruk Aysan, and Nasim Shah Shirazi. 2021. "Open Banking in Europe: The Effect of the Revised Payment Services Directive on Solarisbank and Insha." *Journal of Payments Strategy & Systems* 15 (4): 432–44.

PricewaterhouseCoopers. 2022. "Making Sense of Bitcoin, Cryptocurrency and Blockchain." PwC. 2022. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

Reiff, Nathan. 2021. "Decentralized Autonomous Organization (DAO)." Investopedia. September 24, 2021. https://www.investopedia.com/tech/what-dao/.

Soderberg, Gabriel, Marianne Bechara, Wouter Bossu, Natasha Che, and Akihiro Yoshinaga. 2022. "Behind the Scenes of Central Bank Digital Currency." IMF. February 2022. https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174.

"Time Is Money-FINANTEQ." 2021. Mobile Banking Platforms. 2021. https://finanteq.com/smartwatch/.

"Types of Blockchains." 2018. DataFlair. June 4, 2018. https://data-flair.training/blogs/types-of-blockchain/.

"UK Central Bank Digital Currency." 2022. Bank of England. March 21, 2022. https://www.bankofengland.co.uk/research/digital-currencies.

Zetzsche, Dirk A, Douglas W Arner, and Ross P Buckley. 2020. "Decentralized Finance." *Journal of Financial Regulation* 6 (2): 172–203. https://doi.org/10.1093/jfr/fjaa010.