Preliminary Design Considerations and Characteristics of Afkoin

Edwin Ayisi Opare & Kwangjo Kim

Cryptology and Information Security Lab, School of Computing, KAIST, 34141, Daejeon, South Korea

This is an Internal Report on the *Preliminary Design Considerations and Characteristics of Afkoin* published at the Cryptology and Information Security Lab at KAIST. Date of first publication, August 14, 2019. Date of current version, June 23, 2020.

Abstract: In this report, we present the preliminary design considerations and characteristics of Afkoin, a central bank quantum-resistant digital currency for the Economic Community of West African States (ECOWAS). Afkoin is proposed as a candidate solution to ECOWAS' quest to issue a single currency for use by its fifteen-nation Member States. We posit that, the new target year of 2020 for the issuance of a single paper currency in ECOWAS is infeasible, and that a single currency that is based on distributed ledger technology (DLT) presents the best and fastest route to achieving the goals of an economic and monetary union as envisaged in the revised ECOWAS Treaty. Afkoin will represent a claim on asset on ECOWAS Member States and will be pegged against the Special Drawing Right; thereby mitigating the volatility associated with private sector-issued digital currencies.

Index Terms: Afkoin, ECOWAS, digital currency, DLT, single currency, EMU.

1. Introduction

The Economic Community of West African States (ECOWAS) is a fifteen Member State regional bloc in West Africa established in May 1975 by the *Lagos Treaty* [1] to "*promote co-operation and development in all fields of economic activity"* among Member States.

The Lagos Treaty was succeeded by the *Cotonou Treaty* [2] in July 1993 to *"promote co-operation and integration, leading to the establishment of an economic union in West Africa through the adoption of common policies in the economic, financial, social and cultural sectors, and the creation of a monetary union"*.

An expected outcome of the revised ECOWAS Treaty is the creation of an economic and monetary union (EMU) among ECOWAS Member States, and consequently, the issuance of a single currency for use within the ECOWAS region.

The Member States of ECOWAS are Benin, Burkina Faso, Cape Verde, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, the Gambia, and Togo [16].

ECOWAS Member States can be grouped into eight French-speaking countries, five English-speaking countries and two Portuguese-speaking countries as presented in Fig. 1.

1.1. ECOWAS Single Currency Programme

To establish an ECOWAS EMU and issue a single currency in ECOWAS, ECOWAS Member States proposed to implement the ECOWAS EMU in two phases [7] along currency lines. A number of ECOWAS Member States shared a common currency, the CFA-Franc while other Member States

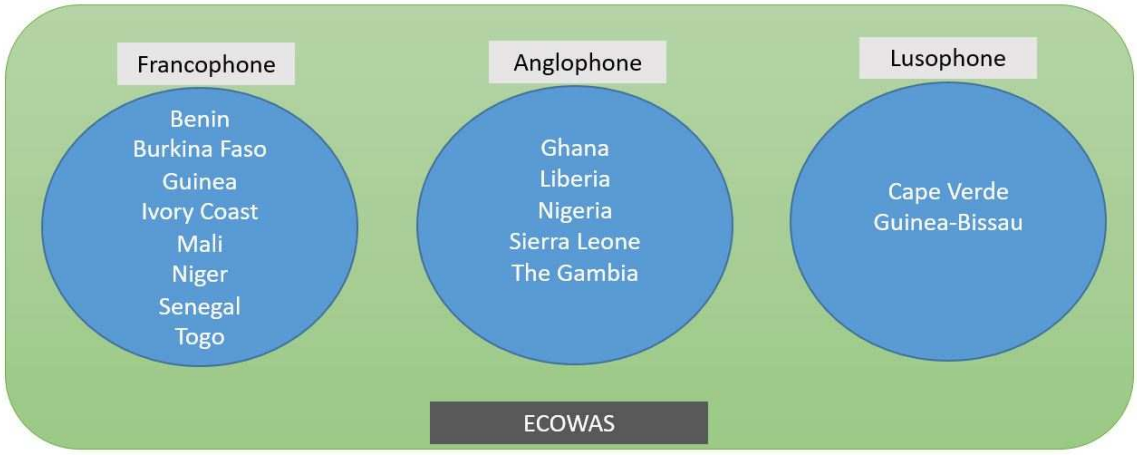


Fig. 1. ECOWAS Regional Grouping by Spoken Language

had individual currencies [7]. ECOWAS therefore established two currency-oriented EMUs with the goal to merge both EMUs in the long term [4].

ECOWAS Member States that shared the CFA-Franc were organized under one EMU called the Union Économique et Monétaire Ouest-Africaine (UEMOA) or the West African Monetary and Economic Union (WAEMU) through the enactment of the *Dakar Treaty* [8] in January 1994. At its creation, WAEMU consisted of seven Francophone countries namely Benin, Burkina Faso, Ivory Coast, Mali, Niger, Senegal and Togo. Guinea-Bissau, a lusophone country joined WAEMU as the eighth Member State in May 1997 [8]. The main objective of WAEMU was to establish a customs union and adhere to a common economic and monetary policy within the WAEMU sub-regional bloc [9].

ECOWAS Member States without a common currency were organized into a second EMU known as the West African Monetary Zone (WAMZ) through the ratification of the *Accra Declaration* [3] in April 2000. At its creation, WAMZ consisted of five Member States namely, Ghana, Guinea, Liberia, Nigeria, Sierra Leone and the Gambia. Liberia joined the WAMZ as the sixth Member State in February 2010 [3]. The composition of the WAEMU and WAMZ Member States is presented in Fig. 2.

Currently, Cape Verde does not belong to any of the two ECOWAS EMUs and is therefore excluded from the EMU grouping in Fig. 2.

The goal of the Accra Declaration [3] is to establish the WAMZ as a second ECOWAS EMU and provide mechanisms for the establishment of a common ECOWAS central bank. The common ECOWAS central bank would be responsible for monetary policy administration and issuance of the *ECO* single currency in WAMZ by the year 2003 [3].

The Accra Declaration [3] proposed a set of economic convergence criteria; an action plan to achieve the convergence criteria; and institutional arrangements for the issuance of the ECO single currency. The economic convergence criteria defined in the Accra Declaration is presented Fig. 3 .

WAMZ Member States were unable to meet the established convergence criteria and therefore postponed the issuance of the ECO on multiple occasions [5]. In July 2014, ECOWAS abolished the ECO project altogether in favour of issuing an ECOWAS-wide single currency in the year 2020 [5], [6] .

In line with the 2020 ECOWAS-wide single currency objective, a revised convergence criteria was ratified by ECOWAS Member States in December 2015 in Dakar through the ECOWAS *Supplementary Act A/SA.01/12/15* [10]. The Supplementary Act revised the convergence criteria from ten criteria items to six criteria items, with Member States expected to comply with the revised

Fig. 2. ECOWAS Regional Grouping by EMU

Primary Criteria
Budget deficit (excluding grants) to GDP ratio: ≤ 5% by 2000 and ≤ 4% by 2002.
Annual average inflation: ≤ 10% by the year 2000 and ≤ 5% by 2003.
Central bank financing of budget deficit: ≤ 10% of previous year's tax revenue.
Gross external reserves: ≥ 3 months of import by end of 2000 and ≥ 6 months of import by end of 2003.
Secondary Criteria
Non-accumulation of domestic and external arrears and liquidation of existing ones.
Ratio of wage bill to tax revenues: ≤ 35%.
Tax revenue to GDP ratio: ≥ 20 percent.
Real interest rate: > 0%.
Stability of the nominal exchange rate: +/-10%.
Public investments to tax revenue: ≥ 20%.

Fig. 3. ECOWAS Convergence Criteria [3]

convergence criteria by December 2019. The revised convergence criteria is presented in Fig 4.

Primary Criteria
Budget deficit (excluding grants) to GDP ratio: $\leq$ 3% in 2019
Annual average inflation rate: $\leq$10% with objective of $\leq$5% in 2019
Central bank financing of budget deficit: $\leq$ 10% of previous year's tax revenue
Gross external reserves $\geq$ 3 months of imports
Secondary Criteria
Public debt to GDP: $\leq$ 70%
Nominal exchange rate variation: +/-10%

Fig. 4. Revised ECOWAS Convergence Criteria [10]

At its Presidential TaskForce meeting in February 2018, the leadership of ECOWAS indicated its commitment to the ECOWAS Single Currency Programme [11].

The ECOWAS Commission, the institution responsible for the day-to-day running of ECOWAS issued a Terms of Reference document in October 2018 inviting *proposals on the name and visual design of the future ECOWAS currency* [12].

We posit that, by leveraging distributed ledger technology (DLT) and adopting best practice approaches for central bank digital currency (CBDC) issuance, an ECOWAS single currency that guarantees adherence to and compliance with the ECOWAS economic convergence criteria may be issued in West Africa.

We propose for the new ECOWAS single currency to be called *Afkoin*. We propose for the Afkoin CBDC to be a DLT-based quantum resistant digital currency.

Afkoin will represent a claim on the assets of ECOWAS Member States and pegged against the Special Drawing Right (SDR) [33] to minimize price volatility.

Afkoin will perform the functions of money and thus can be used to make payments in ECOWAS.

2. Rationale for Afkoin

In this section, we present our rationale for Afkoin, a DLT-based quantum-resistant CBDC. The rationale presented is non-exhaustive.

2.1. Algorithmically Achieve The Convergence Criteria

The revised ECOWAS convergence criteria (Fig. 4) required that by December 2019, ECOWAS Member State's:

- Budget deficit be less than or equal to 3% of gross domestic product (GDP);
- Annual average inflation rate be at most 5%;
- Central bank financing of budget deficit be at most 10% of the previous year's tax revenue;
- Gross external reserves covers at least 3 months of imports.

Additionally, each Member State's public debt to GDP ratio was required to be at most 70% while nominal exchange rate variation was expected to not exceed 10%.

At the Twenty-first Session of the Intergovernmental Committee of Experts in June 2018, the United Nations' Economic Commission for Africa (ECA) noted that no ECOWAS Member State had been able to fully achieve the convergence criteria [13]. In Fig 5, the ECA indicates that, no country in ECOWAS achieved the budget deficit to GDP ratio requirement between 2005 and

2016. Only three Member States, Ivory Coast, Nigeria and Liberia achieved a score of 75% or more for the budget deficit to GDP ratio economic indicator.

Country	Benin	Burkina Faso	Cabo Verde	Côte d'Ivoire	Gambia, the	Ghana	Guinea	Guinea Bissau	Liberia	Mali	Niger	Nigeria	Senegal	Sierra Leone	Togo
Primary rank criteria															
Budget deficit ≤ 3%	50	25	0	75	16.7	8.3	66.7	41.7	91.7	33.3	25	83.3	0	16.7	25
Inflation rate ≤ 10%	100	100	100	100	100	25	33.3	100	91.7	100	91.7	41.7	100	25	91.7
Budget deficit financed by the Central Bank ≤10%	100	100	100	100	58.3	66.7	75	100	100	100	100	91.7	100	66.7	100
Gross Reserves in months of import ≥ 3	100	100	100	100	83.3	75	16.7	100	33.3	100	100	100	100	91.7	100
Second rank criteria															
Public debt/GDP <=70%	100	100	0	100	0	50	83.3	100	100	100	100	100	100	100	66.7
Nominal exchange rate variation ± 10 %	100	100	100	100	83.3	66.7	66.7	100	100	100	100	66.7	100	83.3	100

Fig. 5. ECOWAS Convergence Criteria Compliance from 2005-2016 [13]

For the inflation target, eight Member States achieved 100% success while three other Member States achieved 91.7% success rates. Ghana, Sierra Leone, Guinea and Nigeria scored below 50% for this economic indicator.

In the budget deficit financed by central banks category, ten Member States achieved 100% success rates; Nigeria achieved a 91.7% success rate while Guinea achieved a 75% success rate. The Gambia scored 58.3% while each of Ghana and Sierra Leone scored 66.7% in this category.

For the gross reserves to imports target, ten Member States achieved a 100% success over the 2005-2016 period. Ghana, the Gambia, and Sierra Leone scored 75% or more in this category. Both Guinea and Liberia scored a low of 16.7% and 33.3% respectively in this category.

In the year 2016, the actual public debt to GDP ratio recorded in Ghana was 73.1%, exceeding the required 70% threshold by more than 3% [14]. Guinea (83.3%) and Togo (66.7%) also missed the public debt to GDP ratio target as indicated in Fig.5. Both Cape Verde and the Gambia scored 0% in the public debt to GDP ratio category.

Ten ECOWAS Member States attained 100% success rates for the normal exchange rate variation indicator. Two Member States (The Gambia and Sierra Leone) scored 83.3% while three others (Ghana, Guinea and Nigeria) scored 66.7% respectively.

As at the end of December 2019, no ECOWAS Member State was known to have achieved all the economic convergence targets. Evidently, achieving the macroeconomic convergence targets in ECOWAS using traditional monetary policy tools and transmission mechanisms has been

unsuccessful.

Consequently, we posit that, through the issuance of a DLT-based Afkoin, smart contracts and efficient consensus algorithms may be leveraged to achieve the desired monetary policy and fiscal policy targets among ECOWAS Members States. Afkoin will thus help to achieve the convergence criteria and ultimately the issuance of a single currency in ECOWAS.

2.2. ECOWAS Is Mobile

The ECOWAS region occupies a land area of more than 6 million square kilometer with a population of 399.5 million and a median age of 18.2 years [15]. The youthfulness of the ECOWAS population has led to an exponential growth in mobile services adoption in the sub-region. The number of unique mobile subscribers in ECOWAS grew from 122 million in 2012 to 185 million in 2018. It is estimated that, the mobile penetration rate in ECOWAS based on the number of unique mobile subscribers will reach 50% in 2020, growing to 54% in 2025. We present ECOWAS' unique mobile subscription trend in Fig. 6.

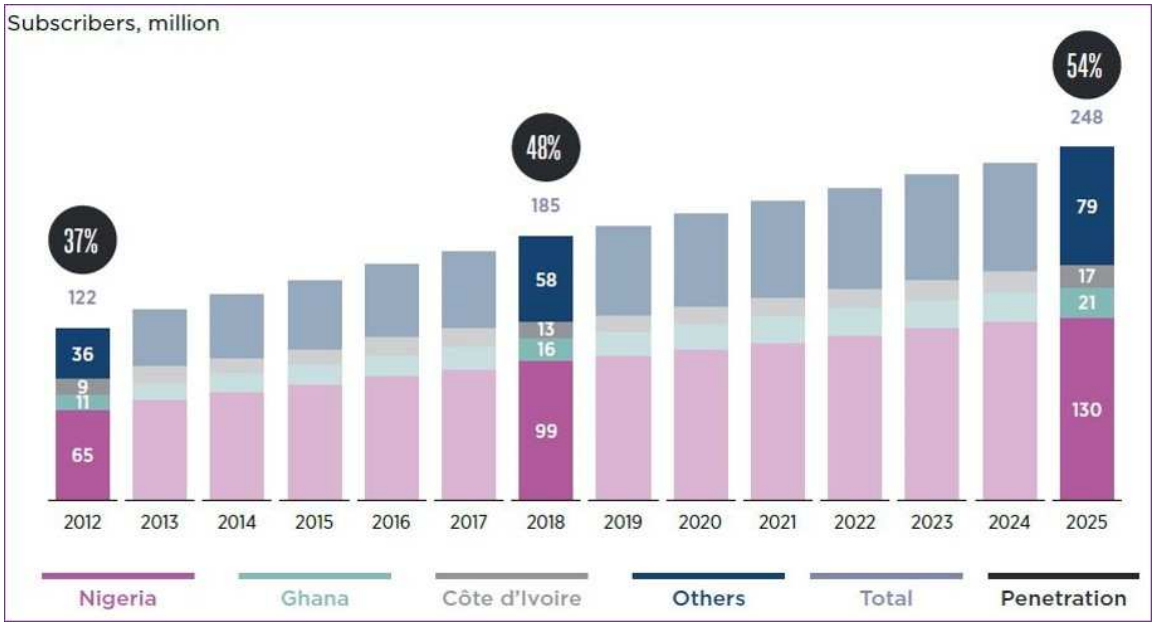


Fig. 6. Unique Mobile Subscription Trend in ECOWAS [17]

In 2025, mobile internet adoption in ECOWAS is expected to increase to 183 million subscribers from 100 million subscribers in 2018. Over the same time interval, internet connections from smartphones will account for up to 67% of all internet traffic in ECOWAS, representing an increase of more than two-folds in less than a decade. The ECOWAS internet adoption rate via smartphones is presented in Fig. 7.

For a majority of the inhabitants of ECOWAS, mobile phones are the primary means by which they access life-changing services including but not limited to finance, healthcare, education and payment services. As a result, fintech companies have leveraged the pervasiveness of mobile adoption in ECOWAS to roll-out various mobile-based services. Mobile-based services accounted for 8.7% of West Africa's GDP in 2018 [17]. The GDP contribution of mobile-based services in West Africa is expected to grow to 9.5% by 2023 [17].

In ECOWAS and other parts of Africa, only about 34% of adults had formal bank accounts in 2014 [18]. Through fintech innovations such as mobile money services, more ECOWAS citizens now have access to formal accounts either with a bank or with a mobile money service provider [19]. Access to accounts through mobile mechanisms is deepening financial inclusion across the

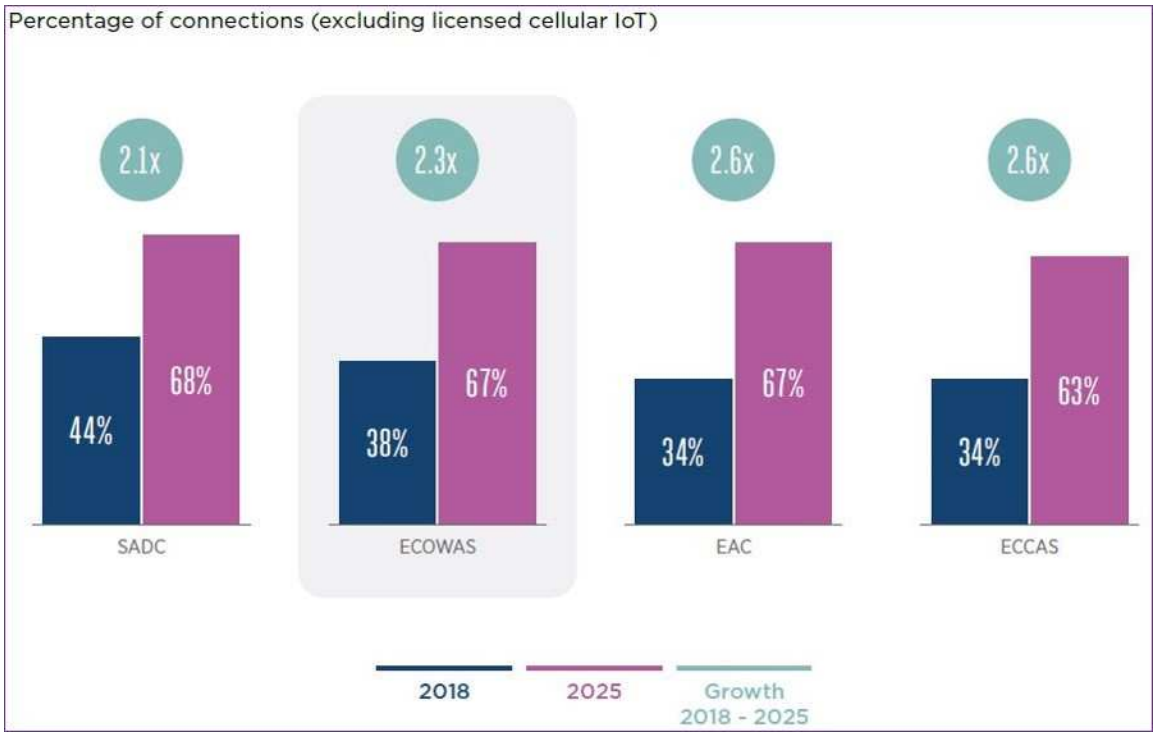
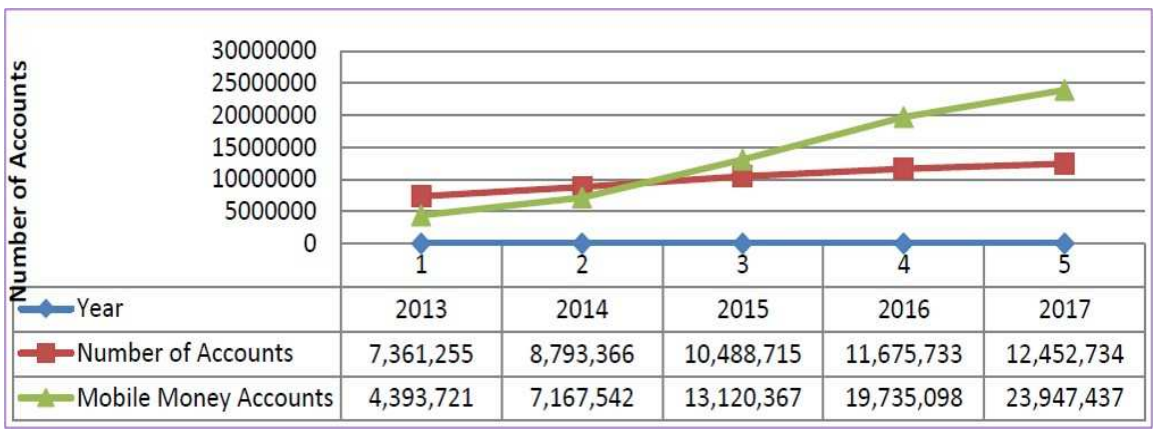


Fig. 7. ECOWAS Mobile Internet Connection Rate via Smartphones [17]

ECOWAS sub-region [17].

In Ghana, mobile money adoption increased from just 4.3 million subscribers in 2013 to a massive 23.9 million subscribers in 2017, representing a massive 445% increase in adoption rate over just five years[20]. Subscriptions for formal bank accounts only increased to 12.4 million subscriptions in 2017 from 7.3 million subscriptions in 2013, representing a mere 69% adoption rate over the 2013 to 2017 time period. A detailed comparison of the formal bank account subscription rate versus the mobile money account subscription from 2013 to 2017 is presented in Fig. 8.



Year	2013	2014	2015	2016	2017
Number of Accounts	7,361,255	8,793,366	10,488,715	11,675,733	12,452,734
Mobile Money Accounts	4,393,721	7,167,542	13,120,367	19,735,098	23,947,437

Fig. 8. Formal Bank Account Versus Mobile Money Account Subscription Trend in Ghana [20]

To continuously increase and deepen financial inclusion for the unbanked, unserved and under-

served populations of ECOWAS, issuing a paper-based currency may erode the financial inclusion gains attained in ECOWAS over the last decade.

We therefore posit that, the planned ECOWAS single currency should be mobile-based instead of paper-based.

2.3. Cash Is Expensive

Cash refers to physical money such as banknotes and coins issued by a given nation-state. Cash represents a claim on the assets of the issuing central bank and liabilities of the country in which the cash is issued [22]. Specialized equipment along with specialized skill set to operate the equipment is necessary to ensure the issuance of cash that is secure and counterfeit-proof [21].

In most jurisdictions, cash is printed by specialized entities authorized by the given government or by the central bank of the given nation-state. In the United States of America, banknotes are printed by the Bureau of Engraving and Printing while coins are minted by the United States Mint all under the authorization of the United States Department of Treasury [22].

The process of creating cash which begins with a detailed design of the underlying currency, followed by the printing or minting, storage and finally distribution is expensive. Following the printing or minting of cash, it is transported to the central bank and authorized cash depository companies via armored carriers for storage in highly secure vaults [24]. Upon request from commercial and/or retail bank, cash is transported from a cash depository company to the requesting bank via cash-in-transit companies [23]. To transport the cash at the requesting bank to its various branches, the requesting bank uses a combination of cash-in-transit companies and other transport mechanisms [23]. We present the cash distribution process in Sweden in Fig. 9.

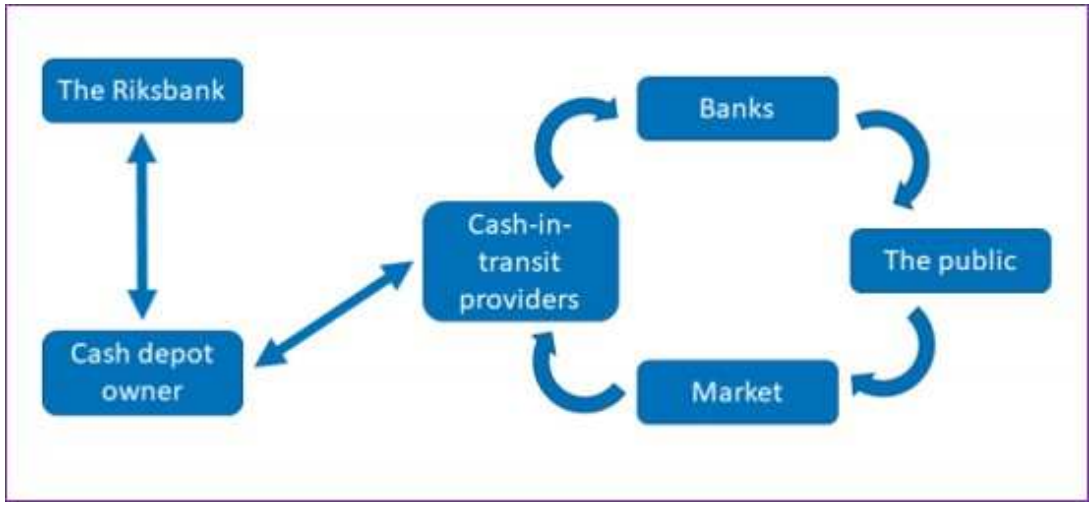


Fig. 9. Cash Distribution Process in Sweden [23]

We note that, the Sweden cash distribution process is designed to improve the efficiency and costs associated with the cash handling process in the country [23]. More importantly, a greater proportion of the Swedish population prefer to use other payment mechanisms such as mobile-based payment methods and credit cards instead of cash [23], therefore Sweden's cash printing and handling cost may be significantly lower than in ECOWAS countries and other jurisdictions.

In the 2019 calendar year, the Bureau of Engraving and Printing charged the the Federal Reserve a total of $959 million (or 13.7% of the monetary value) for the production of $7 billion banknotes for the Federal Reserve [25]. The charge by Bureau of Engraving and Printing to the Federal Reserve includes cost for printing banknotes, transportation of the printed banknotes, R&D, multi-cycle capital budget and other related activities. Elsewhere in Italy, it was reported that minting euro coins cost four times the value of the coins [26].

Although expansive research comparing the costs of issuing paper-based currencies and digital currencies are limited in literature, we posit that the issuance of Afkoin will only require a fraction of the costs associated with the printing and distribution cash [27]. Afkoin will be distributed electronically over the internet to commercial banks and other end users, thereby eliminating the transportation costs and other handling costs related to cash.

Secondly, transporting cash along the cash-distribution value chain requires a significant amount of time and risks. In a crisis such as a bank run, war or political upheaval when demand for cash generally increases, getting cash across to consumers along the value chain will be daunting [23]. On the other hand, Afkoin can be digitally transferred from banks to consumers within microseconds in times of such crisis.

2.4. Existing Payment Mechanisms Are Unsafe

In the paper *Covid-19, cash, and the future of payments* [28], the Bank for International Settlements (BIS) analyzes public perception of the impact of the recent COVID-19 outbreak and previous outbreaks on payment methods such as cash, credit cards and point-of-sale (POS) terminals.

In [28], the authors note that, based on data analysis from Google search queries, citizens in countries with a higher cash-in-circulation to GDP for small-denomination banknotes indicated the most concern with respect to the potential transmission of microbes through the use of cash.

The BIS underscores that there are no recorded cases of COVID-19 transmission through cash although some central banks moved to either sanitize [29] or quarantine [30] cash in the course of the corona disease outbreak.

According to the paper [28], it has been proven through scientific research that, there is the possibility of transmission of microbes through cash; however, the risk of transmission through other payment mechanisms such as credit cards and POS terminals were much higher compared to cash. The rationale for this conclusion is that, microbes survive on different surfaces at different lengths of time as presented in Fig. 10.

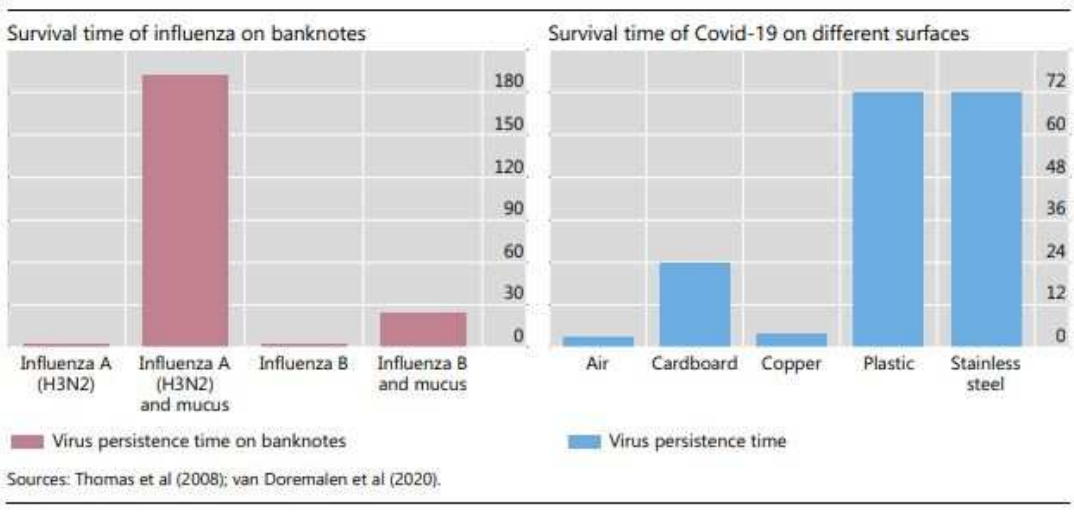


Fig. 10. Survival of Viruses on Multiple Surfaces in Hours [28]

The BIS in its paper [28], therefore enjoined central banks to explore the possibility of issuing CBDCs to mitigate against future disease outbreaks, with a further recommendation to implement safeguards and mechanisms to ensure financial inclusion in the process.

To this end, and in subsequent chapters of this paper, we present the development scope and characteristics of Afkoin.

3. Scope of Afkoin

Two types of payment systems are defined in literature namely, retail payment systems and wholesale payment systems [31].

A retail payment system refers to payment systems that enable the general public and businesses to purchase goods and services[23]. Generally, the value of retail transactions are significantly smaller compared to the value of wholesale transactions. Any consumer can participate in a retail payment system.

A Wholesale payment system enables the transfer of high-value central bank money between authorized payment service providers (PSP) such as commercial banks (CMBs) and other high-value customers [32]. Access to a wholesale payment system is restricted to only PSPs [31]. Wholesale payment transactions are generally executed on a real-time gross settlement (RTGS) system or large-value transfer system (LVTS).

Due to their restricted-access feature, payment systems innovation began with wholesale payment systems in the early 1990s while retail payment system innovation only begun in the 2000s. Coordinating innovation development in wholesale payment systems are more tractable and easy to manage compared to retail payment systems [32].

Following the payment system innovation trend, the Afkoin prototype will be implemented as a wholesale CBDC (W-CBDC) infrastructure.

The scope of the Afkoin prototype will include:

- Issuance of Afkoin as a DLT-based W-CBDC asset.
- Development of a DLT-based RTGS prototype with liquidity-savings mechanism (LSM) functionalities for wholesale interbank settlement of Afkoin.
- Implementation of capabilities to enable Afkoin platform participants pledge tokenized securities as collateral for central bank liquidity.
- Implementation of mechanisms to guarantee counterparty data privacy and settlement finality on the Afkoin platform.

Coordinating such an innovation in a confined geographical setting will also enable the rapid evaluation and assessment of the suitability of DLT to achieve the objectives of this research. As a result, the Afkoin prototype is implemented in line with wholesale payment system infrastructure requirements in Ghana. Ghana's wholesale payment infrastructure is known as the Ghana Interbank Settlement (GIS) system. Ghana's GIS system is owned and operated by the Bank of Ghana [20].

All design decisions relating to the development of Afkoin will be based solely on existing ECOWAS single currency legal statutes and payment system infrastructure requirements in Ghana.

4. ECOWAS Statutes and Payment Systems

To facilitate the establishment of an ECOWAS EMU and single currency, various regional organizations and legal statutes have been ratified in ECOWAS.

We highlight the relevant legal statutes and ECOWAS organizations in this section. Additionally we discuss existing payment systems arrangements in ECOWAS and Ghana.

4.1. ECOWAS Single Currency Statutes

ECOWAS Member States signed the *Accra Declaration* [3] in April 2000 to establish the WAMZ. The goal of the Accra Declaration is to establish the WAMZ as a second ECOWAS EMU and provide mechanisms for the establishment of a common ECOWAS central bank.

The common ECOWAS central bank would be responsible for monetary policy administration and issuance of the *ECO* single currency in the WAMZ by the year 2003 [3].

4.1.1. WAMZ Agreement

In December 2000, WAMZ Member States passed the WAMZ Agreement [34] to establish the following key institutions:

- ***Authority of Heads of State and Government*** as the political and highest decision-making body of WAMZ, with the overall responsibility for the achievement of the objectives of WAMZ.
- ***West African Central Bank (WACB)*** as a common central bank for the WAMZ with responsibility for monetary policy administration in the Zone.
- ***West African Monetary Institute (WAMI)*** as a legal entity to implement the functions leading to the establishment of the WACB.
- ***Stabilization and Cooperation Fund (SCF)*** to provide temporary financial assistance to WAMZ Member States in order to attain the Convergence Criteria enshrined in the Accra Declaration.
- ***Technical Committee*** is responsible for collaborating with WAMI to coordinate policies that would lead to the achievement of the goals of the WAMZ Agreement.

4.1.2. West African Monetary Agency

The ECOWAS Authority of Heads of State and Government, the highest decision-making body of ECOWAS established the West African Monetary Agency (WAMA) in 1996 [35].

The primary responsibility of WAMA is the management and operation of the West African Clearing House (WACH). The WACH was established in 1975 to serve as a multilateral payment facility to promote trade in ECOWAS as well as the settlement of trade and non-trade transactions among ECOWAS central banks.

In 1996, WAMA was further tasked with the responsibility of monitoring, coordinating and implementing the ECOWAS Monetary Cooperation Programme (EMCP), geared towards the creation of the ECOWAS single currency [35].

4.2. Payment Systems in Ghana

Payments systems in Ghana comprises of wholesale and retail payment systems.

Ghana's wholesale payment system is called the Ghana Interbank Settlement (GIS) system [20]. The GIS system is owned and operated by the Bank of Ghana [20].

In 2018, the GIS system settled a total of 1.22 million transactions. The GIS system therefore settled approximately 5000 transactions per day in 2018. On the average, the GIS records a year-on-year transaction volume increase of about 30% [36].

Participants in the GIS in 2018 included thirty-four PSPs, ARB Apex Bank, and the Social Security and National Insurance Trust (SSNIT) [36]. ARB Apex Bank is the clearing bank for rural and community banks in Ghana. SSNIT is Ghana's regulator of social security and pension schemes.

The retail payment system in Ghana is made up of the [37]:

- Ghana Automated Clearing House (GACH);
- Gh-Link™ (National Switch);
- GhIPSS Instant Pay;
- Cheques Codeline Clearing (CCC); and
- Mobile Money payment systems;

The mobile money payment systems are owned and operated by various telecommunication service providers in Ghana.

The rest of Ghana's retail payment systems are operated and managed by the *Ghana Interbank Payment and Settlement Systems Limited (GhIPSS)*, a wholly owned subsidiary of the BOG [37]. More recently, GhIPSS rolled out a mobile money interoperability infrastructure.

The GACH system consists of the, E-Zwich payment system, Direct Credit payment system; and the Direct Debit payment system.

High-value transactions are processed directly on the GIS system while low value transactions are cleared and netted on the GhIPSS's platform and posted into the GIS for settlement.

In this paper, we focus on the the GIS system.

5. Technologies

Afkoin will be implemented on DLT and will be resistant against quantum computing attacks. We provide a brief thesis on the underlying technologies on which Afkoin will be issued.

5.1. DLT

DLT refers to a combination of technologies and capabilities that provide strong auditability and traceability guarantees to enable multiple system participants to share in a trustless environment, access to the same data over multiple logical and geographic locations.

Blockchain, a type of DLT introduced by Satoshi Nakamoto [62], [63] in 2008 popularized the term DLT following the release of the Bitcoin core [69] in 2009.

A blockchain may be defined as a "constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological and immutable way" [40]. A more detailed definition of blockchain is given as "a distributed database, which is shared among and agreed upon a peer-to-peer network. It consists of a linked sequence of blocks, holding timestamped transactions that are secured by public-key cryptography and verified by the network community. Once an element is appended to the blockchain, it cannot be altered, turning a blockchain into an immutable record of past activity" [64] .

All blockchains are a type of DLT; however, not all DLTs are blockchains as various approaches other than *blocks* may be used to chronologically and immutably record transactions on a ledger. Nonetheless, in this research, we use the term blockchain and DLT interchangeably.

Key characteristics of DLT includes distributedness, security, privacy, immutability, data integrity, and redundancy [64], [65]. These characteristics make DLT suitable for several applications and industries that require these features.

Two main types of DLT platforms are identified in literature, namely permissionless and permissioned DLT platforms [68].

5.1.1. Permissionless DLT Platforms

Permissionless DLT platforms are also known as public DLT platforms. A public DLT platform refers to a DLT system that is open for adoption and/or usage by the everyone without the need for authorization from a trusted third-party. Anyone can join such a DLT system and begin to publish or mine blocks without an approval from a central authority [68]. Additionally, anyone can *fork* (download and modify) versions of such a DLT system to create new applications and services without requiring authorization from a trusted party.

Due to the absence of a trusted third-party who checks unacceptable system behaviour in a permissionless DLT network, resource-intensive consensus mechanisms such as Proof-of-Work (PoW) [69] and Proof-of-Stake (PoS) [66], [67] are used to guarantee system trust and integrity.

Examples of a permissionless DLT platform include Bitcoin and Ethereum.

5.1.2. Permissioned DLT Platforms

Permissioned DLT platforms are also known as private DLT platforms. A private DLT platform refers to a DLT system that require authorization from a trusted third-party before participants can join the system [68].

All participants in a permissioned DLT system must be registered, authorized and authenticated by the trusted party before they are able to carry out transactions in the system.

Various consensus approaches including but not limited to Practical Byzantine Fault Tolerance (PBFT) [41], Istanbul Byzantine Fault Tolerance (IBFT) [42], Kafka [43] and Raft-based [44] consensus mechanisms have been proposed for permissioned DLT systems.

Examples of popular permissioned DLT systems include Quorum [45], Hyperledger Fabric [46] and Corda [47].

5.2. Quantum Computing

Quantum computing may be defined as the use of the quantum-mechanics phenomena of superposition and entanglement to perform computations at speeds faster than the computational speeds of classical computing systems.

Classical computing systems store and manipulate information using long strings of *binary bits*. Binary bits can be in a state of *0* or *1* at any given time. Quantum computers, however, manipulate information using quantum bits (*qubits*) that are based on the quantum-mechanical phenomena of *superposition* and *entanglement* [48], [49].

Superposition enables quantum systems to be in multiple states concurrently while entanglement ensures that there is a strong correlation between these states even if states are separated by huge distances [48]. The multi-state feature in quantum systems enable such systems to perform computations at speeds much faster than classical computing systems. The higher the number of qubits in a quantum computer, the faster it is able to perform assigned computations [49]. It is estimated that, quantum computers may be available within the next decade [51]. Once quantum computers are available they will have the potential to speed up drug discovery times, help combat global warming, and facilitate the crunching and processing of data much faster than existing computing systems [49], [51]. Due to the faster processing speeds of quantum computers, they will be able to break majority of the existing public key cryptography systems and digital signature schemes that are used to secure critical national infrastructure such as FMIs, web servers, web services and many more [59].

Classical cryptosystems such as the Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) rely on mathematical hard problems for their security [50]. The RSA cryptosystem is computationally secure against the big-integer factorization problem while DSA and ECDSA are secure against the discrete logarithm problem and the elliptic-curve discrete logarithm problem respectively [54]. Many of the existing DLT platforms including Bitcoin and Ethereum rely on RSA and ECDSA among others for transaction authentication and for achieving transaction consensus [51]. However, advancements in quantum computing based on Shor's algorithm [52], [50] have rendered these classical cryptosystems insecure. Mosca [51] estimates that there is a 50 per cent chance that quantum computers will break RSA-2048 by 2031. Proactively responding to the threat of quantum computers, the NSA deprecated Suite B, an ECC-based cryptographic standard used to secure top-secret US Government information in favor of quantum-resistant standards in 2015 [53].

Two approaches have emerged in literature to address the threat of quantum computers: post-quantum cryptography (PQC) and quantum cryptography based on quantum key distribution (QKD). The security of PQC is based on conventional ciphers that leverage mathematical hard problems other than discrete logarithms and integer factorization [51]. The security of QKD is based on the quantum-mechanics *non-cloning theorem* [55].

PQC approaches such as multivariate-quadratic-equations, lattice-based cryptography, code-based cryptography, hash-based cryptography, and isogeny-based cryptography are studied in literature [51].

Researchers such as [54], [57] and [60], [61] have implemented quantum resistant ledgers using hash-based [56] schemes and lattice-based [58] schemes respectively to secure DLT systems against quantum computing attacks.

Afkoin will thus, be implemented on one of hash-based or lattice-based schemes.

6. Design Considerations and Characteristics of Afkoin

Drawing from CBDC issuance best practice approaches [38] and the unique requirements of an ECOWAS EMU and single currency programme, we propose the following design considerations

and characteristics of the Afkoin CBDC.

6.1. General

Afkoin will be a quantum-resistant digital currency implemented on a permissioned DLT platform that allows its ecosystem participants (central banks, financial institutions, validating nodes, merchants, and end-users) to use the Internet and other communication protocols to perform transactions among ECOWAS members states and non-member states.

Afkoin will be the primarily means of payments for all current and future services in ECOWAS member states and transactions between ECOWAS Member States and non-member states.

Afkoin will provide mechanisms for the fulfilment of remote and online payments in accordance with electronic and mobile payments laws in ECOWAS member countries.

The Afkoin platform will provide mechanisms for the fulfilment of offline transactions in the event of a disruption to the entire Afkoin platform resulting from natural disasters and un-natural disasters such as power outages which are prevalent in most ECOWAS member countries.

6.2. Generation, Supply and Distribution

The generation and supply of Afkoin will be solely by the WACB in accordance with the "The Statutes of the West African Central Bank" legal statute accented to by ECOWAS Member States.

Afkoin generated by the WACB will be stored in NCB wallets that are created/issued by the WACB.

Afkoin held by PSPs in a given ECOWAS Member State will be stored in wallets created/issued by the corresponding NCB.

The management and distribution of Afkoin from the WACB to PSPs operating in ECOWAS will be performed by National Central Banks (NCBs) that are members of the WACB.

For a given ECOWAS Member State, the distribution, maintenance, validation and authentication of Afkoin transactions within the Member State will be performed by the NCB and PSPs that are counterparties to the given transaction.

All Afkoin transactions will be recorded on a permissioned shared ledger accessible by Afkoin system participants with the right access privileges.

6.3. Functions of Money

Afkoin will perform the three functions of money (namely a unit of account, medium of exchange and a store of value) and will serve as a legal tender for all transactions originating from ECOWAS member countries and terminating in ECOWAS member countries.

Afkoin will perform the three functions of money and will serve as a legal tender for all transactions originating from ECOWAS member countries and terminating in non-ECOWAS member countries and vice versa.

6.4. Convertibility

The convertibility of Afkoin will be at par with the IMF's SDR to eliminate the dependency of the value of Afkoin on a single fiat currency such us the US Dollar or the Euro.

6.5. Convergence Criteria

The implementation of Afkoin will include smart contracts and efficient distributed consensus algorithms with parameters that enable the achievement of the ECOWAS convergence criteria in the medium to long-term.

6.6. Compliance

At all times, the Afkoin platform and its related transactions will strictly adhere to the requirements of the principles for financial market infrastructures[39].

6.7. Usability and Interoperability

Afkoin will be easy to use and accessible by PSPs within and outside the ECOWAS region for the conduct of wholesale interbank payments.

The design of Afkoin will be flexible and extensible for use in current and future services in ECOWAS member countries.

The Afkoin platform will be simple, scalable and integrable with existing financial management infrastructures in ECOWAS and non-ECOWAS member state FMIs where applicable.

6.8. Auditability

Afkoin will be implemented with features for transaction traceability and auditability as required by ECOWAS Member State monetary regulations.

6.9. Security

At all material times, Afkoin will be imbued with the best available security solutions that guarantees the safety and protection of Afkoin user information and transaction data so as to instill confidence in the Afkoin platform and promote the quick adoption of Afkoin across the ECOWAS region.

6.10. Efficiency

As the target users of Afkoin is the entirety of ECOWAS and its trading partners, the Afkoin platform will be able to concurrently handle transactions of orders of magnitude $10\hat{x}$ and at speeds superior or comparable to the most efficient transaction processing systems or FMIs in the world over the medium to long term.

6.11. AML/CTF and KYC

Afkoin will be implemented with features that enable the prevention of money laundering and terror-financing within the borders of ECOWAS and the borders of non-member state economies that trade with ECOWAS.

Afkoin will be implemented with efficient identity management mechanisms and features that comply with global accepted know-your-customer regulations.

7. Conclusion and Future Work

In the papers [38], [70], [71], we examined best practice approaches and the technical feasibility of leveraging DLT for CBDC issuance. We identified *well-defined goals*, *multistakeholderism* and *technology* as key practices that enabled successful CBDC experiment outcomes.

Our future work will leverage the lessons learned in [38], [70], [71] to undertake the technical design and implementation of Afkoin within the defined scope in this paper.

Structurally, the issuance of Afkoin will follow the logical architecture presented in Fig. 11.

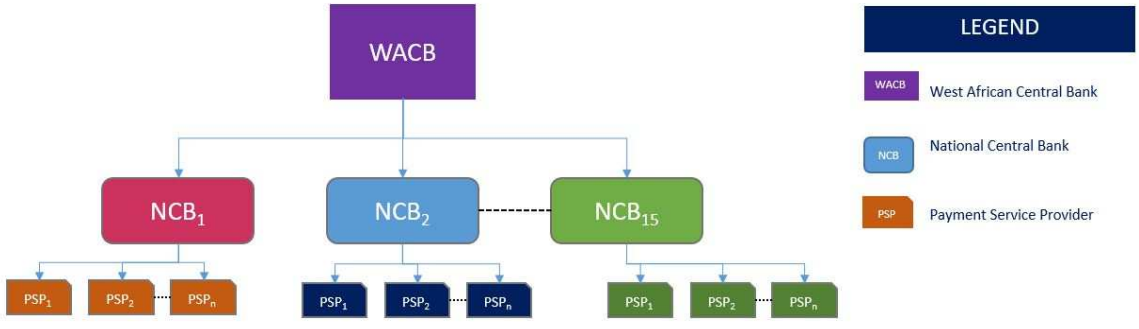


Fig. 11. Afkoin Issuance Logical Architecture

References

[1] ECOWAS, "Treaty of the Economic Community of West African States (ECOWAS)," United Nations - Treaty Series, Lagos, 1976. Available: https://treaties.un.org/doc/Publication/UNTS/Volume%201010/v1010.pdf.

[2] ECOWAS Commission, "Revised ECOWAS Treaty," ECOWAS Commission, Abuja, 1993. Available: http://www.ecowas.int/wp-content/uploads/2015/01/Revised-treaty.pdf.

[3] WAMI, "Accra Declaration," Available: http://www.wami-imao.org/sites/default/files/Accra%20Declaration.docx.

[4] WAMI, "Welcome to WAMI," West African Monetary Institute, [Online]. Available: http://www.wami-imao.org/.

[5] J. Acheampong, "WAMI abandons ECO for new currency," Graphic Online, 8 September 2015. Available: https://www.graphic.com.gh/business/business-news/wami-abandons-eco-for-new-currency.html.

[6] F. Bakoup and D. Ndoye, "Why and when to introduce a single currency in ECOWAS," Africa Economic Brief, vol. 7, no. 1, pp. 1-16, 2016.

[7] S. K. Harvey and M. J. Cushing, "Is West African Monetary Zone (WAMZ) a common currency area?," Review of Development Finance, vol. 5, no. 1, pp. 53-63, 23 June 2015.

[8] UEMOA, "About UEMOA," Available: http://www.uemoa.int/en/about-uemoa

[9] European Commission, "Pascal Lamy to visit West Africa to prepare the launch of negotiations for an Economic Partnership Agreement," 23 April 2003. European Commission. Available: http://europa.eu/rapid/press-release_IP-03-559_en.htm.

[10] M. B. Saho, "The Institutional Framework for ECOWAS Monetary Union," June 2018. West African Monetary Agency. Available: http://amao-wama.org/wp-content/uploads/2018/06/MB-SAHO-ECOWAS-PARLIAMENT-ENG.pdf.

[11] ECOWAS Commission, "Fifth Meeting Of The Task Force On The ECOWAS Single Currency Programme," ECOWAS, 21 February 2018. Available: http://www.ecowas.int/fifth-meeting-of-the-task-force-on-the-ecowas-single-currency-programme/.

[12] ECOWAS Commission, "Terms of Reference for the Competition on the ECOWAS Single Currency Name and Logo," Bank of Ghana. 16 October 2018. Available: https://www.bog.gov.gh/privatecontent/Public_Notices/Notice%20-%20Competition%20on%20the%20Ecowas%20Single%20Currency%20Name%20and%20Logo.pdf.

[13] UNECA, "Regional integration in West Africa: challenges and prospects," 21st Session of the Intergovernmental Committee of Experts. United Nations Economic Commission for Africa. 27-29 June 2018. Available: https://www.uneca.org/sites/default/files/uploaded-documents/SROs/WA/ice21/issue_paper_regional_integration_challenges_and_prospects_final_en.pdf.

[14] ECOWAS Commission, "2016 ECOWAS Convergence Report," ECOWAS Commission, Abuja, 2017. Available: https://www.ecowas.int/wp-content/uploads/2017/11/2016-Convergence-report_Clean-final-final.pdf?biecjmoppphlngdb.

[15] Worldometer, "Western Africa Population," Worldometer 10 November 2018. [Online]. Available: http://www.worldometers.info/world-population/western-africa-population/.

[16] ECOWAS Commission, "Member States," ECOWAS Commission. Available: https://www.ecowas.int/member-states/.

[17] GSMA Intelligence, "The Mobile Economy West Africa 2019," GSMA. Available: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_West_Africa_ENG.pdf.

[18] European Invest Bank, "Banking in sub-Saharan Africa: Interim Report on Digital Financial Inclusion," 2017. European Invest Bank. Available: https://www.eib.org/attachments/efs/economic_report_banking_africa_interim_2017_en.pdf.

[19] A. Demirgüç-Kunt, L. Klapper, D. Singer, S. Ansar and J. Hess, "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution," 2018. World Bank Group. Available: http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf

[20] Payment Systems Department, "Payment Systems Oversight Annual Report, 2017," Bank of Ghana. Available: https://www.bog.gov.gh/wp-content/uploads/2019/08/Payment-Systems-Annual-Report-2017.pdf.

[21] Bureau of Engraving and Printing, "How Money is Made," U.S. Department of the Treasury. Available: https://www.moneyfactory.gov/uscurrency/howmoneyismade.html.

[22] US Department of Treasury, "Distribution of Currency and Coins," US Department of Treasury. Available: https://www.treasury.gov/about/education/Pages/distribution.aspx.

[23] Sveriges Riksbank, "The Riksbank's e-krona project (Report 1)," September 2017. Sveriges Riksbank. Available: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf.

[24] New York Fed, "How Currency Gets into Circulation." July 2013. Federal Reserve Bank of New York. Available: https://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html.

[25] The Fed, "2019 Federal Reserve Note Print Order," 9 August 2018. US Federal Reserve System. Available: https://www.federalreserve.gov/foia/files/2019currency.pdf.

[26] BBC, "Italy: Minting euro cents 'costs four times their value'," 5 November 2013. BBC. Available: https://www.bbc.com/news/blogs-news-from-elsewhere-24819165.

[27] R. Koenig, "Printing Money vs Digital Money," Coinmonks, 18 November 2017. Available: https://medium.com/coinmonks/printing-money-vs-digital-money-1b4e29a498f4.

[28] R. Auer, G. Cornelli and J. Frost, "Covid-19, cash, and the future of payments," BIS Bulletin No.3. April 2020. BIS. Available: https://www.bis.org/publ/bisbull03.pdf.

[29] Bloomberg News, "China Quarantines Cash to Sanitize Old Bank Notes From Virus," February 15, 2020. Bloomberg. Available: https://www.bloomberg.com/news/articles/2020-02-15/china-quarantines-cash-to-sanitize-old-bank-notes-from-virus.

[30] P. Schroeder and A. Irrera, “Fed quarantines U.S. dollars repatriated from Asia on coronavirus caution,” 6 March 2020. Reuters. Available: https://www.reuters.com/article/us-health-coronavirus-fed-dollars/fed-quarantines-us-dollars-repatriated-from-asia-on-coronavirus-caution-idUSKBN20T1YT.
[31] W. Engert and B. S. C. Fung, ”Central Bank Digital Currency: Motivations and Implications,” Bank of Canada, Ottawa, 2017.
[32] M. Bech and J. Hancock, ”Innovations in payments,” BIS Quarterly Review, March 2020. BIS. Available: https://www.bis.org/publ/qtrpdf/r_qt2003f.pdf.
[33] IMF, ”Special Drawing Right (SDR),” International Monetary Fund. Available: https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR.
[34] WAMI, ”WAMZ Agreement,” WAMI. Available: http://www.wami-imao.org/sites/default/files/WAMZ%20Agreement.docx.
[35] West African Monetary Agency, ”ABOUT WAMA,” [Online]. Available: https://amao-wama.org/aboutus/.
[36] Payment Systems Department, ”Payment Systems Oversight Annual Report, 2018,” Bank of Ghana. Available: https://www.bog.gov.gh/wp-content/uploads/2019/10/Payment-Systems-Annual-Report-2018-Final-Version_PUBLICATION.pdf.
[37] Payment Systems Department, ”Payment Systems Oversight Annual Report, 2015,” Bank of Ghana. Available: https://www.bog.gov.gh/wp-content/uploads/2019/08/Ghanas-Payment-Systems-Report-2015.pdf.
[38] E. A. Opare and K. Kim, ”A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures,” in IEEE Access, vol. 8, pp. 110810-110847, 2020, doi: 10.1109/ACCESS.2020.3001970.
[39] BIS, ”Principles for financial market infrastructures ”, April 2012. BIS. Available: https://www.bis.org/cpmi/publ/d101a.pdf.
[40] G. Levy, ”SPEAK BLOCKCHAIN: Become Fluent in Blockchain and Bitcoin,” Blockchain Institute of Technology, 2017.
[41] M. Castro and B. Liskov, ”Practical Byzantine Fault Tolerance,” Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999. Available: http://pmg.csail.mit.edu/papers/osdi99.pdf.
[42] R. Saltini and D. Hyland-Wood, ”Correctness Analysis of Istanbul Byzantine Fault Tolerance,” ConsenSys. August 28, 2019. Available: https://arxiv.org/pdf/1901.07160.pdf.
[43] P. Jain, ”The ABCs of Kafka in Hyperledger Fabric,” CodeBurst. Available: https://codeburst.io/the-abcs-of-kafka-in-hyperledger-fabric-81e6dc18da56.
[44] D. Ongaro and J. Ousterhout, ”In Search of an Understandable Consensus Algorithm (Extended Version),” Stanford University. May 20, 2014. Available: https://raft.github.io/raft.pdf.
[45] JP Morgan Chase, ”Quorum Whitepaper v0.2.pdf,” 24 August, 2018. [Online]. Available: https://github.com/jpmorganchase/quorum/blob/master/docs/Quorum%20 Whitepaper%20v0.2.pdf.
[46] T. Kuhrt. ”Hyperledger Fabric.” Hyperledger Fabric. https://wiki.hyperledger.org/display/fabric.
[47] R3. ”Nodes-R3 Corda Master Documentation.” Available: https://docs.corda.net/key-concepts-node.html.
[48] Institute for Quantum Computing, ”Quantum computing 101,” University of Waterloo. Available: https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101#What-is-quantum-computing
[49] IBM, ”What is quantum computing?,” IBM. Available: https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/
[50] M. Mosca, ”Cybersecurity in an era with quantum computers: will we be ready?,” in Cryptology ePrint Archive, Report 2015/1075, 2015.
[51] M. Mosca and V. Gheorghiu, ”The Quantum Threat: What Really Matters Today?,” Security Education Conference Toronto , p. 24, 15 November 2017.
[52] P. W. Shor, ”Algorithms for quantum computation: discrete logarithms and factoring,” in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.
[53] M. Mimoso, ”NSA’s Divorce from ECC Causing Crypto Hand-Wringing,” Threatpost, 23 October 2015. [Online]. Available: https://threatpost.com/nsas-divorce-from-ecc-causing-crypto-hand-wringing/115150/.
[54] P. Waterland, ”Quantum Resistant Ledger (QRL),” November 2016. Available: https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf.
[55] M. Milicevic, C. Feng, L.M. Zhang, and P.G. Gulak, ”Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography,” npj Quantum Information (2018) 4:21 ; doi:10.1038/s41534-018-0070-6
[56] L. Lamport, ”Constructing Digital Signatures from a One-Way-Function,” SRI International, 18 October 1979. Available: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf.
[57] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto and T. Schroeter, ”Blockchained Post-Quantum Signatures,” IEEE Conferences, pp. 1196-1203, 2018.
[58] D. Micciancio and O. Regev, ”Lattice-based Cryptography,” Post-Quantum Cryptography , pp. 147-191, 2009.
[59] V. Lyubashevsky, ”Preparing for the Next Era of Computing With Quantum-Safe Cryptography,” SecurityIntelligence, 26 October 2016. Available: https://securityintelligence.com/preparing-next-era-computing-quantum-safe-cryptography/.
[60] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu and Y.-X. Yang, ”A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain,” IEEE Access, vol. 6, pp. 27205 - 27213, 2018.
[61] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou and J. Li, ”A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network,” IEEE Access, vol. 7, pp. 2026 - 2033, 2019.
[62] S. Nakamoto. ”Bitcoin P2P e-cash paper.” Available: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.
[63] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System,” October 31, 2008. Available: https://bitcoin.org/bitcoin.pdf.
[64] S. Seebacher and R. Schüritz, ”Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review,” Cham, 2017: Springer International Publishing, in Exploring Services Science, pp. 12-23.

[65] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLOS ONE, vol. 11, no. 10, p. e0163477, 2016, doi: 10.1371/journal.pone.0163477.
[66] V. Buterin, "Proof of Stake FAQ." Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.
[67] V. Buterin, "A Proof of Stake Design Philosophy." Available: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51.
[68] NIST, Blockchain Technology Overview, NISTIR 8202, October 3, 2018. Available: https://csrc.nist.gov/publications/detail/nistir/8202/final.
[69] S. Nakamoto. "Bitcoin v0.1 released." Available: https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.
[70] E.A. Opare and K. Kim, "Understanding Nine Central Bank Digital Currency Experiments Selected from the World", Conference on Information Security and Cryptography-Winter 2019 (CISC-W '19), Nov. 30, 2019, Seoul, Korea.
[71] E.A. Opare and K. Kim, "Design Practices for Wholesale Central Bank Digital Currencies from the World", 2020 Symposium on Cryptography and Information Security (SCIS2020), Jan. 28-31, 2020, Kochi, Japan.