박 사 학 위 논 문
Ph.D. Dissertation

Afkoin: 서아프리카 경제 공동체를 위한 분산 원장 기술 기반의 양자 내성 중앙은행 디지털 화폐

Towards Afkoin: A Distributed Ledger Technology-Based Quantum Resistant Central Bank Digital Currency for the Economic Community of West African States

2021

오파레 에드윈 아이시 (Opare, Edwin Ayisi)

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

박 사 학 위 논 문

Afkoin: 서아프리카 경제 공동체를 위한 분산 원장 기술 기반의 양자 내성 중앙은행 디지털 화폐

2021

오파레 에드윈 아이시

한 국 과 학 기 술 원

기술경영학부 (글로벌IT기술대학원프로그램)

Afkoin: 서아프리카 경제 공동체를 위한 분산 원장 기술 기반의 양자 내성 중앙은행 디지털 화폐

오파레 에드윈 아이시

위 논문은 한국과학기술원 박사학위논문으로
학위논문 심사위원회의 심사를 통과하였음

2020년 12월 14일

심사위원장 Kwangjo Kim (인)

심 사 위 원 Jun Kyun Choi (인)

심 사 위 원 Myungchul Kim (인)

심 사 위 원 Seunghun Han (인)

심 사 위 원 Youngsun Kwon (인)

Towards Afkoin: A Distributed Ledger Technology-Based Quantum Resistant Central Bank Digital Currency for the Economic Community of West African States

Edwin Ayisi Opare

Advisor: Kwangjo Kim

A dissertation submitted to the faculty of
Korea Advanced Institute of Science and Technology in
partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Business and Technology Management (Global Information and Telecommunication Technology)

Daejeon, Korea
December 14, 2020

Approved by

Kwangjo Kim
Professor of School of Computing

The study was conducted in accordance with Code of Research Ethics[1].

[1] Declaration of Ethical Conduct in Research: I, as a graduate student of Korea Advanced Institute of Science and Technology, hereby declare that I have not committed any act that may damage the credibility of my research. This includes, but is not limited to, falsification, thesis written by someone else, distortion of research findings, and plagiarism. I confirm that my thesis contains honest conclusions based on my own careful research under the guidance of my advisor.

DITP
20165644

오파레에드윈 아이시. Afkoin: 서아프리카 경제 공동체를 위한 분산 원장 기술 기반의 양자 내성 중앙은행 디지털 화폐. 기술경영학부 (글로벌IT기술대학원프로그램) . 2021년. 120+vi 쪽. 지도교수: 김광조. (영문 논문)
Edwin Ayisi Opare. Towards Afkoin: A Distributed Ledger Technology-Based Quantum Resistant Central Bank Digital Currency for the Economic Community of West African States. School of Business and Technology Management (Global Information and Telecommunication Technology Program) . 2021. 120+vi pages. Advisor: Kwangjo Kim. (Text in English)

초 록

전 세계의 많은 중앙 은행이 분산 원장 기술(DLT) 기반 중앙 은행 디지털 통화(CBDC) 발행에 대한 연구와 실험을 시작했습니다. 일반적으로 이러한 연구의 목표는 금융 시장 인프라의 보안, 탄력성 및 효율성을 개선하기 위해 DLT의 잠재력을 탐구하는 것이었습니다. 우리는 완전한 개념 증명 프로토 타입과 관련된 CBDC 실험의 모범 사례 접근 방식을 활용하여 서아프리카 경제 공동체(Economic Community of West African States, ECOWAS) 단일 통화 프로그램의 가능한 솔루션으로 DLT 기반 CBDC를 제안하고 개발을 시작하였습니다. ECOWAS는 1975년 5월 라고스 협약을 통해 설립 된 서아프리카의 15개 회원국 지역 경제 공동체입니다. 1993년 7월 ECOWAS 회원국은 베냉 코토누에서 개정된 ECOWAS 협약을 비준했습니다. 코토누 협약은 ECOWAS 하위 지역에서 단일 통화를 발행할 목적으로 ECOWAS 회원국간에 경제 및 통화 연합을 만들 것을 제안했습니다. 2000년 4월, ECOWAS 회원국은 2003년까지 ECO라고 하는 ECOWAS 단일 통화 발행 절차를 시작하기 위해 아크라 선언으로 알려진 법령을 비준했습니다. 지금까지 ECOWAS는 ECO 단일 통화를 발행 할 수 없었습니다. 이 연구에서는 ECOWAS 단일 통화 프로그램의 가능한 솔루션으로 DLT 기반 양자 내성 CBDC인 Afkoin의 개발을 제안하고 시작합니다. 우리는 제안된 Afkoin CBDC의 예비 설계 고려 사항 및 특성을 제시하고 하이퍼레저 패브릭 승인된 DLT 플랫폼에서 Afkoin CBDC 프로토 타입 개발을 안내하는 기술 요구 사항 사양을 개발합니다. 본 연구에서 제안한 Afkoin CBDC는 Afkoin 생태계 참여자들 사이의 국내 은행 간 거래 정산을 위한 대규모의 CBDC로 설계되었습니다. Afkoin CBDC 생태계 참여자에는 가상의 서아프리카 중앙 은행, 대표적인 ECOWAS 국립 중앙 은행인 가상의 가나 은행, 가나의 국내 도매 결제 시스템에 참여하는 상업 은행과 같은 가상 결제 서비스 제공 업체가 포함됩니다. Afkoin CBDC 플랫폼은 사용자 관리, 지갑 생성, Afkoin 생성, 자금 이체, 서약 및 Afkoin 토큰 사용을 위한 기능으로 설계되었습니다. 또한 기본 분산 트랜잭션 원장의 잔액 조회 및 버전 관리 기능은 Afkoin CBDC 프로토 타입의 디자인에서 고려됩니다. Afkoin은 ECOWAS 회원국에 의해 채택된 경우 ECOWAS 회원국의 자산에 대한 청구를 대리합니다. 따라서 Afkoin은 돈의 세 가지 기능, 즉 계정 단위, 교환 매체 및 가치 저장을 수행하며 ECOWAS 회원국 간의 거래에 대한 법적 입찰 역할을 합니다. 또한 Afkoin은 ECOWAS 회원국과 비회원국 간의 거래에 대한 법적 입찰 역할을 할 수 있을 것입니다. Afkoin은 화폐로써의 기능을

수행하고, ECOWAS 회원국이 채택하는 경우 ECOWAS 회원국의 자산에 대한 청구를 대리합니다.

핵 심 낱 말 Afkoin, 중앙은행 디지털 화폐, ECOWAS, Hyperledger Fabric, 양자 내성, 단일 통화 CBDC.

Abstract

Many central banks across the world have begun research and experimentation into the issuance of distributed ledger technology (DLT)-based central bank digital currencies (CBDCs). In general, the goal of such research has been to explore the potential of DLT to improve the security, resiliency and efficiency of financial market infrastructures. We leverage best practice approaches from relevant CBDC experiments with completed proof-of-concept prototypes to propose and initiate the development a DLT-based CBDC as a candidate solution for the Economic Community of West African States (ECOWAS) single currency program.

ECOWAS is a fifteen member State regional economic community in West Africa established in May 1975 through the Lagos Treaty. In July 1993, ECOWAS member States ratified a revised ECOWAS Treaty in Cotonou, Benin. The Cotonou Treaty proposed to create an economic and monetary union among ECOWAS member States with the goal of issuing a single currency in the ECOWAS sub-region. In April 2000, ECOWAS member States ratified a legal statute known as the Accra Declaration to begin processes for the issuance of an ECOWAS single currency called the ECO by the year 2003. To date, ECOWAS has been unable to issue the ECO single currency.

In this research, we propose and initiate the development Afkoin, a DLT-based quantum resistant CBDC as a candidate solution for the ECOWAS single currency program. We present preliminary design considerations and characteristics of our proposed Afkoin CBDC and develop a technical requirement specification to guide the development of the Afkoin CBDC prototype on the Hyperledger Fabric permissioned DLT platform.

The Afkoin CBDC proposed in this research is designed as a wholesale CBDC for domestic interbank transaction settlement among Afkoin ecosystem participants. The Afkoin CBDC ecosystem participants include an imaginary West African Central Bank, a virtual Bank of Ghana as a representative ECOWAS National Central Bank, and virtual Payment Service Providers such as commercial banks that are participants in Ghana's domestic wholesale payment settlement system. The Afkoin CBDC platform is designed with capabilities for User Management, Wallet Creation, Afkoin Creation, Funds Transfer, Pledge, and Redeem of afkoin tokens. Additionally, capabilities for Balance Enquiry and Versioning of the underlying distributed transaction ledger are accounted for in the design of the Afkoin CBDC prototype.

Afkoin will represent a claim on the assets of ECOWAS member States if and when it is adopted by ECOWAS member States. Afkoin will thus perform the three functions of money namely, a unit of

account, a medium of exchange, and a store of value; and will serve as legal tender for transactions between ECOWAS member States. Additionally, Afkoin will serve as legal tender for transactions between ECOWAS member States and non-member States.

Keywords Afkoin, CBDC, ECOWAS, Hyperledger Fabric, single currency, quantum resistant CBDC.

Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1 Economic Community of West African States

The Economic Community of West African States (ECOWAS) [16] is a fifteen member State regional economic community in West Africa established in May 1975 in Lagos, Nigeria, to "*promote co-operation and development in all fields of economic activity*" [1] 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 a monetary union, 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.

The current membership of ECOWAS can be grouped into eight French-speaking countries, five English-speaking countries and two Portuguese-speaking countries as presented in Figure 1.1.

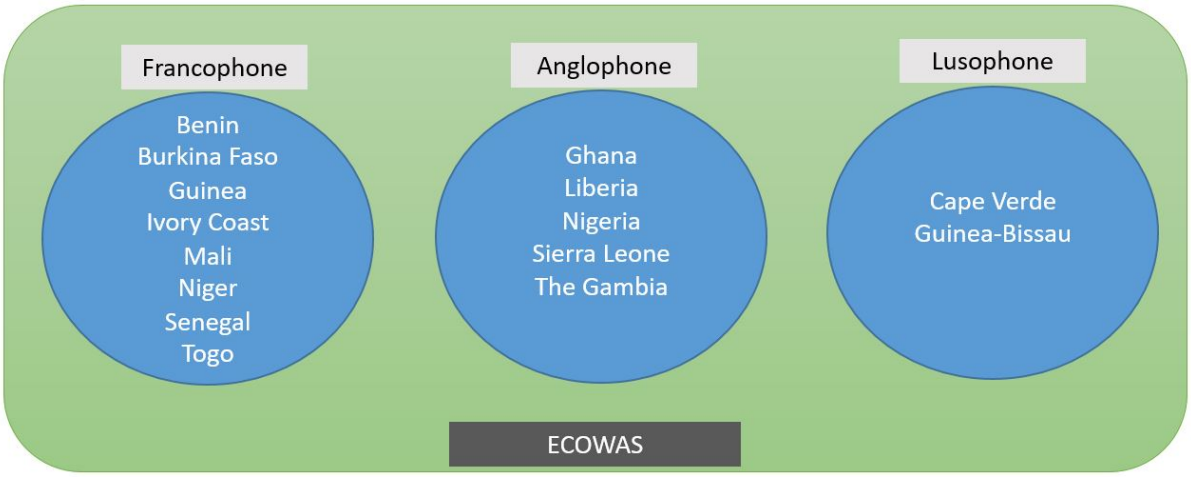


Figure 1.1: ECOWAS Regional Grouping by Spoken Language

1.2 ECOWAS Single Currency Program

To establish an ECOWAS economic and monetary union (EMU) and issue a single currency in ECOWAS, ECOWAS member States proposed to implement the ECOWAS EMU in two phases [7].

ECOWAS proposed to create two EMUs along currency-lines and merge both EMUs in the long term [4].

A number of ECOWAS member States shared a common currency, the *CFA-Franc* while other member States had individual currencies [7]. 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.

The membership of WAEMU consists of seven Francophone countries namely Benin, Burkina Faso, Ivory Coast, Mali, Niger, Senegal and Togo. Guinea-Bissau, a lusophone country joined WAEMU as its eighth member State in May 1997 [8].

The main objective of UEMOA was to establish a customs union and adhere to a common economic and monetary policy within the UEMOA 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 *Accra Declaration* [3] enacted in April 2000. WAMZ consists of five member States namely, Ghana, Guinea, Liberia, Nigeria, Sierra Leone and the Gambia. Liberia joined the WAMZ as its sixth member State in February 2010 [3].

The composition of the WAEMU and WAMZ member States is presented in Fig.1.2.

Currently, Cape Verde does not belong to any of the two ECOWAS EMUs and is therefore excluded from the EMU grouping in Figure 1.2.

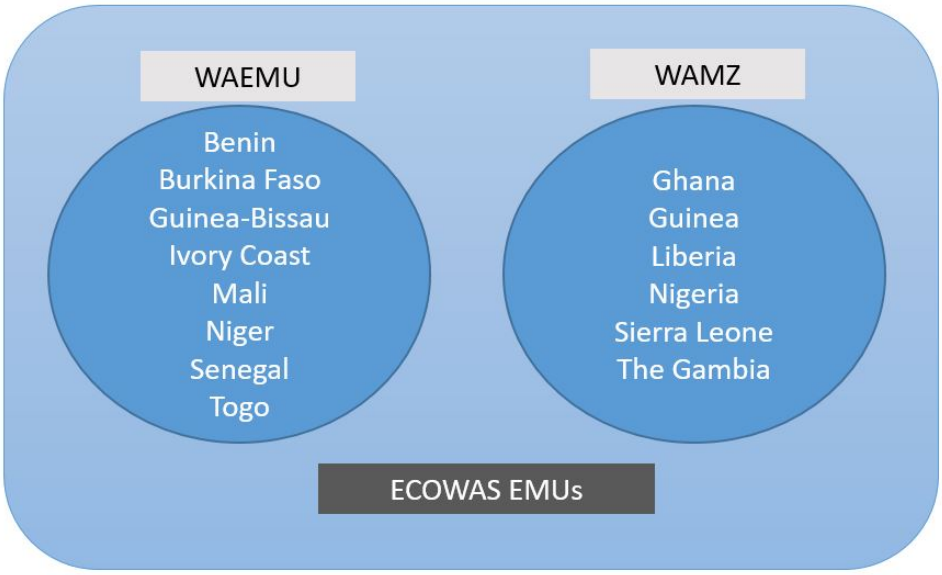


Figure 1.2: ECOWAS Regional Grouping by EMU

ECOWAS member States without a common currency signed the *Accra Declaration* [3] in April 2000 to establish the West African Monetary Zone (WAMZ).

The main goal of the Accra Declaration was to establish the WAMZ as a legal entity and provide

modalities for the establishment of a common ECOWAS central bank [3].

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].

The economic convergence criteria defined in the Accra Declaration is presented Figure 1.3.

Primary Criteria
Budget deficit (excluding grants) to GDP ratio: $\leq$ 5% by 2000 and $\leq$ 4% by 2002.
Annual average inflation: $\leq$ 10% by the year 2000 and $\leq$ 5% by 2003.
Central bank financing of budget deficit: $\leq$ 10% of previous year's tax revenue.
Gross external reserves: $\geq$ 3 months of import by end of 2000 and $\geq$ 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: $\leq$ 35%.
Tax revenue to GDP ratio: $\geq$ 20 percent.
Real interest rate: $>$ 0%.
Stability of the nominal exchange rate: +/-10%.
Public investments to tax revenue: $\geq$ 20%.

Figure 1.3: ECOWAS Convergence Criteria [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 convergence criteria by December 2019. The revised convergence criteria is presented in Figure 1.4.

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

The ECOWAS Commission, the institution responsible for the day-to-day running of ECOWAS

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

Figure 1.4: Revised ECOWAS Convergence Criteria [10]

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 established best practice approaches for central bank digital currency (CBDC) issuance, ECOWAS may be able to efficiently issue a single currency in West Africa.

We propose for the new ECOWAS single currency to be called *Afkoin*. We propose for the Afkoin CBDC to be DLT-based and quantum resistant. Specifically, we propose for the first phase of the Afkoin CBDC platform to be implemented using the Hyperledger Fabric permissioned DLT platform due to its modular structure and use of general-purpose programming languages such as Java, Go and Node.js.

Afkoin, if and when adopted by ECOWAS will represent a claim on the assets of ECOWAS member States. Afkoin will perform the functions of money and thus can be used to make payments in ECOWAS.

1.3 Objective

The key objective of this research is to enable the efficient and expedient issuance of the ECOWAS single currency using DLT. Consequently, we design, develop and propose a DLT-based CBDC framework to achieve our stated research objective.

1.4 Rationale for Afkoin

In this section, we present our rationale for the Afkoin CBDC. The rationale presented is non-exhaustive.

1.4.1 Algorithmically Achieve The Convergence Criteria

The revised ECOWAS convergence criteria (Figure 1.4) required that by December 2019, each 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; and
- 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 in its presentation that no ECOWAS member State had been able to fully achieve the convergence criteria [13].

In Figure 1.5, 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.

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.1.5. 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.

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

Figure 1.5: ECOWAS Convergence Criteria Compliance from 2005-2016 [13]

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.

1.4.2 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 Figure 1.6.

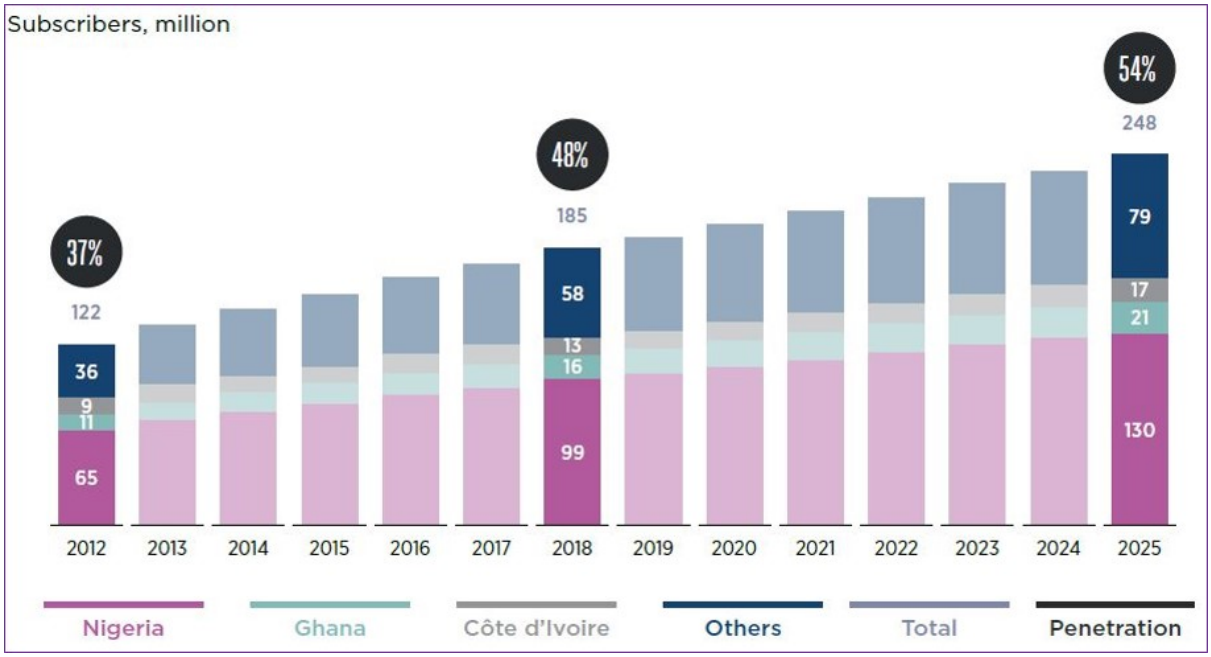


Figure 1.6: Unique Mobile Subscription Trend in ECOWAS [15]

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 Figure 1.7.

For a majority of the inhabitants of ECOWAS, mobile phones are the primary means by which they

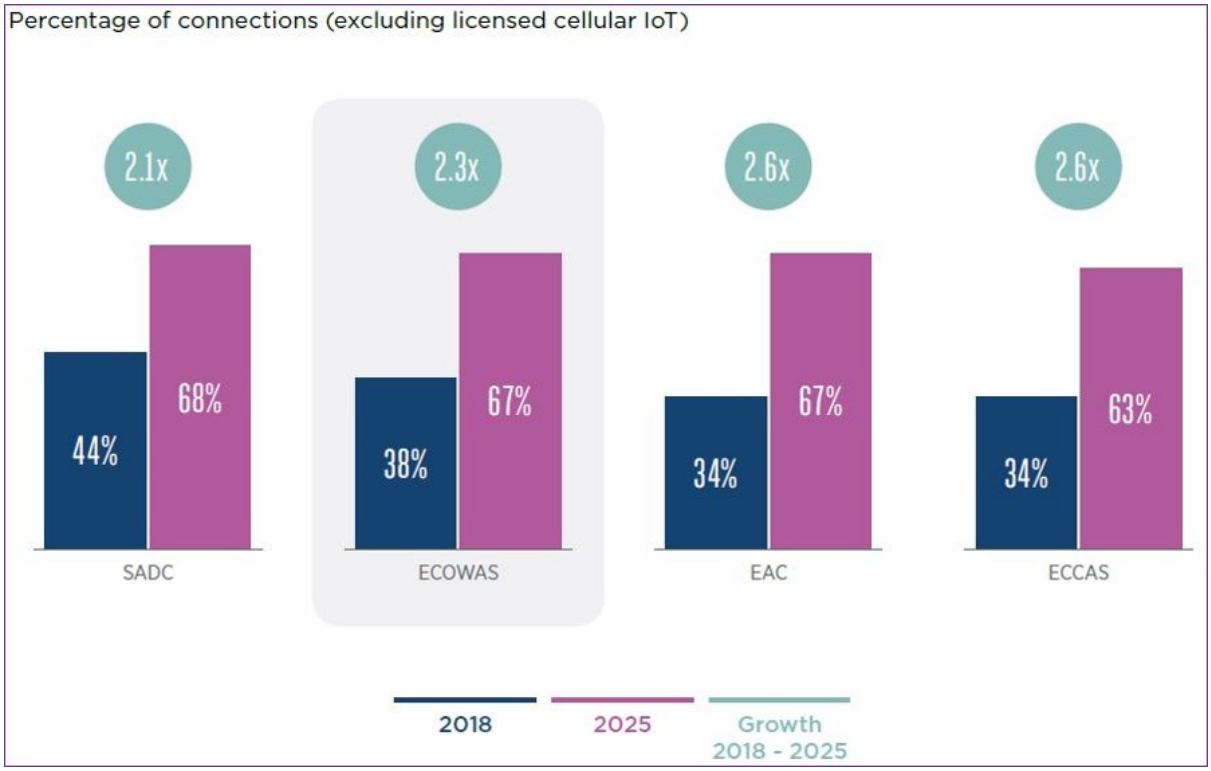


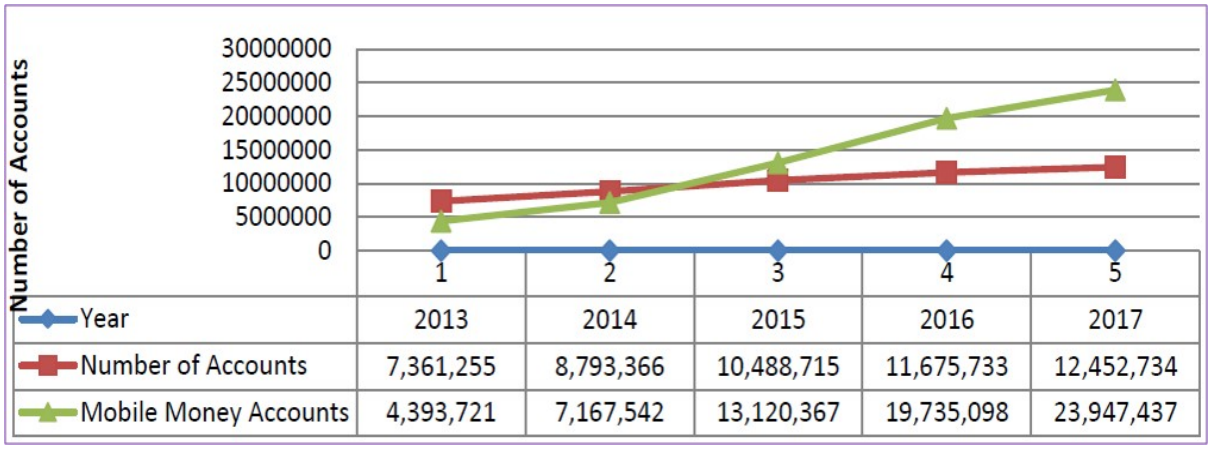
Figure 1.7: ECOWAS Mobile Internet Connection Rate via Smartphones [15]

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 [15]. The GDP contribution of mobile-based services in West Africa is expected to grow to 9.5% by 2023 [15].

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 ECOWAS sub-region [15].

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 [15]. 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 Figure 1.8.

To continuously increase and deepen financial inclusion for the unbanked, unserved and underserved populations of ECOWAS, issuing a paper-based currency may erode the financial inclusion gains attained



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

Figure 1.8: Formal Bank Account Versus Mobile Money Account Subscription Trend in Ghana [20]

in ECOWAS over the last decade.

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

1.4.3 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 Figure 1.9.

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 meth-

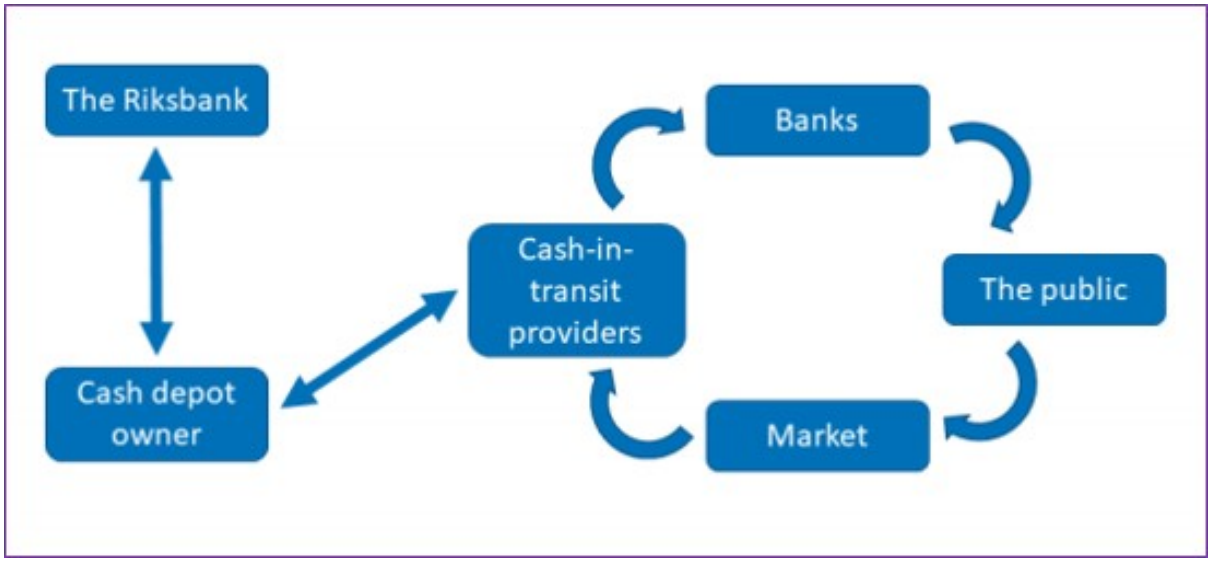


Figure 1.9: Cash Distribution Process in Sweden [23]

ods 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, RD, 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.

1.4.4 Existing Payment Mechanisms Are Unsafe

In the paper *Covid-19, cash, and the future of payments* [28], the Bank for International Settlements 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 Bank for International Settlements (BIS) underscores that there are no recorded cases of COVID-19 transmission through cash although some central banks have 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 Figure 1.10.

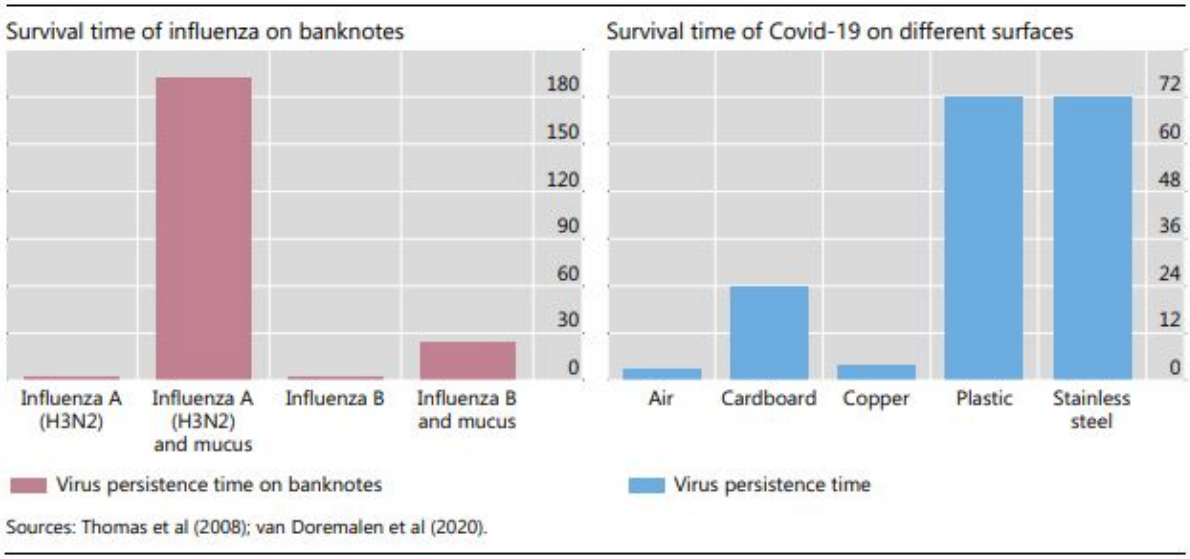


Figure 1.10: Survival of Viruses on Multiple Surfaces in Hours [28]

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 research, we present Afkoin, a DLT-based quantum-resistant CBDC for ECOWAS.

1.5 Scope

Two types of payment systems are defined in literature namely, retail payment systems and wholesale payment systems [39].

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 (PSPs) such as commercial banks (CMBs) and other high-value customers [40]. Access to a wholesale payment system is restricted to only PSPs [39]. 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 [40]. Following the payment system innovation trend, the Afkoin CBDC discussed in this thesis focuses on Afkoin as a domestic wholesale CBDC infrastructure. Future implementations of the Afkoin CBDC will include capabilties for retail and cross-border transaction settlement.

We refer to the entire Afkoin CBDC infrastructure as the *Afkoin platform* or *Afkoin*; and the digital currency transacted on the Afkoin platform as *afkoins* or *afkoin tokens*.

The scope of the capabilties of our proposed Afkoin CBDC platform is as follows:

- Capabilities for the issuance of afkoin tokens.
- Capabilities for domestic wholesale interbank settlement of afkoin tokens.
- Capabilities that enable Afkoin platform PSP participants pledge collateral to an ECOWAS National Central Bank in exchange for afkoin tokens.
- Provision mechanisms that guarantee counterparty data privacy and settlement finality of afkoin tokens on the Afkoin platform.

Implementing the Afkoin CBDC within a limited geographical area and within the context of a regulatory sandbox will enable the rapid assessment and evaluation of the suitability of DLT to achieve the objective of this research. As a result, the Afkoin CBDC prototype is designed in line with the wholesale payment system requirements in the Republic of Ghana. Ghana is one of the economically

vibrant and politically stable countries in ECOWAS. Ghana's wholesale payment infrastructure is called the Ghana Interbank Settlement (GIS) system. Ghana's GIS system is owned and operated by the Bank of Ghana (BOG) [19].

All design and implementation decisions about the Afkoin CBDC proposed in this research are based on a combination of current CBDC research best practice approaches such as those discussed in [146]; an extensive survey of existing ECOWAS single currency legal statutes; and a review of Ghana's GIS system operational requirements [20]. The ECOWAS single currency legal statutes and the GIS system operational requirements are discussed in subsequent sections of this chapter.

1.6 ECOWAS Single Currency Organizations and Legal Statutes

To facilitate the establishment of an ECOWAS EMU and issuance of a single currency, various regional organizations and legal statutes have been ratified in ECOWAS. The relevant ECOWAS regional organizations and legal statutes that are applicable to the design and development of the Afkoin CBDC are discussed in this section.

1.6.1 Legal Statutes

ECOWAS member States proposed to implement a West Africa-wide monetary union in two stages as discussed in section 1.2. To achieve its intended objectives, ECOWAS member States signed the *Accra Declaration* [3] in April 2000 to establish the West African Monetary Zone (WAMZ). The main goal of the Accra Declaration was to establish the WAMZ as a legal entity and provide modalities for the issuance of the ECO single currency by January 2003 [3].

Following the ratification of the Accra Declaration by ECOWAS, member States passed the West African Monetary Zone (WAMZ) Agreement in December 2000 to provide the legal, administrative and institutional framework for the establishment of WAMZ. WAMZ is generally referred to as the Zone.

The WAMZ Agreement further established six key institutions to enable the achievement of the ECOWAS single currency objective. The core responsibility of each institution is presented below.

- ***Authority of Heads of State and Government*** is the political and highest decision-making body of the Zone, with the overall responsibility for the achievement of the objectives of the WAMZ.
- ***Convergence Council*** is the second highest legal entity in the Zone after the Authority of Heads of State and Government. The Convergence Council is responsible for supervising all the institutions and activities of the Zone.
- ***West African Central Bank (WACB)*** is established as a Common Central Bank of the Zone with responsibility for monetary policy administration and single currency issuance.

- ***West African Monetary Institute (WAMI)*** is a legal entity with responsibility for the implementation of the functions and activities leading to the establishment of the WACB.
- ***Stabilization and Cooperation Fund (SCF)*** is established to provide temporary financial assistance to WAMZ member States in order to attain the Convergence Criteria enshrined in the Accra Declaration.
- ***Technical Committee*** is a technical arm responsible for collaboration with WAMI to coordinate policies that would lead to the achievement of the goals of the WAMZ Agreement.

Of the six institutions established under the WAMZ Agreement, the role of WAMI is deemed the most critical to achieving the ECOWAS single currency objective as WAMI is primarily tasked with the implementation of the *Statutes of the WACB* [17] accented to by ECOWAS member States. The Statutes of the WACB describes the role and responsibilities of the WACB in the Zone.

1.6.2 Relevant Articles of the Statutes of the WACB

Key articles relevant for the design and development of the Afkoin CBDC are presented below.

Article 6: Functions of the WACB

The main functions of the WACB shall be to:

- Issue a common convertible currency within the WAMZ;
- Define and implement the monetary policy of the WAMZ;
- Conduct foreign exchange operations consistent with the provisions and objectives of price stability;
- Hold and manage the official foreign reserves of the member States;
- Promote the smooth operation of payment systems;
- Serve as banker to financial institutions and fiscal agents to government;
- Exercise prudential supervision over credit and financial institutions.

Article 16: Functions of the National Central Banks

The National Central Banks (NCBs) shall perform the following functions in their territories:

- Currency management, distribution and withdrawal;
- Implement the monetary policy of the WACB;
- Manage the payments and settlements systems;

- Serve as bankers to financial institutions in the Zone, and fiscal agents to governments;
- Exercise prudential supervision over financial institutions;
- Conduct foreign exchange operations under the guidance of the WACB.

The design and development of the Afkoin CBDC takes into account the functions, roles and responsibilities of the WACB and NCBs.

1.6.3 West African Monetary Agency

To promote coordination between the two ECOWAS EMUs (WAEMU and WAMZ), 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 [174].

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 Program (EMCP), geared towards the creation of the ECOWAS single currency [174].

The function of WAMA is out of scope for the Afkoin CBDC proposed in this research.

1.7 Payment Systems in Ghana

The Afkoin CBDC platform is modeled after the Bank of Ghana (BOG)'s domestic wholesale interbank payment settlement system. In this section we examine the underlying payment system on which the Afkoin CBDC is modeled.

Ghana has two types of payment systems, namely, wholesale payment system and retail payment system. The Bank of Ghana (BOG) has supervisory and regulatory authority over payment and settlement systems in Ghana. The BOG derives its payment systems oversight authority through the *Bank of Ghana Act, 2002 (Act 612)* passed by the Parliament of Ghana along with other statutory and regulatory policies and directives.

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 [19]. The GIS system was launched by the BOG the year 2002 [180]. Settlement on the GIS system is final, irrevocable and unconditional in conformance with the BIS' Principles for Financial Market Infrastructures (PFMIs) [50].

In the BOG's most recent payment systems report published in 2018 [175], the GIS had 34 participating PSPs, ARB Apex Bank, and the Social Security and National Insurance Trust (SSNIT) [175]. 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.

A timeline of the development of Ghana's payment systems in presented in Fig.1.11.

< 2001	2002	2003	2004 - 2008
Exchange Act, Act 55: This is an adaptation of the English Bills of Exchange Act 1882 which specifies how cheques are drawn, accepted and paid.	Act 612: The Act makes the Bank of Ghana the authority responsible for payment and settlement systems in Ghana. 2002 – the Real Time Gross Settlement (Ghana Interbank Settlement) for wholesale payment and settlements was introduced (Rules and Guidelines).	Systems Act, Act 662: This is a sound legislative framework which further empowers the Bank of Ghana to oversee and manage the payment systems.	– 2006: Foreign Exchange Act, Act 723 – 2007: Credit Reporting Act, Act 726 – 2007: Central Securities Depository Act, Act 733 – 2008: Anti-Money Laundering Act, Act 749 – 2008: Electronic Transactions Act, Act 772
2009 - 2010	**2012**	**2013 - 2014**	**2015 - 2016**
– 2009: Cheque Codeline Clearing System for the electronic clearing of cheques and other paper payment instruments introduced (Rules and Guidelines). – 2010: Automated Clearing House for automated direct credit and direct debit payments launched (Rules and Guidelines).	– 2012: Operationalization of gh-link-the national interbank ATM transaction switch (Rules and Guidelines).	– 2013: National Payments Systems Oversight Framework document prepared by Bank of Ghana. – 2014: Strategic Payments Roadmap for Ghana, document prepared by Standard Chartered Ghana under the auspices of Bank of Ghana.	– 2015: Guidelines for e-Money Issuer and Agent Guidelines to regulate and guide mobile money business activities in Ghana. – 2016: Introduction of GHIPSS Instant Pay (GIP) (Rules and Guidelines).

Figure 1.11: Ghana Payment System Development Trend [180]

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% [175]. All high-value transactions are processed directly on the GIS system.

The GIS system operates during Ghana banking hours from 8:00AM UTC to 5:00PM UTC on weekdays and at variable times on Saturdays.

To promote a cashless economy in Ghana, the BOG has authored and implemented various e-payment policies and directives. To achieve its goal of a cash-lite economy, the BOG established the *Ghana Interbank Payment and Settlement Systems Limited (GhIPSS)* in 2007 to own, promote, and operate e-payment systems and services in Ghana's retail payment industry [176].

GhIPSS owns and operates the Ghana Automated Clearing House (GACH), the Cheque Code-line

Clearing (CCC), the Gh-Link^{TM} National Switch, GhIPSS Instant Pay, the Mobile Money Interoperability Platform, and the e-zwich Biometric Smart Card Payment System which are all geared towards improving Ghana's retail payment industry especially in the area of e-payments. Retail payments such as cheques, mobile money payments, and ATM transactions among others are processed on GhIPSS' FMIs and are further settled in batches on the GIS system as high-value transactions on net settlement basis [180].

A logical view of Ghana's payment landscape is presented in Fig.1.12.

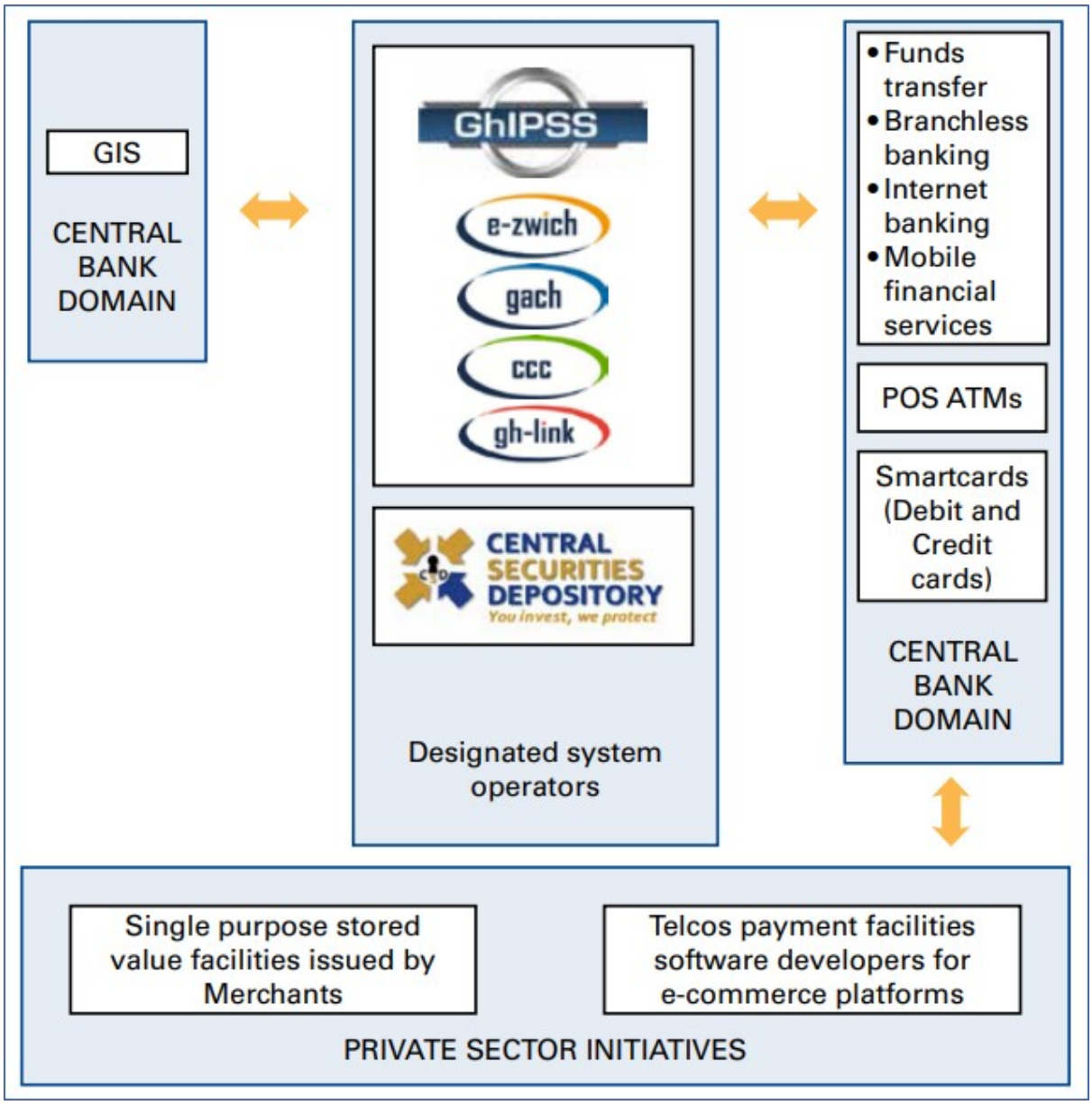


Figure 1.12: Logical View of Ghana Payment Landscape [180]

Ghana's retail payment system is out of scope in this research and is therefore not examined further in this dissertation.

1.8 Contribution

This dissertation focuses on implementing a DLT-based quantum resistant CBDC known as Afkoin in ECOWAS. In this regard, we provide the following key contributions:

- Preliminary design considerations and characteristics of Afkoin;
- A Hyperledger Fabric-based CBDC framework that can be leveraged to issue a single currency in ECOWAS;
- Technical requirement specification of the Afkoin prototype highlighting various user stories and capabilties that are to be implemented on the Afkoin CBDC prototype;
- Contribution to the existing body of knowledge on CBDCs with a specific focus on ECOWAS.

1.9 Dissertation Structure

The rest of the dissertation is organized as follows. In chapter 2, we provide an introductory thesis on DLT. We highlight some of the shortfalls of *first generation* DLT platforms within the context of the financial services industry (FSI); and discuss some of the solutions that have emerged to address these shortfalls, in the form of *second generation* DLT platforms. Further, we present some of the potential use cases of DLT in the FSI. In chapter 3 we discuss quantum computers, post quantum cryptography schemes and quantum resistant DLTs. In chapter 4, we discuss central bank-issued money (such as banknotes and coins) and CBDCs as another type of central bank money. We analyze some of the similarities and differences between both types of central bank currencies. Further, we discuss three types of CBDCs and present a generic framework for each type of CBDC discussed in this chapter. Lastly in this chapter, we discuss some of the practical implications for CBDC issuance by central banks. Subsequently in chapter 5, we present our preliminary design considerations and characteristics of the Afkoin CBDC. Then in chapter 6, we present our initial technical requirement specification for the Afkoin CBDC prototype. We conclude this chapter by highlighting some of the practical implications for Afkoin CBDC issuance in ECOWAS. Finally in chapter 7, we give our conclusion, future research directions and open problems. In Appendix I, we present excerpts of our major research work on relevant CBDC research initiatives from across the world, which research has been published in a peer-reviewed Science Citation Index Expanded (SCIE) journal.

Chapter 2. Review of Distributed Ledger Technologies

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 [31, 32] in 2008 popularized the term DLT following the release of the Bitcoin core [38] 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" [42]. 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" [33] .

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 [33,34]. These characteristics make DLT suitable for several applications and industries that require these features.

2.1 Classification of DLT

Two main types of DLT platforms are identified in literature, namely permissionless and permissioned DLT platforms [37].

2.1.1 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 [37]. 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) [38] and Proof-of-Stake (PoS) [35, 36] are used to guarantee system trust and integrity.

Examples of a permissionless DLT platform include Bitcoin and Ethereum.

2.1.2 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 [37].

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) [43], Istanbul Byzantine Fault Tolerance (IBFT) [44], Kafka [45] and Raft-based [46] consensus mechanisms have been proposed for permissioned DLT systems.

Examples of popular permissioned DLT systems include Quorum [47], Hyperledger Fabric [48] and Corda [49].

2.2 Limitations of First Generation DLT Platforms

Permissionless DLT platforms such as Bitcoin and Ethereum are also known as first generation DLT platforms as they were the first DLT platforms of any kind to be developed. While these DLT platforms possess several desirable attributes for the FSI, a number of shortfalls in their original design and implementation undermine their suitability for FMIs.

Firstly, a majority of the first generation DLT platforms are public, allowing anyone to join and conduct transactions on the platforms without a need for approval from anyone. Ensuring compliance with the PFMIs [50] requires that counterparties in an FMI must meet strict access and participation requirements (*PFMIs Principle 18 - Access and Participation Requirements*) in order to guarantee the safety and security of the underlying FMI.

Secondly, the public nature of the first generation DLT platforms means that all transactions are publicly visible, representing a lack of compliance with *PFMIs Principle 17 - Operational Risk*, whose goal is to ensure transaction and data privacy for FMI participants.

PoW is the dominant consensus protocol for a majority of the first generation DLT platforms. PoW, however, is resource intensive, requiring excessive amounts of energy and time to append new blocks to the transaction ledger of a blockchain system [51]. In FMIs, payment transactions usually require a fraction of a second to be completed while Bitcoin only adds transactions to blocks and propagates

such blocks to the shared ledger every 10 minutes [32]. This design feature of blockchains violate the immediate and final settlement (*Principle 8 - Settlement Finality*) requirement of the PFMIs.

Additionally, the PoW consensus mechanism is probabilistic rather than deterministic [37]. As a result, there is a small chance that transactions in blocks farthest from the *genesis block* of a first generation DLT network may be reversed, invalidating the settlement irrevocability (*Principle 8 - Settlement Finality*) requirement of the PFMIs.

Other limitations of the first generation DLT platforms include but are not limited to scalability challenges [52] (*PFMIs Principle 17 - Operational Risk*) as well as susceptibility to the 51% attack [37].

To address the limitations of the first generation DLT platforms, leading PSPs and financial technology (fintech) companies are collaborating to develop permissioned DLT platforms that meet the needs of the FSI [53].

We refer to these new DLT platforms seeking to address the above limitations as second generation DLT platforms. Notable platforms in this category are JP Morgan Chase's Quorum, R3's Corda, and Linux Foundation's Hyperledger Fabric.

Other less known but notable second generation DLT platform with desirable features for the FSI include Digital Asset's Digital Asset [57] platform, Blockstream's Elements [54], Anquan Capital's Anquan Permissioned Blockchain [55], and Chain Inc.'s Chain Core [56] DLT platforms.

We describe the Quorum, Corda, and Hyperledger Fabric DLT platforms in the subsequent subsection.

2.3 Second Generation DLT Platforms

2.3.1 Quorum

Built in 2016 by JP Morgan Chase, Quorum is an open source Ethereum-based permissioned DLT platform with support for smart contracts, transaction and contract privacy, and multiple voting-based consensus mechanisms [58].

Quorum is a fork of go-Ethereum with support for IBFT and Raft-based consensus mechanisms, ensuring faster block propagation times and guaranteeing transaction finality and irrevocability [47].

Quorum provides for a single shared ledger underpinned by cryptographic mechanisms that ensures that only parties to a transaction can see data related to the transaction.

The architecture of Quorum is presented in Figure 2.1. It is made up of the transaction manger, crypto enclave, consensus, and network manager.

The *Transaction Manager* manages access to encrypted transaction data in Quorum as well as managing the platform's interactions with other transaction managers and the local data store of a

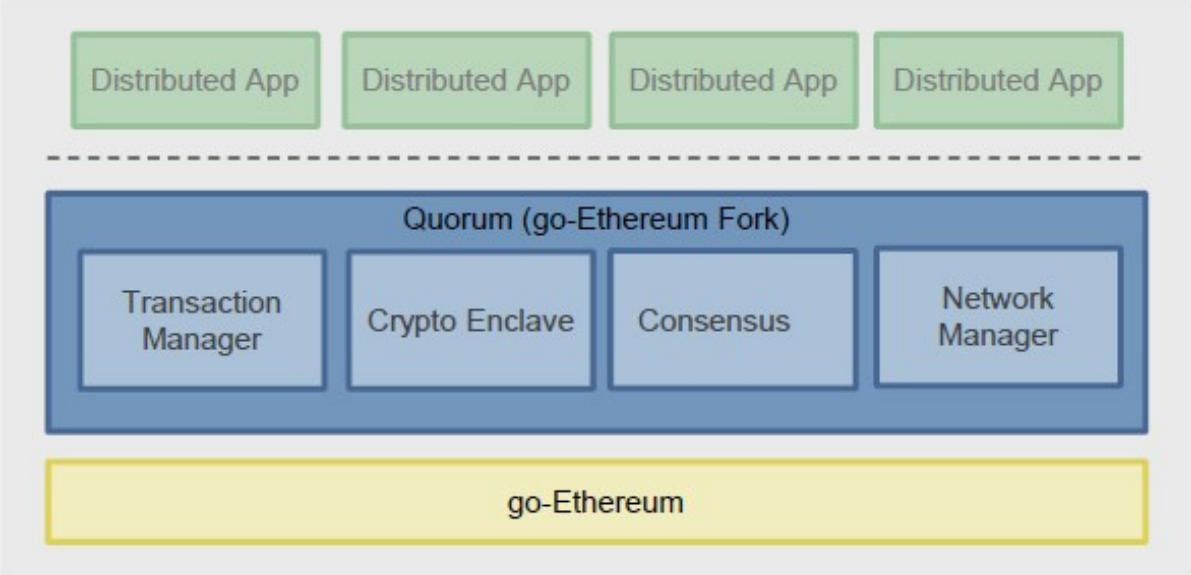


Figure 2.1: Quorum DLT Platform Architecture [47]

Quorum node.

The *Crypto Enclave* is responsible for key management and data encryption and decryption in Quorum.

The *Consensus* component provides for the use of various consensus mechanisms in Quorum. Consensus mechanisms currently supported on Quorum are the Raft-based consensus mechanisms and the IBFT consensus mechanism.

Raft-based consensus mechanisms are suitable for a closed membership-based consortium/organization where transaction settlement finality is a requirement. In such a system, there exists a leader/follower relationship such as in a wholesale interbank payments settlement setting where the central bank is the defacto leader for authenticating and validating transactions while CMB participants are considered followers.

An IBFT is a three-phase consensus mechanism suitable for DLT implementations where fault tolerance is a key requirement. IBFT also provides for settlement finality.

The *Network Manager* controls access to a Quorum network, thereby enabling a permissioned network of nodes to be created for a Quorum implementation.

2.3.2 Corda

Corda is an open-source permissioned enterprise DLT platform developed from the ground up with a focus on the FSI by the R3 consortium in 2016. R3 is a distributed ledger technology consortium established in 2014 [59]. The consortium is made of more than 300 members and partners across multiple industries from the private and public sector [60].

Inspired by developments in the blockchain industry, Corda introduces a new consensus algorithm that is based on the concept of notary nodes. A notary's primary responsibility is preventing double spending in Corda. For a given transaction in Corda, a notary ensures that it has not signed another transaction consuming any of the same input states known as unspent transaction outputs (UTXO), thereby preventing double spending [61].

A Corda state is an immutable object representing a fact known by one or more Corda nodes at a specific point in time. Every Corda state has an appointed notary. Each Corda node has its own database, known as a vault where it stores any relevant states to itself. A Corda node's internal architecture is presented in Figure 2.2.

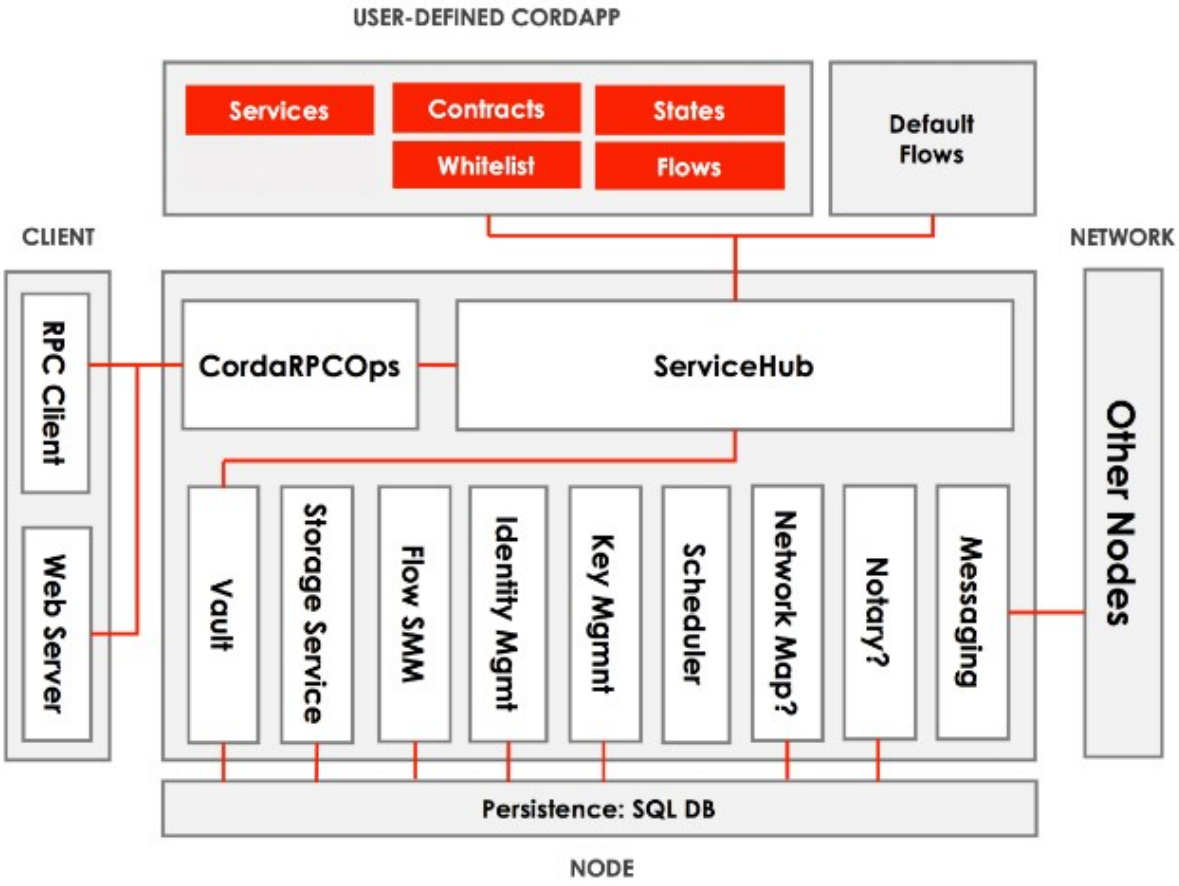


Figure 2.2: Corda Node Internal Architecture [62]

The Corda DLT architecture is made up of five key layers which are the persistence layer, network interface layer, remote procedural calls (RPC) client layer, service hub layer, and user-defined CorDapp interface layer [61].

The *Persistence* layer is responsible for data storage in Corda.

The *Network* interface layer is responsible for interaction between a Corda node and other nodes in a Corda network.

The *RPC Client* allows a Corda node owner to interact with the node under its ownership through RPC calls.

The *ServiceHub* provides capabilities that allows a given Corda node to call its other services.

The *CorDapp* layer allows a given Corda node to be extended through the installation of CorDapps. CorDapps are distributed applications that run on a Corda platform.

2.3.3 Hyperledger Fabric

Hyperledger Fabric [62] is an open source plug-and-play permissioned DLT platform started in 2016 by IBM and Digital Asset and currently hosted and managed by the Linux Foundation [63].

Fabric has a modular and configurable architecture with support for smart contracts (known as chaincode in Fabric) written in general-purpose programming languages such as Java, Go and Node.js. This allows for easy Fabric deployments with no additional training required [48, 64].

Fabric provides flexibility with its support for pluggable consensus protocols such as Kafka and Raft-based consensus protocol that do not require the use of cryptocurrencies, thus, allowing different consensus mechanisms to be implemented for various use case scenarios [64].

Unlike most DLT platforms including Quorum and Ethereum's PoW implementation that employs an order-execute architecture whereby the blockchain network orders transactions first using a consensus protocol, and then executes them in the same order on all peers sequentially [64]; Fabric employs an execute-order-validate architecture allowing Fabric deployments to achieve better performance (throughput), resiliency, scalability and confidentiality for transactions. The Fabric approach makes it a deterministic DLT platform and provides for concurrent transaction execution., which leads to better system performance, transaction scalability and confidentiality [65].

The key components of a Fabric DLT platform are ordering service, membership service provider, peer-to-peer gossip service, chaincode service, transaction ledger, and the endorsement and validation policy enforcement protocol [66]. We present Fabric's reference architecture in Figure 2.3.

The *ordering service* is responsible for establishing consensus on the order of transactions and broadcasting of blocks to peers through a shared communication channel. A channel in Fabric is a "subnet" provisioned by the ordering service for private and confidential communication between two or more peers in a given Fabric network.

The *membership service provider* performs identity management functions in Fabric by associating entities in the Fabric network with cryptographic identities.

The *peer-to-peer gossip service*, which is optional, is responsible for disseminating the ordering service's outputs to other peers.

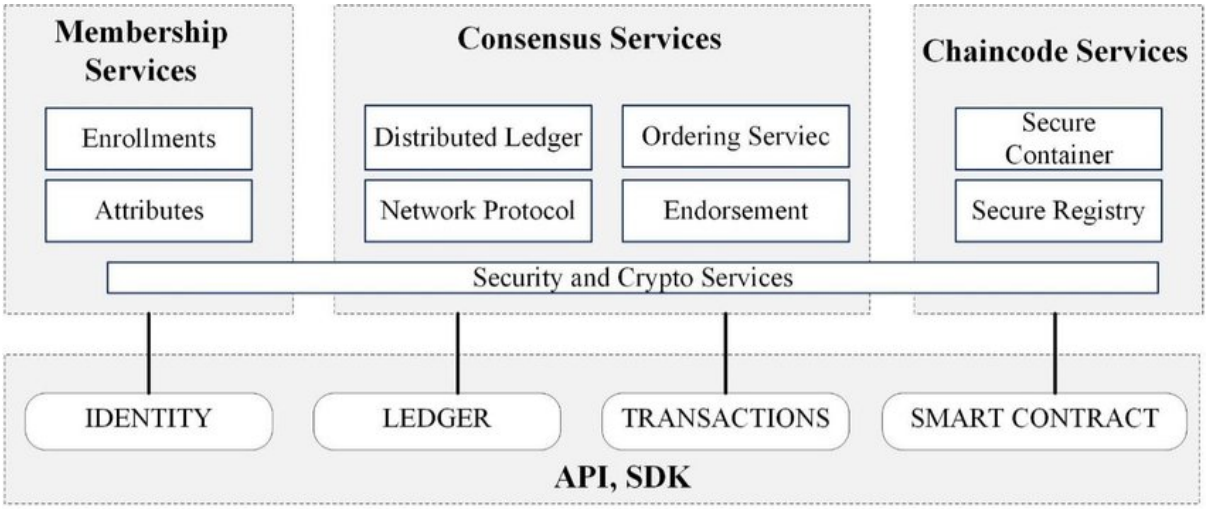


Figure 2.3: Hyperledger Fabric Reference Architecture [63]

The *chaincode service* provides for the execution of chaincodes in a container environment to guarantee transaction isolation.

The *transaction ledger* is responsible for recording all transactions on Fabric.

Lastly, the *endorsement policy* is used by a chaincode to specify the Fabric nodes that participate in transactions and for validating transactions before they are committed to the transaction ledger.

2.4 Financial Service Industry DLT Use Cases

DLT has applicability across several domains of the FSI. It is envisaged that DLT will drive operational and regulatory efficiency, improve transaction processing times, and minimize fraud and risks associated with transactions in the FSI. In Table 2.1, we highlight some of the FSI DLT use cases in literature [52, 67]. We assign a coding system, *UC + number*, for all the identified use cases solely for the purpose of ease of referencing. The use cases examined in this section are non-exhaustive.

Table 2.1: FSI DLT Use Cases

Use Case	Use Case Description
UC1	**G-CBDC** – DLT may be used to issue general-purpose CBDCs (G-CBDCs) for retail and other general purpose transactions.
UC2	**W-CBDC** – DLT may be used to issue W-CBDCs for interbank payments settlement.
UC3	**RTGS System** – DLT may be used to improve pay ments system resiliency by implementing various RTGS or LVTS functions in a decentralized manner to eliminate the single-point-of-failure problem associated with traditional centralized RTGS system implementations. We use RTGS system and LVTS interchangeably
UC4	**KYC and AML** – Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations are essential for the security and safety of FMIs. DLT may be used to implement immutable user identities (KYC) that may be shared across multiple stakeholders in the FSI and other vertical industries to minimize money laundering (AML) and other fraudulent transactions. KYC/AML may then be connected to CBDCs to achieve AML regulatory and transaction anonymity requirements for different CBDC implementations.
UC5	**Trade Finance** – DLT may be used to improve the efficiency of trade finance activities which are predominantly manual, time-consuming and inefficient. DLT-based KYC/AML processes may then be connected to DLT-based trade finance implementations to enhance the overall trade finance sub-sector of the FSI.
UC6	**Securities Settlement** – Processing times for securities settlement functions such as Delivery-versus-Payments (DvP), Delivery-versus-Delivery (DvD) and Payment-versus-Payment (PvP) may be improved with DLT. DLT-based implementation of these securities settlement functions may enable the simultaneous and efficient exchange of multiple asset types such as the exchange tokenized bond and cash assets.
UC7	**Bond Issuance** – DLT may be used to implement bond issuance and lifecycle management functions to improve the efficiency and cost of bond issuance activities both domestically and internationally.
UC8	**Information Exchange and Data Sharing** – DLT implementation of KYC is a first step to achieving a coherent and consistent global database of immutable user identities that may be shared across multiple horizontal and vertical industries or with governments in a decentralized manner to improve global transaction efficiency while mitigating against fraudulent transactions.
UC9	**Crossborder Payments** – DLT may be used to improve the efficiency of cross-border payments.
UC10	**Cash Supply Chain** – In scenarios where CBDCs are implemented as complement to cash and not replacement of cash, DLTs may be used to improve the lifecycle of the production, transfer and management of cash from the central bank to CMBs and to end users.

Chapter 3. Post Quantum Cryptography and Quantum Resistant Ledgers

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 [70]. 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 [74].

However, advancements in quantum computing based on Shor's algorithm [70,72] has rendered these classical cryptosystems insecure. Mosca [71] 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 [73].

Two approaches have emerged in literature to address the threat of quantum computers namely, 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 [71]. The security of QKD is based on the quantum-mechanics *non-cloning theorem* [75].

In this chapter we focus on PQC schemes. PQC approaches such as multivariate-quadratic-equations, lattice-based cryptography, code-based cryptography, hash-based cryptography, and isogeny-based cryptography are studied in literature [71]. Researchers have begun to leverage PQC schemes such as hash-based and lattice-based schemes to secure DLT systems against quantum computing attacks.

3.1 NIST PQC Third Round Finalists

To mitigate the quantum computing threat, the National Institute of Standards and Technology (NIST) initiated the NIST PQC Standardization Process in December 2016 [177]. The NIST PQC Standardization Process invited the general-public to submit candidate PQC algorithms for review and evaluation with the goal of selecting and standardizing suitable PQC algorithms to protect critical national infrastructure and sensitive information in the age of quantum computers.

The NIST PQC Process has reached the third round stage with shortlisted finalists and alternative finalists. The third-round finalist public-key encryption and key-establishment mechanism (KEM) are Classic McEliece, Crystals-Kyber, NTRU, and SABER. The third-round finalists for digital signatures

are Crystals-Dilithium, Falcon, and Rainbow. These finalists will be considered for standardization at the end of the third round [177].

The NIST third round finalists consists of four KEMs and three digital signature schemes. Of the four KEM schemes, all except Classic McEliece are lattice-based schemes. Of the three signature schemes, all except Rainbow are lattice-based schemes. Of the three lattice-based KEM schemes, NIST intends to choose at most one of Crystals-Kyber, NTRU or SABER as its PQC KEM standard. Of the two lattice-based digital signature schemes, NIST will choose at most one of Crystals-Dilithium or Falcon as its PQC digital signature standard. Overall, NIST intends to choose at least one KEM scheme and one digital signature scheme for further standardization in the third round. In NIST's current view, structured lattice schemes appear to be the most promising general-purpose algorithms for public-key encryption/KEM and digital signature schemes.

In addition to the third round finalists, NIST advanced the following eight alternate candidate algorithms to the third round: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic, and SPHINCS+. The NIST alternate candidates are considered candidates for future standardization; therefore, NIST will not review them further in the third round. The NIST third round alternate candidates are therefore not considered for implementation with Afkoin.

NIST indicates in its report [177] that, Crystals-Kyber, is one of the most promising KEM schemes that advanced to the third round. Afkoin will therefore be implemented with the Crystals-Kyber KEM scheme. Crystals-Kyber is a structured lattice construction. It is based on the hardness of the Module-LWE (MLWE) problem. Crystals-Kyber is based on Regev's original idea for public-key encryption from plain LWE and provides IND-CCA2 security which is achieved with a Fujisaki-Okamoto transform. The security of Crystals-Kyber is supported by a security proof in QROM. Currently no attacks are known against MLWE that do not also apply to the well-established plain LWE.

Crystals-Kyber enables fast computations via the number theoretic transform (NTT) over the cyclotonic ring and has an excellent all-around performance for most applications. Kyber enables relatively straightforward adjustment of the performance/security trade-off by varying module rank and noise parameters. The final key derivation of Crystals-Kyber uses SHAKE256 instead of SHA3-256. Crystals-Kyber shares a common framework with the Crystals-Dilithium signature scheme, which is also a NIST third round finalist.

Regarding a signature scheme, if Afkoin is to implement a PQC digital signature scheme, then the obvious choice will be Crystals-Dilithium as it shares a common framework with Crystals-Kyber. Additionally, Crystals-Dilithium is simpler to implement and performs well in real-world experiments as indicated by NIST. Crystals-Dilithium, similar to its KEM equivalent is a lattice-based signature scheme. The security of Crystals-Dilithium relies on the hardness of the MLWE and Module SIS (MSIS) problem

and follows the Fiat-Shamir with aborts technique. Crystals-Dilithium provides simpler implementation than its main lattice-based competitor, Falcon. Overall, Crystals-Dilithium has strong, balanced performance in terms of key and signature sizes and in the efficiency of the key generation, signing, and verification algorithms. NIST indicates in [177], that Crystals-Dilithium performs well in real-world experiments.

3.2 Quantum Computers

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* [68, 69].

Superposition enables quantum systems to be in multiple states at the same time while entanglement ensures that there is a strong correlation between these states even if states are separated by huge distances [68]. 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 [69].

It is estimated that, quantum computers may be available within the next decade [71]. 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 [69, 71]. 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 [88].

Many of the existing DLT platform including Bitcoin and Ethereum rely on RSA and ECDSA among others for transaction authentication and for achieving transaction consensus [71]. A quantum resistant ledger is a DLT system that is resilient against quantum computing attacks giving sufficiently large key sizes. We examine several approaches to quantum-secure DLT platforms in subsequent sections of this chapter.

3.3 Hash-based Quantum Resistant DLT Schemes

Hash-based cryptography as proposed by Lamport [76] refers to the use of a one-way hash function f to generate one-time signatures (OTS) and the application of the OTS to a message m to produce a hash digest h of fixed length n.

Given the one-way hash function f and the hash digest h, it should be computationally infeasible to find the value of m such that $f(m) = h$, that is m should be pre-image resistant. Given f and m, it should be computationally infeasible to find a different $m1$ such that $f(m) = f(m1)$, that is, m should be collision resistant [76] .

A major drawback with the Lamport OTS is that, each Lamport signature can be used only once [83]. Several researchers including including Perrig [77] Reyzin et al [78], Buchmann et al [79] and Buchmann et al [80] have therefore attempted to provide a more efficient hash-based signature scheme that allows for multiple signature use.

Secondly, Lamport OTS have relatively large key and signature sizes [77]. Bleichenbacher et al [81] and Huelsing [82] have provided constructions that reduce the key and signature sizes significantly.

Of the many OTS schemes, Huelsing's OTS scheme, the Winternitz OTS (W-OTS+) is deemed one of the most efficient. Huelsing's W-OTS+ is secure in the quantum-accessible random oracle (QROM) model and has therefore seen widespread adoption for quantum-resistant systems implementations.

3.3.1 Quantum Resistant Ledger

In the paper [74], Waterland leverages hash-based cryptography to implement the quantum-resistant ledger (QRL), a public quantum-secure DLT platform on a fork of the Ethereum blockhain.

The QRL is a chained extended merkle signature scheme (XMSS) based on an extensible stateful asymmetric hypertree.

Waterland indicates that the choice of a chained stateful asymmetric hypertree-based XMSS provides the dual benefit of utilizing a validated signature scheme as well as allowing the generation of ledger addresses that avoid a lengthy pre-computation delay when signing transactions.

Leveraging the pseudorandom number generator *HMAC_DRBG*, Huelsing's W-OTS+ hash-based OTS scheme, and the *SHA-256* hash function, Waterland implements the QRL signature scheme on Ethereum with PoS consensus mechanism .

Waterland indicates that, the QRL implementation offers 196-bit security with resilience against brute force computational attack until the year 2164 [74].

3.3.2 Blockchained Post-Quantum Signatures

Similar to the QRL [74] scheme, the R3 consortium has proposed a hash-based quantum-resistant signature scheme known as the Blockchained-Post Quantum Signatures (BPQS) [84].

BPQS leverages XMSS and Huelsing's W-OTS+ scheme to secure DLT platforms against quantum computing attacks.

A key difference between the QRL [74] signature scheme and the BPQS [84] scheme is in the hash function used by both schemes. While the QRL scheme [74] uses *SHA-256* as its hash function, the BPQS proposes to use *SHA-384*. Chalkias et al. argue that *SHA-384* provides 128-bit security against collisions, whereas *SHA-256* provides only 85-bit security, thereby making *SHA-256* unsuitable for schemes basing their security on collision resistance.

The BPQS scheme is based on two building blocks namely *BPQS-FEW* and *BPQS-EXT*. *BPQS-FEW* allows for the generation of a limited number of few-times signatures while the *BPQS-EXT* allows for the generation of an unlimited number of many-times signatures. For *BPQS-FEW*, all keys are pre-computed during key generation; while for *BPQS-EXT*, only two OTS keys are required.

A full BPQS implementation however requires the concatenation of a *BPQS-EXT* to *BPQS-FEW* such that the last leaf in the chain of *BPQS-FEW* is a *BPQS-EXT* fallback key.

Chalkias et al. [84] implements a PoC of their BPQS-EXT scheme on a 2.80GHz Intel Core i7-7700HQ octa-core with a 15.5GB RAM running a Linux 4.13.0-38 operating system and the JRE 1.8.0_161 java-runtime-environment and compare the performance results with other renowned signature schemes.

The authors note that, the BPQS implementation is not optimized for parallel processing [84].

3.4 Lattice-based Quantum Resistant DLT Schemes

Lattice-based cryptography refers to the construction of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. Lattice-based cryptography is regarded as one of the best and strongest crypto approaches to combating the threat of quantum computers [85].

First proposed by Ajtai [86] in his seminal paper on *generating hard instances of lattice problems*, Ajtai provides strong security proofs against quantum computers by connecting the average-case problem of lattices to the complexity of the worst-case hardness problem [86].

Lattice-based primitives are computationally efficient with signature and key sizes that compare favorably to signature and key sizes of many classical digital signature schemes [88].

Two approaches of lattice-based cryptography have emerged in literature: average-case hardness schemes and worst-case hardness schemes [85].

Average-case hardness schemes include the shortest vector problem (SVP), shortest independent

vector problem (SIVP), closest vector problem (CVP), short integer solutions (SIS) problem, ring-SIS problem, learning with errors (LWE) problem, ring-LWE problem and many more [87]. For the average-case hardness schemes, the security of the scheme is based on the hardness of the underlying lattice problem [85]. Average-case hard problem schemes are deemed fast, efficient, simple and easy to implement.

Worst-case hardness problem schemes include the hash-and-sign digital signature scheme, conjunction obfuscation, attribute-based encryption, and identity-based encryption schemes. Worst-case problem schemes are deemed space- and compute-intensive and therefore less efficient compared to the average-case hardness schemes [85].

Due to their efficiency, implementation simplicity and robustness against quantum computing attacks, many researchers have begun to explore the applicability of lattice-based cryptographic schemes to DLTs to mitigate against quantum attacks. Consequently, we examine some of the current research aimed at securing DLTs using lattice-based cryptographic schemes.

3.4.1 Post Quantum Blockchain

Gao et al [90] have proposed the Post Quantum Blockchain (PQB), a quantum resistant DLT that leverages lattice-based signature schemes to secure a fork of the Bitcoin blockchain against quantum computing attacks.

Secret keys for the PQB are generated using the lattice-basis delegation algorithm while message signing is achieved using the preimage sampling algorithm [91]. Gao et al attempt to reduce the correlation between a message and a signature by designing the first and last signatures respectively.

The security of the PQB signature scheme is based on the SIS problem.

Gao et al [90] indicate that the security model of PQB is existentially unforgeable against chosen message attack in the standard model.

3.4.2 Post Quantum Blockchain Network

Contributing to the body of knowledge for PQC signature schemes, Li et al [92] have proposed the Post Quantum Blockchain Network (P-BQN) signature scheme to secure DLT platforms against quantum computing attacks.

Similar to Gao et al [90], the security of the P-BQN scheme depends on the SIS problem.

In the proposed P-QBN [92] signature scheme, public and private keys were generated from the root keys using the Bonsai Trees technology [92] together with the RandBasis algorithm, which randomizes the lattice basis to guarantee private key randomness. The ExtBasis algorithm [92] is further used to extend control over the growth of the lattice to an arbitrary higher-dimensional extension in keeping

with the core principles of the Bonsai Trees technology.

Li et al [92] argue that the P-QBN is strongly unforgeable under adaptively chosen message attack in the random oracle model except the probability $\varepsilon/lq2$.

Chapter 4. Analysis of Central Bank Currencies

A central bank controls economic activity in a given economy through the use of monetary policy and other relevant economic management tools. Central bank implement monetary policy by controlling monetary supply, managing interest rates and maintaining price stability in a given nation-state [96]. Central banks enjoy a legal monopoly on the issuance of currency in a given economy [97].

The invention of Bitcoin in 2009, however, has given rise to the issuance of alternative forms of currencies popularly known as cryptocurrencies by private actors. In less than a decade since the introduction of Bitcoin, private sector actors have issued more than five thousand different cryptocurrencies [94]. Most of these cryptocurrencies lack intrinsic value and are not backed by any tangible resources [99]. Besides Bitcoin, other notable private sector-issued digital currencies include Ethereum [99], Ripple [100], Tether [101], Stellar [102] and other altcoins.

With cryptocurrency issuances posing a threat to monetary policy preservation and financial market instability, many central banks have delved into research and experimentation on CBDCs to guarantee financial market stability and monetary policy preservation [39, 104].

In a recent survey [105] conducted by the BIS to examine central banks efforts on CBDC research, more than 70% of the central bank respondents indicated that they were investigating the possibility of issuing a CBDC. Cumulatively, the BIS survey participants are located in jurisdictions covering more than 70% of the world population and over 90% of its GDP [105]. 65% of the survey participants were from emerging market economies (EMEs) while 35% were from advanced economies. Overall, survey participants from EME cited financial inclusion and domestic payment efficiency as their motivation for investigating CBDCs and thus, indicated the strongest preparedness to issue a CBDC over the medium term (1-6 years). In total, about 30% of all survey respondents indicated a preparedness to issue a CBDC in the medium term.

In this chapter, we examine the relationship between CBDCs and central bank money such as banknotes and coins. Subsequently, we discuss three types of CBDCs and present generic frameworks for the CBDCs discussed in this chapter. Finally in this chapter, we discuss some of the relevant CBDC research initiatives from across the world.

4.1 Central Bank Currency

Central banks issue two types of currency: *physical money or cash* such as banknotes and coins and *electronic money* otherwise known as reserves or settlement accounts [39].

For money to be accepted as legal tender, it must perform three functions: it must be a unit of account, a medium of exchange, and a store of value [23]. The value of money is derived from the economic strength of the issuing-country.

Money has value because people accept it as a means of payment or a medium of exchange. People accept money as a medium of exchange because it is perceived to have value [145].

This cyclical view about money is possible because Government-issued money represents a claim on the assets of the issuing the central bank and liabilities to the state government [23]. It is assumed that a Government will never go bankrupt as central banks can and always print new monies into existence through monetary policy tools such as quantitative easing and open market operations [145]. This mechanism imposes a reasonable level of confidence in central bank-issued money [26].

We describe the properties of cash and settlement accounts in the subsequent section.

4.1.1 Cash

From the perspective of accessibility, cash is also referred to as *general-purpose* money. It is widely available and accessible to the general-public.

General purpose money is non-interest bearing and can be used to make payments in a peer-to-peer anonymous manner without intermediation from third-parities [23].

Cash transactions settle immediately and are irrevocable [125].

In cash transactions, counterparties are each responsible for independently keeping records of the given transaction, therefore record-keeping for cash transactions is distributed [125].

4.1.2 Settlement accounts

Settlement accounts from the perspective of accessibility are referred to as wholesale money.

Wholesale money is accessible by only authorized PSPs such as CMBs and other high-value customers. PSPs must maintain settlement accounts on the books of a central bank.

Wholesale e-money is interest-bearing and does not have the anonymity property of cash. All participants in a wholesale payment system must be pre-registered, validated and authorized by the central bank before they can carry out transactions in the central bank's underlying FMI [39, 126].

4.2 CBDC

A CBDC may be defined as monetary value similar to central bank money that is stored electronically and represents a claim on assets of the issuing central bank [39]. It may be distributed in a decentralized manner and used to make payments [147].

Similar to the central bank currency, there are two types of CBDCs: *G-CBDC* and *W-CBDC*.

4.2.1 W-CBDC

A W-CBDC a is digital currency similar to a settlement account at a central bank. A W-CBDC is accessible by only PSPs such as CMBs and other high-value customers [39, 53, 95].

W-CBDCs are issued, distributed, stored and maintained solely by a central bank or an entity designated by the central bank to perform such functions.

All transactions involving W-CBDCs are processed by a central bank or an entity designated by the central bank to perform such a function.

Participants in a W-CBDC system have no anonymity. They must be pre-registered, authenticated and authorized by the central bank in order to access and conduct transactions on the central bank's FMI [39, 126].

From the perspective of transactions between counterparties, only parties involved in a specific W-CBDC transaction are able to access data relating to the transaction, thereby guaranteeing counterparty data privacy in conformance with the PFMIs [50].

In a W-CBDC system, a central bank's responsibilities includes the provision of:

- *W-CBDC* tokens for interbank transactions;
- *RTGS platform* for interbank transactions settlement;
- *Intranet infrastructure* to facilitate the bilateral transfer of W-CBDCs between counterparties;
- *On-ledger settlement accounts or wallets* to hold PSP W-CBDCs;
- *Transaction ledger* to record W-CBDC transactions;
- Any other services as may be required for the smooth and efficient functioning of the W-CBDC system.

A generic framework for a W-CBDC is presented in Figure 4.1.

4.2.2 G-CBDC

G-CBDCs are of two types: general purpose account-based CBDC (GA-CBDC) and general purpose value-based CBDC (GV-CBDC).

a. GA-CBDC

A GA-CBDC is similar to a W-CBDC; however, unlike a W-CBDC, a GA-CBDC is accessible by the general-public.

GA-CBDCs are issued, distributed, stored and maintained by a central bank or an entity designated by the central bank to perform such functions.

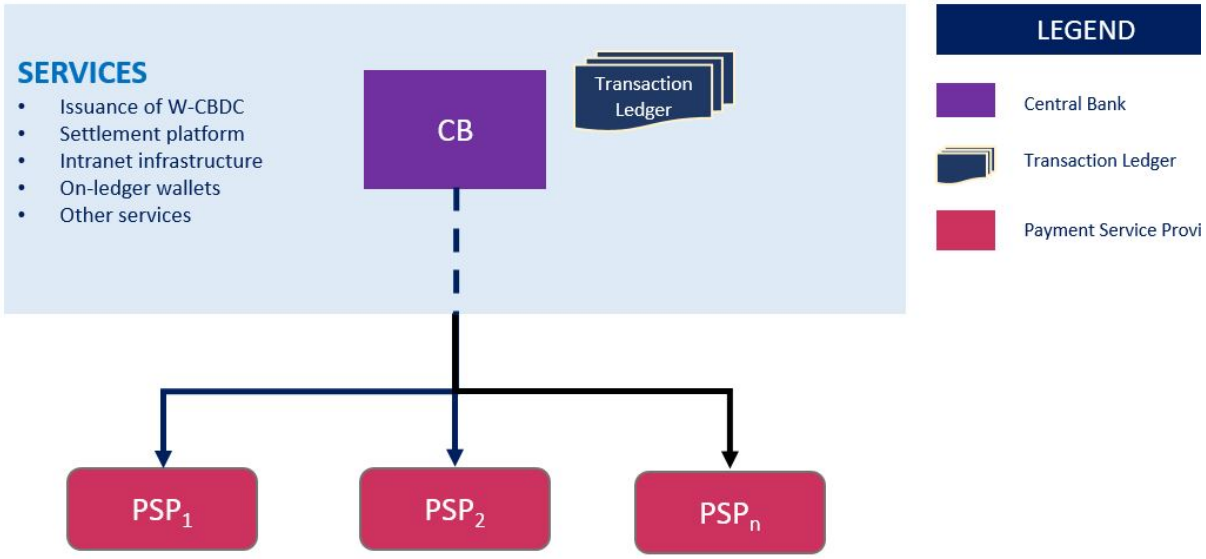


Figure 4.1: W-CBDC Generic Framework

Issuance of a GA-CBDC grants the general-public direct access to accounts held at the central bank. A GA-CBDC user will then access the CBDC using an electronic application (wallet) or other access mechanisms provided by the central bank [126].

Similar to W-CBDCs, GA-CBDC users must be pre-registered and approved by a central bank before they can hold GA-CBDC accounts with the central bank. A GA-CBDC, therefore represents a claim on asset of the central bank.

In a GA-CBDC system, a central bank's responsibilities includes the provision of:

- *GA-CBDC* tokens for the general public;
- *Payments settlement platform* for processing GA-CBDC transactions;
- *Internet banking infrastructure* to facilitate GA-CBDC user interaction with the central bank's public-facing FMIs;
- *On-ledger customer accounts or wallets* to hold GA-CBDC user tokens;
- *Transaction ledger* to record GA-CBDC transactions;
- *Customer support* to handle customer service related issues or problems;
- Any other services as may be required for the smooth and efficient functioning of the GA-CBDC system.

In Figure 4.2, a generic framework for a GA-CBDC is presented.

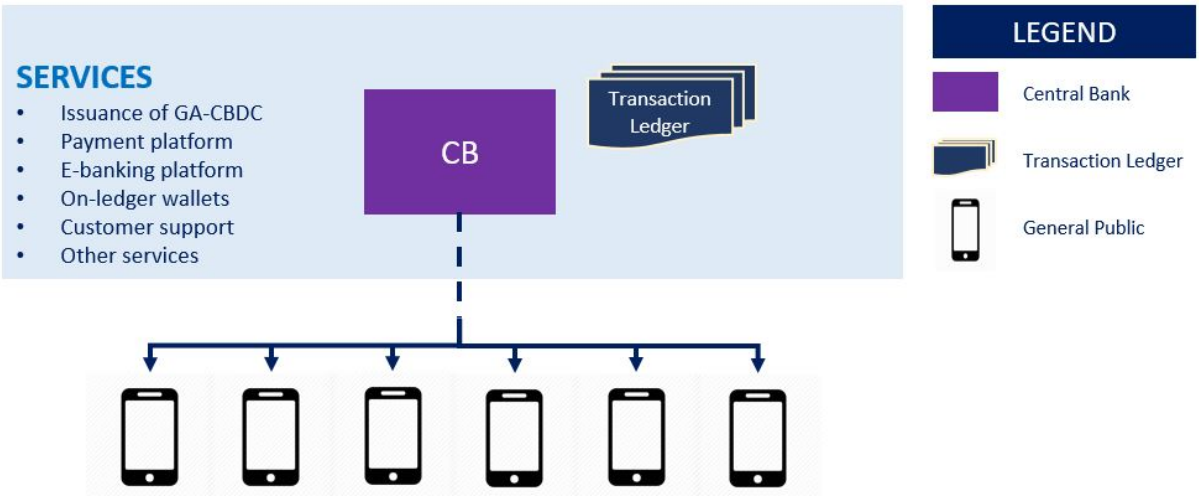


Figure 4.2: GA-CBDC Generic Framework

b. GV-CBDC

A GV-CBDC is similar to cash. It is accessible by the general-public and may be embedded with anonymity properties similar to that of cash [23, 126].

A key difference between a GV-CBDC and a GA-CBDC lies in how both CBDCs are distributed, stored and/or transferred [105].

A GV-CBDC once issued by a central bank may be distributed to PSPs into special PSP accounts held at the central bank for onward transmission to the general-public. The general-public will then store the GV-CBDC in special customer accounts provided by the PSP. To access the GV-CBDC held at the PSP, the general public may use e-wallets, payment cards or other access mechanisms provided by the PSP [23].

Depending on the mode of implementation, a GV-CBDC may represent a direct or indirect claim on the assets of the issuing central bank.

In a GV-CBDC system, a central bank's responsibilities includes the provision of:

- *GV-CBDC* tokens for distribution to PSPs and onward distribution from PSPs to the general public similar to current banknote distribution approaches;
- *On-ledger wallets* issued to PSPs to hold GV-CBDC tokens issued by the central bank for onward distribution to the general public;
- *Intranet infrastructure* to facilitate the distribution of GV-CBDCs to PSP on-ledger wallets;
- *Centralized payment processing platform* to process inter-PSP retail and wholesale payments;
- *Transaction ledger* to aggregate and record GV-CBDC transactions from PSPs.

- Any other services as may be required for the smooth and efficient functioning of the GV-CBDC system.

PSPs will be required to maintain local transaction ledgers that record all transactions carried out by their customers in addition to providing the following:

- *Internet banking infrastructure* to facilitate GV-CBDC user interaction with an PSPs' public-facing FMIs;
- *Customer accounts or wallets* to hold customer GV-CBDC tokens;
- *Retail payment platform* to process customer GV-CBDC retail transactions;
- *Customer service* to handle GV-CBDC customer service issues or problems;
- Any other services as may be required for the smooth and efficient operation and performance of the GV-CBDC system.

A generic framework for a GV-CBDC is presented in Figure 4.3.

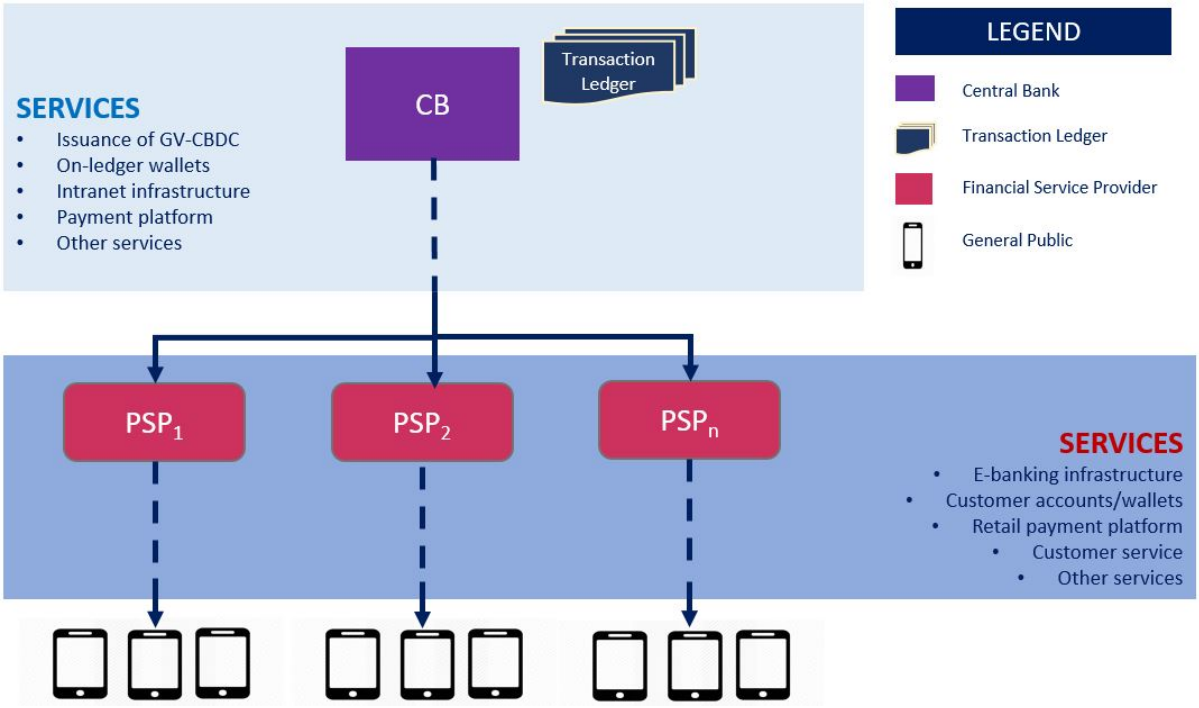


Figure 4.3: GV-CBDC Generic Framework

The BIS, widely regarded as the central bank of all central banks provides a classification of money and CBDCs based on four properties: *issuer* of money (central bank or not); *form* (digital or physical); *accessibility* (widely or restricted) and *technology* (account-based or token-based) [148]. The BIS further develops a *money flower* to depict its classification of money.

An annotated version of the BIS money flower is presented in Figure 4.4.

In Figure 4.4, the dark grey shaded areas represent the types of CBDCs issuable by a central bank.

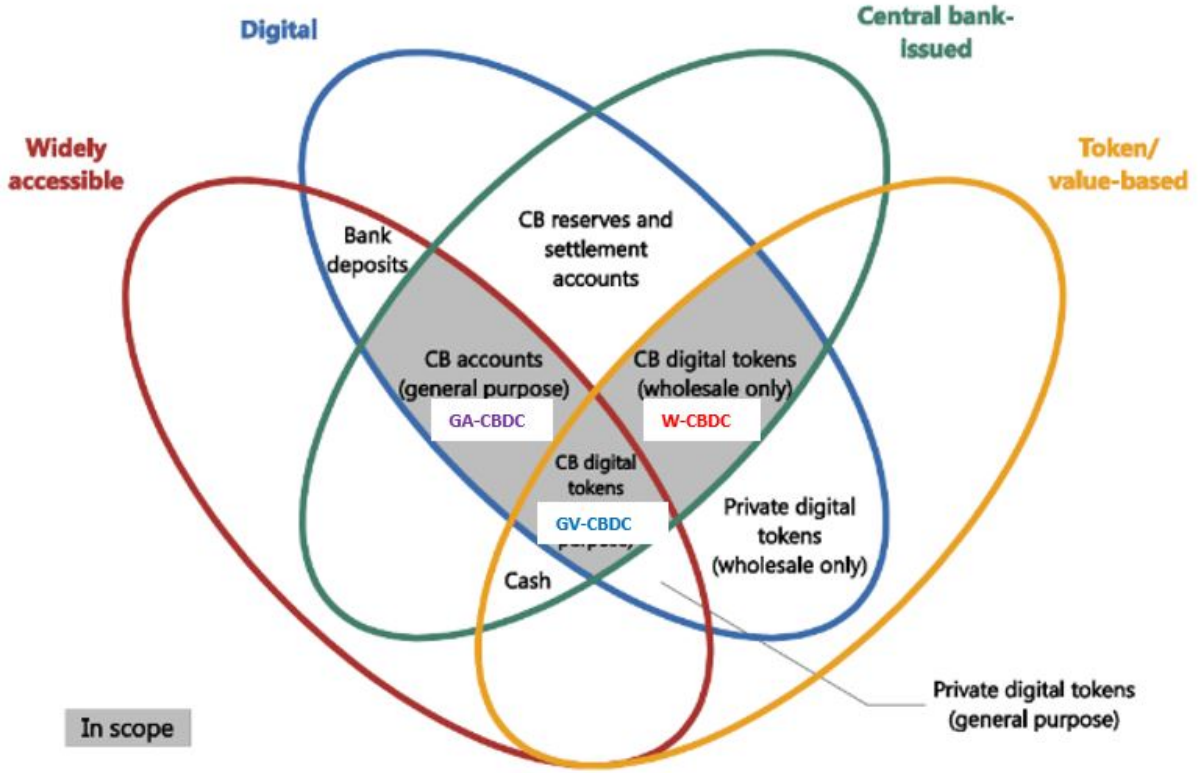


Figure 4.4: Annotated Money Flower [148]

4.3 Practical Implications of CBDC Issuance by Central Banks

Issuance of CBDCs by central banks and their widespread adoption may have significant operational and regulatory ramifications for domestic and global FMIs. Some of the potential implications for CBDC issuance are discussed in this section. The implications discussed are non-exhaustive.

4.3.1 Operational Implications

Leveraging DLT for CBDC issuance may yield potential benefits for central banks in the area of FMI operational efficiency. In our paper [146], excerpts of which are presented in Appendix I, we present relevant CBDC research that leveraged DLT to improve FMI operational efficiency both domestically (e.g. Project BLOCKBASTER [113]) and across borders (e.g. Project Jasper-Ubin [143]). Leveraging DLT can also enable central banks to implement more resilient and robust FMIs (e.g. Project SALT [115]) thereby increasing the public perception and trust in the central bank. Although DLT platforms are yet to become fully mature, current DLT platforms such as Hyperledger Fabric, Quorum and Corda provide adequate capabilties for central banks to achieve their data privacy goals (e.g. Project Inthanon Phase

I [138]), transaction scalability requirements (e.g. Project Khokha [130]), operational risk objectives (e.g. Project Jasper Phase II [111]) and settlement finality requirements (e.g. Project Ubin Phase II [161]) within the context of the PFMIs.

4.3.2 Legal and Regulatory Implications

CBDC issuance have the potential to pose legal challenges for central banks [29]. In most jurisdictions, existing laws on currency and/or legal tender does not include provisions for CBDCs. For CBDC to be accepted as legal tender, governments may have to spend a significant amount of resources to rewrite existing financial market laws and regulations to accommodate the issuance and adoption of CBDCs. The breadth of legal and regulatory issues that must be addressed by central banks varies from country to country and from continent to continent. It is therefore our position that any central bank intending to issue a CBDC as legal tender should carefully examine its existing financial laws and make amendments where applicable in order to accommodate CBDCs.

4.3.3 Implications for Financial Market Stability

Depending on the type or model of CBDC that is issued by a central bank the financial market in a given economy may be significantly impacted. Issuance of GA-CBDCs for example will give the general public direct access to central bank accounts and will therefore eliminate the need for financial intermediaries such as commercial banks in the given economy. Central banks must therefore reason about the type of CBDC to issue carefully in order not to disrupt the stability of existing financial systems both domestically and globally.

4.3.4 Implications for Monetary Policy

Lastly, issuance of CBDCs and their widespread adoption by end users will impact the implementation of monetary policy in many ways. We do not examine the full implications of CBDC issuance on monetary policy in this research. Nevertheless, central banks may need to carefully assess the potential impacts CBDC issuance may have on the implementation of monetary policy in order not to disrupt their underlying financial systems.

Chapter 5. Design Considerations for Afkoin

Drawing from CBDC research best practice approaches discussed in Opare and Kim [146], the specific requirements of the ECOWAS single currency program, and payment system requirements of ECOWAS member States (using Ghana's GIS system as a benchmark), the following design considerations are proposed for the Afkoin CBDC platform.

5.1 General Considerations

Printing and distribution of paper-based currency involves a laborious process that is costly and time consuming. For every dollar of bank note printed and distributed in the United States by the US Bureau of Engraving and Printing in 2019, it cost the US Federal Reserve 13.7% of the monetary value of the printed financial instrument [25]. Elsewhere in Italy, minting euro coins cost four times the face value of the coins [26]. Additionally, there are several security risks involved in the movement of cash from cash printing companies to central bank offices and authorized cash depository companies [24].

To ensure the efficient issuance and distribution of the Afkoin CBDC, afkoin tokens shall be issued and distributed on DLT. The Afkoin CBDC shall leverage the Internet and other communication protocols to ensure that the transmission and distribution of afkoin tokens are safe, secure and efficient.

Regarding the potential threat of quantum computers, the fully functional Afkoin CBDC platform shall leverage efficient PQC schemes such as the Crystals-Kyber KEM scheme and the Crystals-Dilithium digital signature scheme to mitigate against the threat of quantum computers.

The Afkoin CBDC, if and when adopted by ECOWAS member States, shall be the primary means of payment within the ECOWAS region. The Afkoin CBDC shall 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 in ECOWAS. The Afkoin CBDC platform shall therefore provide mechanisms for fulfilment of offline payments in the event of a disruption to the entire Afkoin platform resulting from natural and unnatural occurrences such as power outages which are prevalent in most ECOWAS member countries.

All Afkoin platform participants shall access the underlying Afkoin CBDC system using a range of web and mobile client applications in such a manner as to initiate new afkoin transactions, cancel pending transactions, check completed transactions, and check available balances.

All Afkoin transactions shall be recorded on a permissioned shared ledger accessible by Afkoin CBDC platform participants with the right access privileges. Afkoin CBDC platform data, data retention, data

privacy, and data publication shall be governed by data retention policies and laws of ECOWAS member States as well as globally accepted general data protection regulations.

Afkoin platform participants shall include the WACB, ECOWAS NCBs and PSPs operating within the ECOWAS. Additionally, software, programming codes and related technologies that enable the efficient functioning of the Afkoin CBDC platform shall be considered as Afkoin CBDC platform participants to the extent that the functionality of the Afkoin CBDC platform may be adversely impacted without such software, programming codes and related technologies.

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

5.2 Generating, Distributing and Transacting Afkoin Tokens

5.2.1 WACB

The generation and supply of afkoin tokens shall be in accordance with the Statutes of the WACB [17] as accented to by ECOWAS member States in December 2000. In accordance with the Statutes of the WACB, the Afkoin CBDC platform shall provide capabilties that enables the WACB to issue afkoin tokens as a common convertible currency to NCBs within the ECOWAS region.

The Afkoin CBDC platform shall provide capabilities that enables the WACB to onboard up to 15 ECOWAS NCBs and issue PKI certificates to the NCBs it onboards onto the platform. The role of the WACB in the issuance of PKI certificates on the Afkoin CBDC platform shall be as a root certificate authority (CA).

Afkoin tokens generated by the WACB shall be transmitted to NCBs via on-ledger wallets that are uniquely assigned to NCBs by the WACB.

The fully functional Afkoin CBDC platform shall provide the WACB with the requisite tools to enable the efficient implementation of monetary policy in the ECOWAS region. Additionally, the platform shall enable the WACB to act as the bank of last resort for ECOWAS NCBs. The WACB node on the Afkoin CBDC platform shall have capabilties to oversee the implementation of monetary policy in ECOWAS member States in a manner that is consistent with existing ECOWAS statutes.

As adoption of the Afkoin CBDC as legal tender may require new regulatory and legal statutes, the Afkoin CBDC platform shall provide the WACB node with capabilties to seamlessly implement new financial laws and regulations as accented to by ECOWAS member States.

5.2.2 NCBs

An NCB shall be responsible for the performance of national monetary policy activities on the Afkoin CBDC platform within a given ECOWAS member State, in a manner that is consistent with laid down ECOWAS statutes as well as the member State's national laws and regulations.

An NCB node on the Afkoin platform shall have capabilities to onboard as many PSPs as necessary in accordance with established national banking and finance laws and regulations. The Afkoin CBDC platform shall provide an NCB with capabilties to issue on-ledger wallets to PSPs and to manage the distribution of afkoin tokens to PSPs operating within its jurisdiction. The NCB node on the Afkoin CBDC platform shall have capabilties that enables it to perform the role of an intermediary CA that issues PKI certificates to PSPs.

An NCB shall provide a DLT-based RTGS platform with capabilties to transfer afkoin tokens from its on-ledger wallets to PSPs. The platform shall have capabilties that enable the transfer of afkoin tokens among platform participants. A fully functional DLT-based RTGS platform shall provide mechanisms to enable PSPs pledge reserve balances and/or tokenized collateral to an NCB in exchange for afkoin tokens. Additionally, the Afkoin CBDC platform shall provide capabilties that enables the redemption of afkoin tokens for central bank reserve balances or tokenized collateral. Afkoin tokens, once redeemed by an NCB shall be returned to the NCB's on-ledger wallet and shall be made available for future allocation to PSPs following the same "pledge-distribute" mechanism.

An NCB node on the Afkoin CBDC platform shall have capabilties to perform its statutory role and responsibility as payment system oversight authority in accordance with the national laws of the given NCB. For a given ECOWAS member State, Afkoin CBDC transaction authentication and validation shall be in accordance with existing national payment system laws, rules and regulations in a manner that is consistent with the achievement of the overall ECOWAS monetary policy and single currency objectives.

As adoption of the Afkoin CBDC as legal tender may require new regulatory and legal statutes, the Afkoin CBDC platform shall provide NCB nodes with capabilties to seamlessly implement new national financial laws and regulations that are consistent with the overall ECOWAS monetary policy and single currency objectives.

5.2.3 PSPs

For a given ECOWAS member State, the corresponding NCB shall have the sole responsibility of onboarding PSP participants. PSPs onboarded by the corresponding NCB shall become Afkoin CBDC platform participants and shall be issued on-ledger wallets and PKI certificates by the NCB as part of the onboarding process.

A PSP participant node shall have capabilities that enables it to pledge reserve balances or tokenized collateral to the NCB in exchange for afkoin tokens. A PSP participant node shall have capabilities that enables it to transfer afkoin tokens from itself to all other Afkoin CBDC platform participants except the WACB. Additionally, a PSP participant node shall have capabilities that enables it to redeem afkoin tokens for NCB reserve balances. All Afkoin CBDC platform capabilties available to a PSP shall be provided by the given NCB through its DLT-based RTGS platform.

5.3 Convertibility and Exchange Rate Considerations

It is assumed that if the Afkoin CBDC is adopted by ECOWAS member states, the adoption process would be in a phased approach whereby afkoin tokens are used concurrently with existing payment instruments in the given ECOWAS member State. For such a phased approach, Afkoin CBDC platform participants shall pledge reserve balances denominated in the national currency of the given member State in exchange for Afkoin tokens.

To ensure uniformity in the value of the *afkoin token vs. national currency* exchange rate and to minimize the volatility of the value of the Afkoin CBDC, the value of the Afkoin CBDC shall be pegged against a basket currencies. The Afkoin CBDC shall be pegged against IMF's SDR to ensure a stable value for afkoin tokens over the long term.

Firstly, the value of the underlying national currency pledged by an Afkoin platform participant (e.g. PSP) shall be converted to the prevailing rate of the SDR. Secondly, afkoin tokens corresponding to the US dollar value of the pledged and SDR-converted national currency value shall be issued to the pledging participant. Capabilities for the *pledge-exchange rate* conversion process shall be automated and shall be provided by the underlying DLT-based RTGS platform provided by the given NCB.

5.4 PFMIs Compliance Requirements

At all times, the Afkoin CBDC platform and its related transactions shall strictly adhere to the requirements of the PFMIs [50]. Specifically, transactions settled on the Afkoin CBDC platform shall achieve settlement finality, i.e. transactions committed to the underlying Afkoin CBDC shared ledger shall be deterministic, final and irrevocable.

The Afkoin CBDC platform shall provide mechanisms to ensure that the value of afkoin tokens transacted on the Afkoin platform is visible only to the counterparties involved the transaction in keeping with the operational risk requirement of the PFMIs.

Additionally, information about counterparties involved in a given transaction on the Afkoin CBDC platform shall be visible only to the involved counterparties in keeping with counterparty data privacy

goals of the PFMIs.

The above PFMI requirements notwithstanding, the Afkoin CBDC platform shall enable an NCB perform its oversight responsibilities in accordance with laid down banking and finance regulations in the given ECOWAS member State.

5.5 Usability, Extensibility and Interoperability Considerations

Research on technology adoption and usage indicates that the widespread adoption and use of a given technology or platform relies highly on the ease of use of such platforms [184]. In this regard, the Afkoin CBDC platform shall provide web and mobile application clients that are easy to use with minimal training or education. The platform shall include an online FAQ menu to allow platform users easily assimilate the working functionality of the platform.

The Afkoin CBDC platform shall be designed and developed in a manner that allows for the extension of the platform's capabilties to include new capabilities, features and services as may be dictated by future banking and finance regulations in ECOWAS member States.

The Afkoin CBDC platform shall provide capabilities that enables its integration with existing ECOWAS member States' FMIs.

5.6 Security Considerations

The Afkoin CBDC platform shall implement security functionalities that ensure a safe, secure and reliable transaction environment. The platform shall guarantee the safety and protection of Afkoin platform user information and transaction data so as to instill confidence in the platform and promote the quick adoption of platform across the ECOWAS region.

Notwithstanding, the need for a secure, safe, and reliable transaction environment, the Afkoin CBDC platform shall ensure a balance between the platform's security and usability considerations so that one consideration is not sacrificed at the expense of the other

5.7 Auditability and Non-Repudiation Considerations

The choice of DLT platform used to implement the Afkoin CBDC platform shall enable transaction traceability and auditability as required by ECOWAS member States banking and finance regulations. Once a transaction is committed to the underlying ledger, any modifications to the transaction shall be duly recorded on the ledger. Unless otherwise permitted by existing financial laws and regulations, the Afkoin CBDC platform shall prevent the alteration of a transaction once it is committed to the transaction ledger. .

5.8 Efficiency Considerations

As the target users of the Afkoin CBDC platform is the entirety of ECOWAS and its trading partners, the fully functional Afkoin CBDC platform shall be able to concurrently process transactions of orders of magnitude 10^{X} and at speeds superior or comparable to the most efficient FMIs in the world over the medium to long term.

5.9 AML/CFT Considerations

The fully functional Afkoin CBDC platform shall adopt and implement international Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) rules and regulations. To achieve the AML/CFT goals, the Afkoin CBDC platform shall implement an ECOWAS-wide identity management system that is accessible and verifiable by ECOWAS member States' NCBs and allied security agencies both in ECOWAS and other global jurisdictions.

5.10 Legal Considerations

Current banking and finance laws in most ECOWAS member States do not make express provisions for issuance and usage of digital currencies. The lack of appropriate legal statutes led to either outright ban or partial ban on digital currency trading activities in most parts of the world in the early days of the bitcoin bubble [185]. More recently, however, DLTs, the technology behind bitcoin and other leading digital currencies have become well understood and are viewed favorably by leading central banks across the world as discussed in Opare and Kim [146]. To provide the legal backing for issuance and adoption of the Afkoin CBDC, ECOWAS member States may need to review their existing banking and finance laws to include provisions for issuance, adoption and usage of digital currencies if the Afkoin CBDC is to be successful in the ECOWAS region.

Chapter 6. Afkoin CBDC Platform Requirement Specification

In this chapter, the requirement specification for the Afkoin CBDC platform is presented. Key themes or Epics, User Stories, Functional and Non-functional Requirements, Platform and System Design as well as System Performance Requirements are described in this chapter.

Primarily, we leverage experiences from Singapore's Project Ubin Phase II [161] and South Africa's Project Khokha [130] to design an Afkoin CBDC platform that is technically sound and technologically feasible to implement.

The Afkoin platform is designed to be implemented on Hyperledger Fabric as a wholesale FMI for domestic interbank transaction settlement among Afkoin platform participants. Afkoin platform participants include a virtual West African Central Bank (WACB), a virtual Bank of Ghana (BOG) as a representative ECOWAS NCB, and virtual PSPs such as commercial banks that are participants in Ghana's wholesale payment settlement system. The Afkoin platform provides capabilities for User Management, Wallet Creation, Afkoin Creation, Funds Transfer, Pledge, Redeem, Balance Enquiry, and Versioning of the underlying distributed transaction ledger.

A high-level overview of the Afkoin platform participants is presented in Fig.6.1.

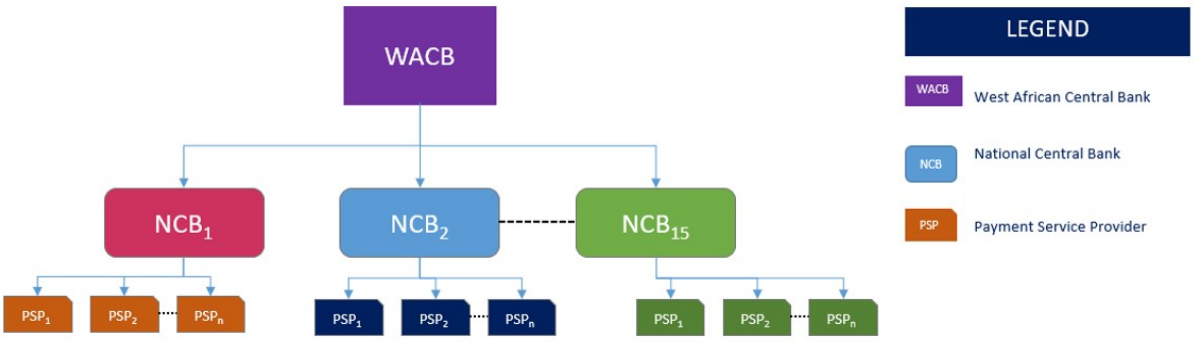


Figure 6.1: Afkoin Platform Participant High-Level Overview

Additionally, the Afkoin platform will be quantum-resistant in subsequent iterations, making it resilient against known quantum computing attacks. To achieve quantum-resistance, Afkoin will be implemented with the Crystals-Kyber public key encryption scheme and the Crystals-Dilithium digital signature scheme; both schemes being lattice-based Post Quantum Cryptography (PQC) schemes that advanced to the third round of the NIST PQC process [177].

The afkoin token will represent a claim on the assets of ECOWAS member States if and when adopted by ECOWAS. The afkoin token will perform the three functions of money namely, a unit of

account, a medium of exchange, and a store of value; and will serve as legal tender for transactions between ECOWAS member States. The afkoin token as a unit of account is pegged against the Special Drawing Right (SDR) to mitigate against the volatility associated with private sector-issued digital currencies. Additionally, afkoin will serve as legal tender for transactions between ECOWAS member States and non-member States.

6.1 High Level Requirements

The Afkoin platform is implemented from two requirements perspectives namely, functional requirement and non-functional requirement perspectives. Overall, a total of fourteen (14) functional and non-functional requirements or Epics are to be implemented on the Afkoin platform. Additionally, the 14 Epics are further broken down into 35 user stories reflecting the totality of the functions to be implemented with the Afkoin platform. A summary of the high-level requirements and user stories are provided below.

Functional requirements to be implemented include capabilities for Wallet Creation, Afkoin Creation, Manage Accounts, Funds Transfer, Pledge, Redeem, Balance Enquiry, and Versioning of the underlying transaction ledger.

Non-functional requirements to be implemented include mechanisms to guarantee Transaction Privacy, Transaction Security, Transaction Validity, Settlement Finality, System Performance, System Resiliency.

The high-level requirements of the Afkoin platform are presented in Fig.6.2.

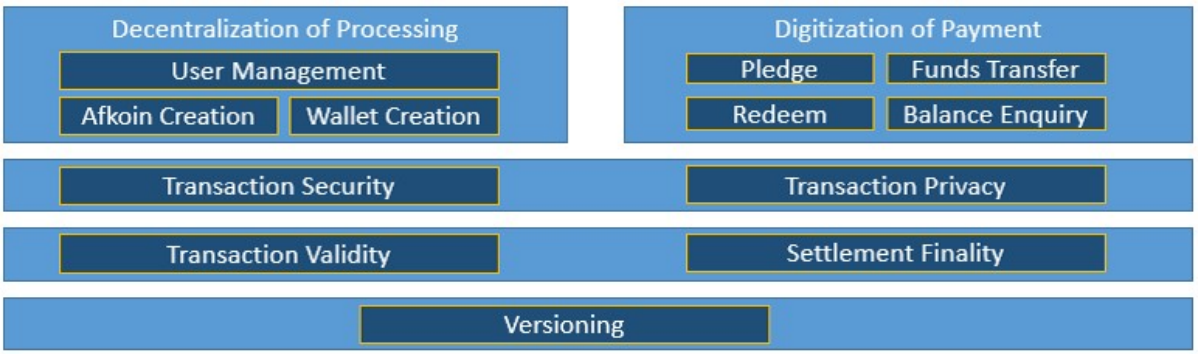


Figure 6.2: Afkoin High-Level Requirements

The high-level Afkoin platform requirements in Fig.6.2 are further described in Tab.6.1 and Tab.6.2 as below.

Furthermore, User Stories which represent the full capabilities of the Afkoin platform in-scope of this research are presented in Tab.6.3 and Tab.6.4.

Table 6.1: High-Level Functional Requirement Description

Epic	**Functional Requirement**
User Management	Onboard and manage Afkoin platform user accounts.
Wallet Creation	Create wallets for the storage of afkoin tokens.
Afkoin Creation	Create and distribute afkoin tokens to BOG.
Funds Transfer	Validate payment instructions sent by Afkoin platform users and execute payment instructions as final and irrevocable after successful transaction validation.
Pledge	Pledge tokenized collateral or reserve balances held in BOG reserve accounts in exchange for afkoin tokens.
Redeem	Exchange afkoin tokens for BOG reserve balances.
Balance Enquiry	Check available afkoin tokens or reserve balance.
Versioning	Update transaction ledger to the latest state with confirmed and/or rejected transactions.

Table 6.2: High-Level Non-Functional Requirement Description

Epic	**Non-Functional Requirement**
Transaction Privacy	Ensure privacy of all transactions on the Afkoin platform.
Transaction Security	Ensure that all transactions are quantum secure.
Transaction Validity	Implement consensus mechanisms that ensure that transaction instructions are valid before they are executed and committed to the transaction ledger.
Settlement Finality	Ensure that transaction settlement are deterministic, final and irrevocable.
System Performance	Ensure that system performance (throughput, scalability etc) exceeds current BOG key performance indicators.
System Resiliency	Ensure that the Afkoin platform is resilient and able to satisfy and/or exceed BOG key performance indicators for operating and managing the GIS system.

Table 6.3: Summary of Afkoin Platform Epics and User Stories (A)

Epic	**User Stories**
User Management	1. Onboard Afkoin platform user (i.e. WACB, NCBs/BOG and Banks) 2. Issue PKI certificates 3. Manage PKI certificates 4. Identify Afkoin platform user 5. Update Afkoin platform user information 6. Suspend Afkoin platform user
Wallet Creation	7. Create special WACB e-wallet 8. Create special BOG e-wallet 9. Creates e-wallet for Banks
Afkoin Creation	10. Issue afkoins tokens 11. Transmit afkoin tokens to NCBs/BOG
Funds Transfer	12. Initiate funds transfer to Afkoin platform user 13. Transfer funds across channels 14. Optimize funds transfer route 15. Receive funds from Afkoin platform user
Pledge	16. Pledge reserve balances or tokenized collateral to NCBs/BOG in exchange for afkoins tokens 17. NCB/BOG issues afkoin tokens to Bank in exchange for pledged collateral
Redeem	18. Bank initiates redemption of afkoin tokens for reserve balances or tokenized collateral 19. BOG redeems afkoins tokens and credit Bank's reserve account or tokenized collateral account 20. BOG returns afkoins tokens to its wallet
Balance Enquiry	21. Check Afkoin account balance 22. Check account balance of all Afkoin platform users 23. View all transaction history

Table 6.4: Summary of Afkoin Platform Epics and User Stories (B)

Epic	**User Stories**
Versioning	24. Update ledger state on pre-determined schedule 25. Check ledger state on pre-determined schedule
Transaction Privacy	26. Ensure system user transaction privacy 27. Ensure account balance privacy 28. Ensure transaction value privacy
Transaction Security	29. Ensure all transactions are quantum-secure
Transaction Validity	30. Confirm and validate outgoing transactions 31. Confirm and validate incoming transactions 32. Prevent double spending
Settlement Finality	33. Ensure completed transaction are deterministic, final and irrevocable
System Performance	34. Ensure that system performance (throughput, scalability etc) exceeds current BOG key performance indicators
System Resiliency	35. Ensure that system is resilient and able to exceed BOG key performance indicators

6.2 Afkoin Platform and System Design Overview

The Afkoin platform consists of a Fabric-based RTGS system, WACB node, a BOG node, four commercial bank nodes, and one Ordering Service node. Afkoin nodes are deployed independently on the Linode cloud computing platform. Additionally, Afkoin nodes are deployed over multiple geographical zones/locations. The multi-geographical-zone deployments are necessary to examine how node deployments across different geographical locations impacts overall Afkoin platform performance.

6.2.1 Ghana Interbank Settlement System

The Afkoin prototype is implemented in line with Ghana's wholesale payment system infrastructure requirements. Ghana's wholesale payment infrastructure is known as the Ghana Interbank Settlement (GIS) system. Ghana's GIS system is owned and operated by the BOG.

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 per cent.

Participants in the GIS system in 2018 included 34 PSPs, ARB Apex Bank, and the Social Security and National Insurance Trust (SSNIT). 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.

6.2.2 Afkoin Platform Working Mechanism

The Afkoin prototype is designed to be implemented on Hyperledger Fabric. The Afkoin platform is designed to leverage Fabric's channel feature to achieve transaction privacy as discussed in section 2.3.3. Using Fabric's channel feature, participants in a given transaction create a private and confidential communication medium for exchange of afkoin tokens and related transaction information on the Afkoin platform. The BOG is included as a participant in all channels to enable it perform its role as Ghana's supervisory and regulatory authority over payment and settlement systems.

Mechanisms for double spending prevention on the Afkoin CBDC platform are achieved through the use of endorsement policies. Each peer on the Afkoin platform maintains a full version of the transaction ledger; however only a subset of peers known as *endorsing peers* are responsible for executing Afkoin transaction proposals as well as performing data integrity checks.

Endorsed transactions on the Afkoin platform are then sent to the Orderer service node for further processing and transmission to the relevant transaction counterparties. The Orderer service node firstly packages endorsed transactions into blocks and then broadcasts them to all counterparties in an applicable Afkoin transaction channel. Upon receipt of the transaction blocks through the applicable channels, the relevant counterparties validate the transactions, commit them to the underlying ledger and update the state of the ledger.

6.2.3 Afkoin Platform Physical Architecture

The physical architecture of the Afkoin prototype being developed comprises of eight (8) compute nodes deployed on the Linode Cloud platform over multiple geographical regions. The Afkoin platform is implemented on Hyperledger Fabric v1.4. Each Afkoin experimental node setup consists of a dedicated 16GB RAM, 8 vCPUs and 320GB SSD storage running on Ubuntu Server 18.04LTS.

The physical node architecture of the Afkoin platform is presented in Fig.6.3.

6.3 Afkoin Node Building Blocks

A node on the Afkoin platform is made up of key building blocks including a web application client, Fabric peer, chaincodes, certificate authority (CA), and a transaction ledger.

The building blocks of an Afkoin node is presented in Fig.6.4.

6.4 Afkoin Issuance and Transaction Process Flow

Afkoin token issuance and transaction process flow on the Afkoin platform are described in this section.

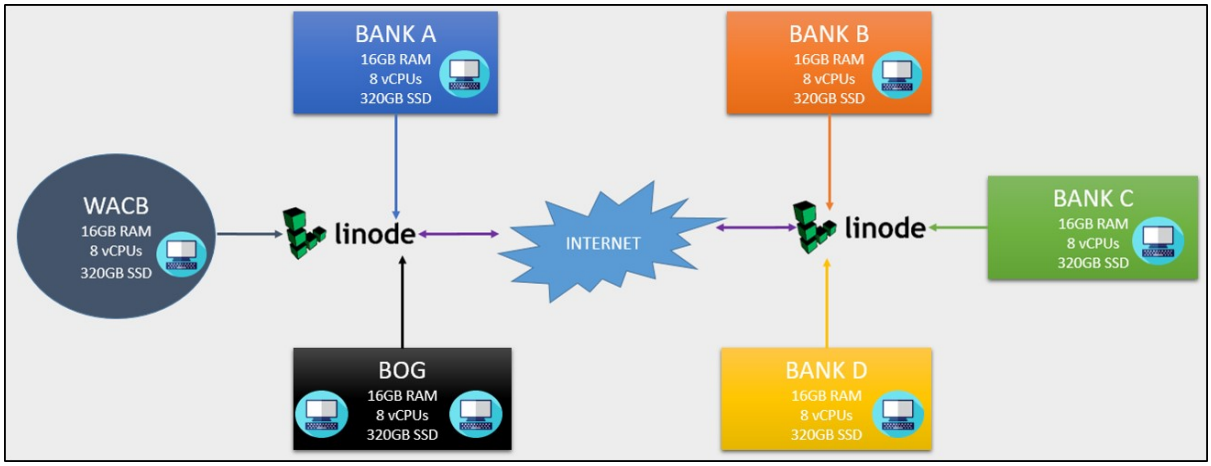


Figure 6.3: Afkoin Platform Physical Node Architecture

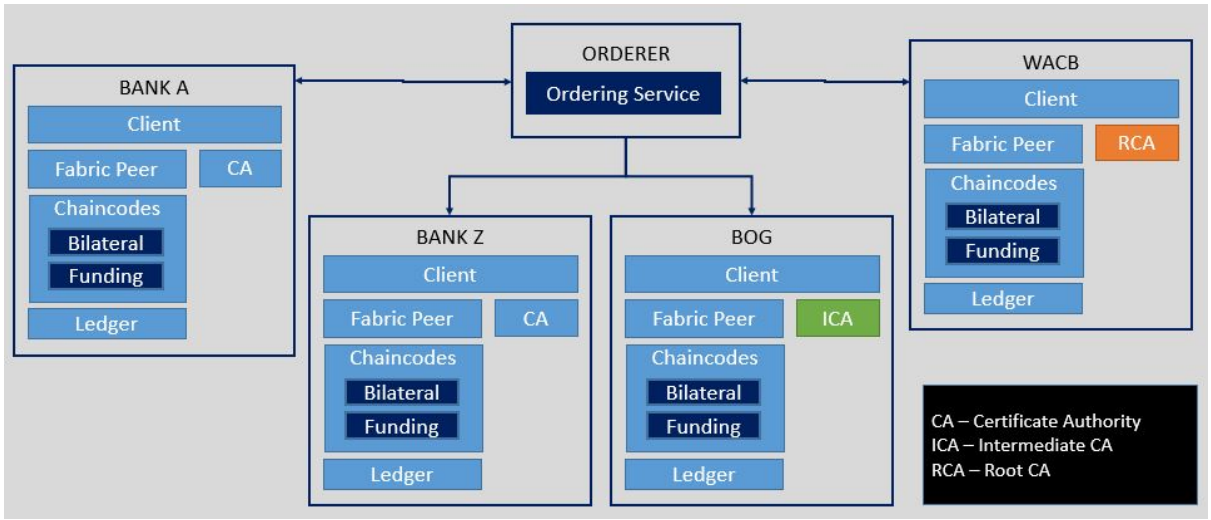


Figure 6.4: Afkoin Node Building Blocks

6.4.1 WACB Process Flow

- WACB onboards a central bank (i.e. the BOG) on the Afkoin platform.
- WACB creates and assign an on-ledger wallet to BOG.
- WACB which is the Root CA creates and issue an intermediary PKI certificate to BOG.
- WACB creates and issue afkoin tokens on the Afkoin platform.
- WACB transfers a pre-determined number of afkoin tokens to the BOG's on-ledger wallet.

.

The process flow for two essential activities of the WACB node is presented in Fig.6.5.

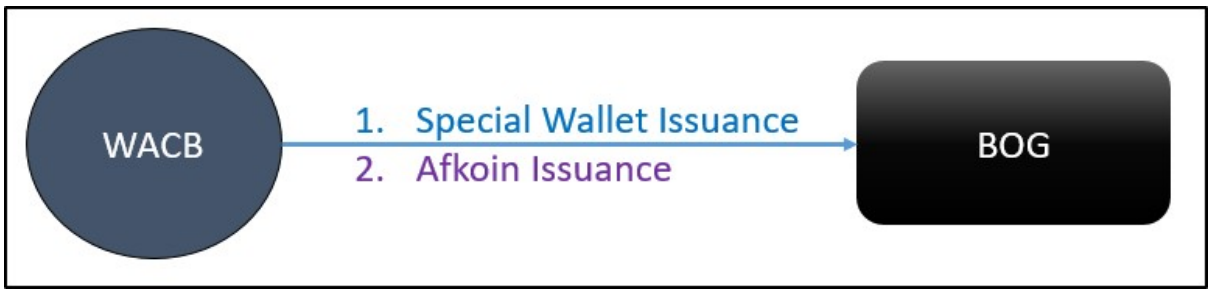


Figure 6.5: WACB Process Flow

6.4.2 BOG and Banks Process Flow

- The BOG creates and assign on-ledger wallets to each of four participating Banks (i.e. Bank A, B, C, and D) on the Afkoin platform.
- A participating Bank pledges cash (or tokenized collateral) held in their reserve accounts at the BOG to the BOG in exchange for afkoin tokens.
- BOG transfers the requisite amount of afkoin tokens to the pledging Bank.
- A pledging Bank transacts the afkoin tokens which it received from the BOG with other Afkoin platform participants (with the exception the WACB).

An abridged process flow for the BOG and Bank transactions are presented in Fig.6.6.

6.5 System Performance Requirements

The Afkoin platform is expected to achieve the following performance goals.

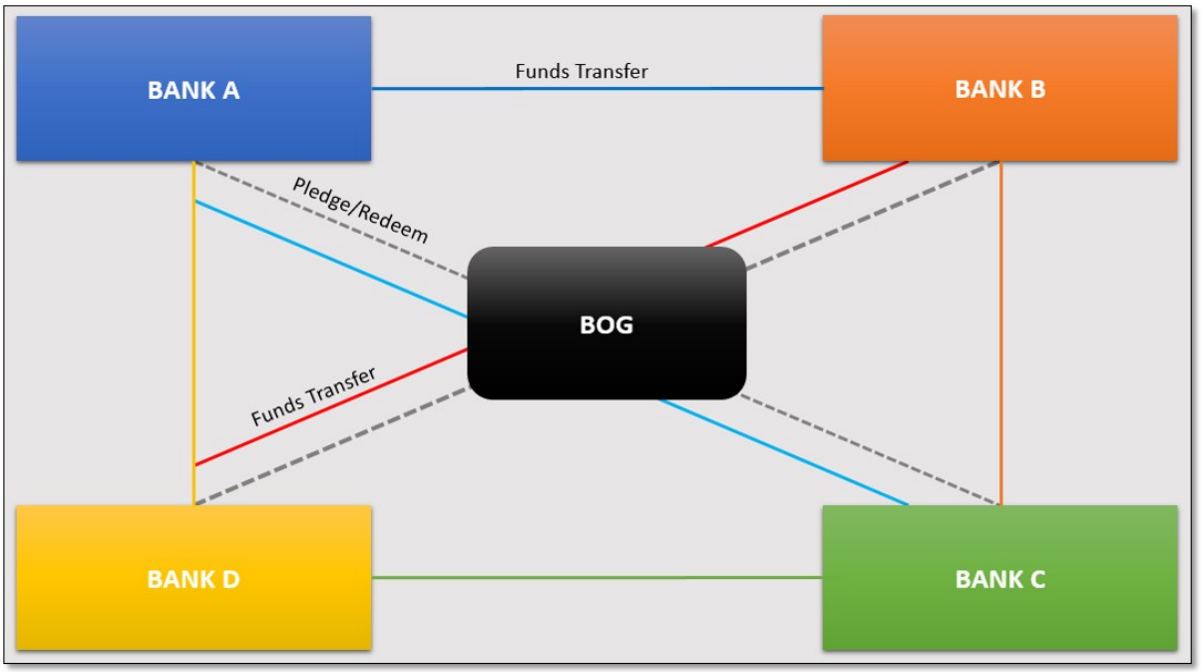


Figure 6.6: BOG and Banks Process Flow

6.5.1 Scalability Goals

The Afkoin prototype shall process at least twice the daily transaction volumes of the GIS system within the daily operating hours of the GIS system.

6.5.2 Throughput Goals

- Up to 95% of all transactions shall be propagated through the Afkoin platform within one second.
- Up to 99% of all transactions shall be propagated through the Afkoin platform in two seconds.
- Up to 100% of all transactions shall be propagated through the Afkoin platform at least twice faster than the transaction propagation requirements of the GIS system.

6.5.3 Settlement Finality Goals

The Afkoin prototype shall ensure that transactions are final and irrevocable once they are committed to the transaction ledger.

6.5.4 Privacy Goals

The Afkoin prototype shall enable the preservation of counterparty data privacy for all transactions on the Afkoin platform.

6.5.5 Privacy Goals

The Afkoin prototype shall enable the preservation of counterparty data privacy for all transactions on the Afkoin platform.

6.5.6 Oversight Goals

The Afkoin prototype shall provide mechanisms for the BoG to perform its oversight and regulatory responsibilities as it relates to the operation of the GIS system.

6.6 Afkoin Platform Minimal Viable Product

The development of the Afkoin CBDC PoC is currently ongoing. The below minimal viable product (MVP) shall be achieved once development and deployment of the platform is complete.

6.6.1 WACB Node/Client

The WACB node/client shall have capabilities to:

- Create up to 15 national central bank (NCB) nodes representing the number of ECOWAS member countries.
- Issue PKI certificates to NCBs
- Create and assign unique on-ledger wallets to NCBs.
- Create and issue afkoin tokens to NCBs.

6.6.2 BOG Node/Client

The BOG node/client shall have capabilities to:

- Create as many Bank nodes as necessary.
- Revoke or suspend a Bank whenever necessary.
- Issue PKI certificates to Banks
- Assign unique on-ledger wallets to each Bank it creates.
- Transfer afkoin tokens to Banks.
- Provide a Fabric-based RTGS platform to enable the transfer of afkoin tokens among Banks.
- Enable the settlement of at least 15,000 interbank transactions per day.

- Observe/oversee all transactions between Banks on the Afkoin platform.
- Ensure that Banks have enough afkoin tokens in their on-ledger wallets before they can transfer them.
- Prevent double-spending of afkoin tokens.
- Have a dashboard that can show the total number of transactions conducted on the Afkoin platform per minute, per hour, per month or per year.
- Have a dashboard that can show the total value of afkoin tokens transacted on its network per minute, per hour, per month or per year.

6.6.3 Bank Node/Client

A Bank node/client shall have capabilities to:

- Pledge collateral to the BOG in the form of reserve balance or tokenized collateral in exchange for afkoin tokens.
- Receive afkoin tokens from the BOG into their uniquely assigned on-ledger wallets.
- Transfer afkoin tokens on the Afkoin platform.
- Check their afkoin balance in their on-ledger wallets.
- Have a dashboard that can show the total number of transactions they have conducted on BOG's network per minute, per hour, per month or per year.
- Have a dashboard that can show the total number of transactions they have conducted on the Afkoin platform per minute, per hour, per month or per year.
- Have a dashboard that can show the total value of afkoin tokens they have transacted on the Afkoin platform per minute, per hour, per month or per year.
- Redeem afkoin tokens in exchange for BOG reserve balances.

6.7 Practical Implications of Afkoin Issuance in ECOWAS

In section 1.4, the rationale and potential benefits of leveraging DLT to issue the ECOWAS single currency is discussed. In this section, we examine other practical implications the issuance of Afkoin CBDC could have for ECOWAS.

6.7.1 Elimination of Currency Convertibility Barrier

Issuance of afkoin tokens will eliminate currency convertibility barriers [6] that exist in ECOWAS member States and most parts of Africa. Currency convertibility refers to the ability to freely exchange a given currency (e.g. Ghanaian Cedi) for a foreign currency (e.g. Nigerian Naira). Currency convertibility challenges are cited as one of the biggest barriers for intra-ECOWAS and intra-Africa trade. Currently, a direct exchange of the Ghanaian Cedi to the Nigerian Naira does not occur without first converting the Ghanaian Cedi to a benchmark currency such as the US Dollar. Conversion of the Cedi to the benchmark currency and from the benchmark currency to the Naira results in exchange rate losses that ECOWAS traders have to bear. As a result, ECOWAS and African businesses prefer to conduct trade activities with America, Europe and Asia instead of among ECOWAS member States or from within the African Union. Between 2015-2017 the total value of all exports from Africa to the rest of the world was a paltry USD 760 billion while the total value of imports into Africa from America totaled USD 5.14 trillion, from Europe USD 4.1 trillion and USD 6.8 trillion from Asia respectively [181]. Intra-African exports for the year 2017 is estimated at a mere 16.6% while exports from Africa to the rest of the world is ranges from 80%-90% between the same time period [181].Issuance of afkoin in ECOWAS would ensure that such exchange rate losses are eliminated and intra-ECOWAS trade increased over time.

6.7.2 Faster Economic Integration

In March 2018, 44 out of the 55 member States of the African Union signed into law the agreement establishing the *African Continental Free Trade Area* popularly known as the AfCFTA [183]. The goal of the AfCFTA is to "accelerate intra-African trade and boost Africa's trading position in the global market". Ghana has been designated as the host of the AfCFTA Secretariat, the headquarters of the AfCFTA. In August 2020, the Government of Ghana commissioned and handed over the AfCFTA Secretariat Building to the African Union [182]. Taking practical steps in adopting and issuing the Afkoin CBDC as single currency in ECOWAS will enable intra-ECOWAS trade and integration which can then spillover into the broader integration of the entire African region. A faster ECOWAS economic integration will be achievable as a result of improved efficiency in the distribution of afkoin tokens from ECOWAS NCBs to ECOWAS citizens and businesses. Afkoin tokens will be distributed through efficient distribution channels such as mobile wallets, thereby eliminating the bureaucracy, physical security risks and exorbitant costs central banks incur in moving paper currency one from location to the other. The efficient distribution of afkoin tokens will potentially lead to improved factor mobility among ECOWAS member States as well as increased intra-ECOWAS trade activities.

6.7.3 Loss of Monetary Policy Sovereignty

By issuing and adopting the Afkoin CBDC as legal tender in ECOWAS, ECOWAS member States would lose control over their ability to administer monetary policy independently of other ECOWAS member States. Such a loss in monetary policy sovereignty would mean that an ECOWAS member State may not be able to print money to address pressing national issues such as addressing the economic downturn ushered in by the COVID-19 pandemic or addressing basic infrastructural needs of the given ECOWAS member State. The benefits of a monetary union, however, far outweighs the downside of loss of monetary sovereignty [6]. With a monetary union, intra-ECOWAS trade may significantly increase [181]. Issues regarding currency convertibility challenges would be eradicated [6] while factor mobility across the ECOWAS region may lead to a more prosperous, independent ECOWAS region that no longer relies on foreign aid to achieve its development objectives.

The leadership of ECOWAS member States must therefore reason about the impact of a loss of monetary sovereignty quantitatively and from a broader perspective so as not to derail the ECOWAS single currency efforts.

6.7.4 Potential for Financial Exclusion

Depending on the medium of access and ease of use of the Afkoin CBDC platform, certain groups of people in the ECOWAS region may be deprived access to Afkoin-based financial services.

Elderly people who are not technologically inclined may be unable to use the Afkoin CBDC platform unless the design of the platform is simple and easy to use.

Additionally, in underserved and unserved parts of ECOWAS where universal internet access may still be a problem, different access mechanisms other than web or mobile applications may be required to ensure financial inclusion of the inhabitants in such regions. One practical way to address this challenge is to leverage Unstructured Supplementary Service Data (USSD) solutions to bring Afkoin-based services to people living in unserved and underserved parts of the ECOWAS region.

6.7.5 Cybersecurity

In the 2018 Global Cybersecurity Index [178] report by the ITU that measures the level of commitment by countries towards a safe and secure cyber infrastructure, a majority of the ECOWAS member States fell in the *medium* and *low* commitment categories. The widespread adoption of the Afkoin CBDC if and when issued by ECOWAS will largely depend on ECOWAS citizens' trust and confidence in the security and safety of the Afkoin FMI. It is therefore imperative that ECOWAS member States take the requisite steps to deepen their commitments towards implementing a safe and secure cyber environment within the ECOWAS region to ensure that an Afkoin CBDC platform will be safe and secure.

In conclusion, we contend that the benefits of issuing an Afkoin CBDC far outweighs the disadvantages, therefore ECOWAS should take practical steps towards the issuance of the Afkoin CBDC while implementing mitigating strategies to minimize the occurrence of the the potential disadvantages.

Chapter 7. Conclusion

In this dissertation, we have discussed about ECOWAS, the ECOWAS single currency program and our approach to achieving the goals of the ECOWAS single currency program through the use of DLTs.

In chapter 2, we discussed various DLT platforms and their suitability for the financial services industry. Then in chapter 3, we provided an introductory thesis on PQC and quantum resistant ledgers and discussed the NIST PQC Standardization Process. Subsequently in chapter 4, we discussed the concept of money and established a relationship between central bank money and CBDCs. Further in chapter 4 we indicated some of the practical implications to central banks for issuing CBDCs. Following a thorough review of existing ECOWAS legal statutes and institutional arrangements for the ECOWAS single currency program; and leveraging Ghana's wholesale payment system as a benchmark RTGS platform, we proposed preliminary design considerations for the Afkoin CBDC in chapter 5. Then in chapter 6, we provided a technical requirement specification for the development of the Afkoin CBDC prototype based on the design considerations presented in chapter 5.Lastly in chapter 6, we highlight some of the practical implications of issuing an Afkoin CBDC in ECOWAS.

Further, we have began the development of a minimum viable product (MVP) of the Afkoin platform in accordance with the Afkoin technical requirement specification in chapter 6.

Lastly in this chapter, we discuss our future research direction and open problems that may need to be examined in subsequent development of the Afkoin CBDC.

7.1 Future Research

As our immediate future research objective, the Afkoin minimal viable product discussed in section 6.6 is being implemented on Hyperledger Fabric using an agile software development approach that leverages the Scrum framework.

The Afkoin MVP is being developed over five sprints with each sprint lasting a maximum of two weeks. At the end of each sprint, a mini MVP *sprint output* shall be produced and evaluated through a *sprint review* and *sprint retrospective* to ensure conformance with the expected goal for the sprint. All sprint outputs shall undergo unit testing, functional testing and integration with other sprint outputs where necessary.

The Fabric-based Afkoin CBDC platform is being developed on Hyperledger v1.4 using Java and Node.js. Java SDK and Node.js SDK provided out-of-the-box by the Hyperledger Fabric Developer Community are being leveraged for the Afkoin prototype development. Chaincodes are being programmed in

Java while client applications for all platform participants are being implemented with Node.js. Other technologies being leveraged to implement the Afkoin CBDC prototype includes Docker containers and X.509 certificates among others. The quantum resistant feature of the Afkoin platform shall be implemented in future iterations using Crystals-Kyber as the KEM scheme and Crystals-Dilithium as the digital signature scheme.

The functional Afkoin CBDC MVP shall be hosted at www.afkoin.org.

7.2 Afkoin CBDC Platform Limitations

The Afkoin CBDC prototype discussed in this research focuses primarily on domestic wholesale interbank payment settlement. We do not examine issues relating to liquidity-savings mechanisms, cross-border interbank payment settlement, cross-border retail payment settlement and domestic retail payment settlements. It is expected that future iterations of the Afkoin CBDC prototype development shall examine and address the current limitations.

Bibliography

[1] ECOWAS, "Treaty of the Economic Community of West African States (ECOWAS)," United Nations - Treaty Series. Lagos, 1976.

[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," West African Monetary Institute. WAMI. Available: http://www.wami-imao.org/sites/default/files/Accra%20Declaration.docx.

[4] WAMI, "Welcome to WAMI," West African Monetary Institute. WAMI. 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," West African Economic and Monetary Union. 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," West African Monetary Agency. June 2018. 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] S. Nakamoto. "Bitcoin P2P e-cash paper." Available: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[32] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 31, 2008. Available: https://bitcoin.org/bitcoin.pdf.

[33] 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.

[34] 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.

[35] V. Buterin, "Proof of Stake FAQ." Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.

[36] V. Buterin, "A Proof of Stake Design Philosophy." Available: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51.

[37] NIST, Blockchain Technology Overview, NISTIR 8202, October 3, 2018. Available: https://csrc.nist.gov/publications/detail/nistir/8202/final.

[38] S. Nakamoto. "Bitcoin v0.1 released." Available: https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.

[39] W. Engert and B. S. C. Fung, "Central Bank Digital Currency: Motivations and Implications," Bank of Canada, Ottawa, 2017.

[40] M. Bech and J. Hancock, "Innovations in payments," BIS Quarterly Review, March 2020. BIS. Available: https://www.bis.org/publ/qtrpdf/r_qt2003f.pdf.

[41] 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.

[42] G. Levy, "SPEAK BLOCKCHAIN: Become Fluent in Blockchain and Bitcoin," Blockchain Institute of Technology, 2017.

[43] 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.

[44] 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.

[45] P. Jain, "The ABCs of Kafka in Hyperledger Fabric," CodeBurst. Available: https://codeburst.io/the-abcs-of-kafka-in-hyperledger-fabric-81e6dc18da56.

[46] 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.

[47] JP Morgan Chase, "Quorum Whitepaper v0.2.pdf," 24 August, 2018. [Online]. Available: https://github.com/jpmorganchase/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf.

[48] T. Kuhrt. "Hyperledger Fabric." Hyperledger Fabric. https://wiki.hyperledger.org/display/fabric.

[49] R3. "Nodes-R3 Corda Master Documentation." Available: https://docs.corda.net/key-concepts-node.html.

[50] BIS, "Principles for financial market infrastructures ", April 2012. BIS. Available: https://www.bis.org/cpmi/publ/d101a.pdf.

[51] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies," Network and Distributed System Security Symposium 2016 San Diego, CA, USA, 28 May, 2016.

[52] WEF, "Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today?," 3 April 2019. World Economic Forum. Available: https://www.weforum.org/whitepapers/central-banks-and-distributed-ledger-technology-how-are-central-banks-exploring-blockchain-today.

[53] J. Chapman, R. Garratt, S. Hendry, A. McCormack, and W. McMahon. "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?," Financial System Review. 1-11.

[54] Blockstream, "Elements Project," Blockstream. Available: https://elementsproject.org/.

[55] Anquan Capital, "Anquan Permissioned Blockchain," Anquan Capital. Available: https://www.anquancapital.com/.

[56] Chain Inc., "Chain Core," Chain Inc. Available: http://fedchains.com/core/.

[57] Digital Asset, "The Digital Asset Platform - Non-technical White Paper," Digital Asset. Available: https://hub.digitalasset.com/digital-asset-platform-non-technical-whitepaper.

[58] JP Morgan Chase, "A permissioned implementation of Ethereum supporting data privacy," JP Morgan Chase. Available: https://github.com/jpmorganchase/quorum.

[59] R3. "The R3 Story." R3. Available: https://www.r3.com/about/.

[60] R3. "R3 (company)," R3. Available: https://en.wikipedia.org/wiki/R3_(company).

[61] R3. "Consensus and notaries," R3. Available: https://docs.corda.net/releases/release-M9.2/key-concepts-consensus-notaries.html.

[62] R3. "Nodes-R3 Corda Master Documentation." Available: https://docs.corda.net/key-concepts-node.html.

[63] N. Nawari and R. Shriraam, "Blockchain technology and BIM process: review and potential applications," Journal of Information Technology in Construction - ISSN 1874-4753. Available: https://www.itcon.org/papers/2019_12-ITcon-Nawari.pdf

[64] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," 17 April, 2018. Available: https://arxiv.org/pdf/1801.10228.pdf.

[65] Hyperledger Community, "Hyperledger Documentation (Release master)," 10 May, 2019. [Online]. Available: https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf.

[66] IBM Corp, "Protocol Specification - Hyperledger Fabric," 2016. IBM. Available: https://openblockchain.readthedocs.io/en/latest/protocol-spec/.

[67] ITU, "Distributed ledger technology use cases," ITU. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf.

[68] 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

[69] IBM, "What is quantum computing?," IBM. Available: https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/

[70] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," in Cryptology ePrint Archive, Report 2015/1075, 2015.

[71] M. Mosca and V. Gheorghiu, "The Quantum Threat: What Really Matters Today?," Security Education Conference Toronto , p. 24, 15 November 2017.

[72] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.

[73] 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/.

[74] P. Waterland, "Quantum Resistant Ledger (QRL)," November 2016. Available: https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf.

[75] 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

[76] 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.

[77] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in Proceedings of the 8th ACM conference on Computer and Communications Security, Philadelphia, 2001.

[78] L. Reyzin and N. Reyzin, "Better than BiBa: Short One-time Signatures with Fast Signing and Verifying," ACISP 2002. Lecture Notes in Computer Science, vol. 2348, pp. 28-37, 2002.

[79] J. Buchmann, E. Dahmen, E. Klintsevich, K. Okeya and C. Vuillaume, "Merkle Signatures with Virtually Unlimited Signature Capacity," ACNS 2007. Lecture Notes in Computer Science, vol. 4521, pp. 31-45, 2007.

[80] J. Buchmann, E. Dahmen and A. Hülsing, "XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions," PQCrypto 2011. Lecture Notes in Computer Science, vol. 7071, pp. 117-129, 2011.

[81] D. Bleichenbacher and U. Maurer, "On the efficiency of One-Time Digital Signatures," in Advances in Cryptology — ASIACRYPT '96, 1996.

[82] A. Hulsing, " W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes," Progress in Cryptology – AFRICACRYPT 2013, Vols. Lecture Notes in Computer Science, vol 7918, pp. 173-188, 2013.

[83] A. Perrig. The BiBa one-time signature and broadcast authentication protocol. In Eighth ACM Conference on Computer and Communication Security, pages 28–37. ACM, November 5–8 2001.

[84] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto and T. Schroeter, "Blockchained Post-Quantum Signatures," IEEE Conferences, pp. 1196-1203, 2018.

[85] D. Micciancio and O. Regev, "Lattice-based Cryptography," Post-Quantum Cryptography , pp. 147-191, 2009.

[86] M. Ajtai, "Generating Hard Instances of Lattice Problems," Proceedings of the 28th Annual ACM symposium on Theory of Computing, pp. 99-108 , 22-24 May 1996.

[87] T. Laarhoven, J. v. d. Pol and B. d. Weger, "Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems," IACR Cryptology ePrint Archive, vol. 2012, p. 533, 2012.

[88] 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/.

[89] L. Zhang and Y. Sang, "A Lattice-based Identity-based Proxy Signature from Bonsai Trees," International Journal of Advancements in Computing Technology, vol. 4, no. 20, pp. 99-104, 2012.

[90] 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.

[91] S. Agrawal, D. Boneh and X. Boyen, "Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE," Proceedings of the 30th annual conference on Advances in Cryptology, pp. 98-115 , 15-19 August 2010.

[92] 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.

[93] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, "Bonsai Trees, or How to Delegate a Lattice Basis," EUROCRYPT 2010: Advances in Cryptology, vol. 6110, pp. 523-552, 2010.

[94] CoinMarket Cap. "Cryptocurrency Market Capitalization." CoinMarket Cap. https://coinmarketcap.com/

[95] B. S. C. Fung and H. Halaburda, "Central Bank Digital Currencies: A Framework for Assessing Why and How," Bank of Canada, Ottawa, 2016.

[96] K. Lien, "The Major Central Banks." Investopedia, Sep 17, 2019, https://www.investopedia.com/articles/forex/06/centralbanks.asp.

[97] T. Segal, "Central Banks" Investopedia, May 21, 2019, https://www.investopedia.com/terms/c/centralbank.asp.

[98] ECB. "Virtual Currency Schemes," European Central Bank. October 2012. Available: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en
.pdf.

[99] V. Buterin, "Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform." Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[100] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm." Ripple Labs Inc, 2014. Available: http://www.cs.yale.edu/homes/jf/Schwartz.pdf.

[101] Tether Ltd., "Tether: Fiat currencies on the Bitcoin blockchain," May 3, 2018. Available: https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

[102] D. Mazieres, "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus," February 26, 2016. Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[103]

[104] World Economic Forum. "Central Bank/Macroeconomics DLT Research List." https://docs.google.com/document/d/1c8iGtoG7BkPriufnIPELEWvtZiNtouOyJp2IYjhAEY/edit.

[105] C. Barontini and H. Holden, "Proceeding with caution – a survey on central bank digital currency," 2019. BIS. Available: https://www.bis.org/publ/bppdf/bispap101.pdf.

[106] Deutsche Börse Group, "Deutsche Börse Group – company profile," Available: https://www.deutsche-boerse.com/dbg-en/our-company/deutsche-boerse-group.

[107] Bank of England, "One Bank Research Agenda," 25 February, 2015. Available: https://www.bitcoinnews.ch/wp-content/uploads/2013/12/discussion.pdf.

[108] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies," in Network and Distributed System Security Symposium 2016 San Diego, CA, USA, 28 May, 2019 2016.

[109] People's Bank of China. "Digital Currency Symposium Held in Beijing," January 20, 2016. Available: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html.

[110] N. Varshney, "People's Bank Of China Plans to Launch Its Own Digital Currency," January 20, 2016. Available: https://cointelegraph.com/news/peoples-bank-of-china-plans-to-launch-its-own-digital-currency.

[111] Payments Canada, Bank of Canada and R3, "PROJECT JASPER: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement," Payments Canada, Bank of Canada and R3, 2017. Available: https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf.

[112] Payments Canada, Bank of Canada and R3, "Project Jasper Primer," February 9, 2017. Available: https://www.payments.ca/sites/default/files/project_jasper_primer.pdf.

[113] Deutsche Bundesbank and Deutsche Börse AG, "BLOCKBASTER." Deutsche Bundesbank. Available https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf

[114] S. Kunesch. "MADRE: a Banque de France blockchain project." European Payments Council AISBL. https://www.europeanpaymentscouncil.eu/news-insights/insight/madre-banque-de-france-blockchain-project.

[115] Central Bank of Brazil, "Distributed ledger technical research in Central Bank of Brazil," August 31, 2017. Central Bank of Brazil. Available: https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledge_technical_research_in_Central_Bank_of_Brazil.pdf

[116] D. Mills, K. Wang, B. Malone, A. Ravi, J. Marquardt, C. Chen, A. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian, M. Ellithorpe, W. Ng, and M. Baird. "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series 2016-095. Board of Governors of the Federal Reserve System, Washington DC, 2016. Available: https://doi.org/10.17016/FEDS.2016.095.

[117] MAS, "Project Ubin: Central Bank Digital Money using Distributed Ledger Technology," Monetary Authority of Singapore. Available: https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.

[118] European Central Bank and the Bank of Japan. "Project Stella," December 2016. Available: https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a2.pdf.

[119] European Central Bank and Bank of Japan, "Payment systems: liquidity saving mechanisms in a distributed ledger environment," September 2017. Available: https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf.

[120] European Central Bank and Bank of Japan, "Securities settlement systems: delivery-versus-payment in a distributed ledger environment," March 2018. Available: https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf.

[121] European Central Bank and Bank of Japan, "Synchronised cross-border payments," June 2019. Available: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf.

[122] Hong Kong Monetary Authority, "Welcome Speech at the Best Fintech Awards 2017," Available: https://www.hkma.gov.hk/chi/news-and-media/speeches/2017/03/20170327-1/.

[123] Hong Kong Legislative Council Commission, "Development of Financial Technologies," April 18, 2017. Available: https://www.legco.gov.hk/yr16-17/english/panels/fa/papers/fa20170418cb1-777-3-e.pdf

[124] Hong Kong Monetary Authority, "Research and Application," Available: https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/.

[125] A. Grym, P. Heikkinen, K. Kauko, and K. Takala, "Central bank digital currency," Bank of Finland. BoF Economics Review 5/2017. Available: https://pdfs.semanticscholar.org/9fa6/e095fa409d199e7aec8b50b657a7075fbe9e.pdf.

[126] Sveriges Riksbank, "The Riksbank's e-krona project (Report 2)," Sveriges Riksbank, Stockholm, October 2018. Available: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf.

[127] Central Bank of Uruguay, "Uruguayan e-Peso on the context of financial inclusion." Gerardo Licandro. November 16, 2018.

[128] Bank of Israel, "Report of the team to examine the issue of Central Bank Digital Currencies." Available: https://www.boi.org.il/en/NewsAndPublications/PressReleases/Documents /Digital%20currency.pdf.

[129] Danmarks Nationalbank, "Central bank digital currency in Denmark?," no. 28, December 15, 2017.

[130] South African Reserve Bank, "Project Khokha Fintech Report," Available: https://www.resbank.co.za/Lists/News%20and%20Publications/Attachment s/8491/SARB_ProjectKhokha%2020180605.pdf.

[131] SUPCACVEN, "Petro."https://whitepaperdatabase.com/venezuela-petro-cryptocurrency-ptr-english-whitepaper/.

[132] Bank of Lithuania. "Bank of Lithuania calls for proposals to develop a blockchain platform," March 16, 2018. Available: https://www.lb.lt/en/news/bank-of-lithuania-calls-for-proposals-to-develop-a-blockchain-platform.

[133] Bank of Lithuania, "Pre-commercial procurement," October 2, 2019. Available: https://www.lb.lt/en/pre-commercial-procurement.

[134] Bank of Lithuania. "LBChain project: six financial products already being tested." July 4, 2019. Available: https://www.lb.lt/en/news/lbchain-project-six-financial-products-already-being-tested.

[135] A. M. Maechler, "The financial markets in changing times Changes today and tomorrow: the digital future," 5 April 2018. Swiss National Bank. Available: https://www.snb.ch/en/mmr/speeches/id/ref_20180405_amr/source/ref_20180405_amr.en.pdf

[136] Norges Bank, "Central bank digital currencies," Norges Bank Papers, no. 1/2018.

[137] G. Bascand, "In search of gold: Exploring central bank issued digital currency," The Point Conference, 26 June 2018.

[138] Bank of Thailand, "Project Inthanon Phase 1," 2019. Available: https://www.bot.or.th/Thai/PaymentSystems/Documents/Inthanon_Phase1_Report.pdf.

[139] Monetary Authority of Singapore, Bank of Canada, and Bank of England. "The Bank of Canada, Bank of England and Monetary Authority of Singapore share assessment on emerging opportunities for digital transformation in cross-border payments." Available: https://www.mas.gov.sg/news/media-releases/2018/assessment-on-emerging-opportunities-for-digital-transformation-in-cross-border-payments.

[140] Monetary Authority of Singapore, Bank of Canada, and Bank of England, "Cross-Border Interbank Payments and Settlements: Emerging opportunities for digital transformation," 15 November 2018. Available: https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf.

[141] Y. S. Kim and O. Kwon, "Central bank digital currency and financial stability," BOK Working Paper, no. 2019-6, February 2019.

[142] N. Yanagawa and H. Yamaoka, "Digital innovation, data revolution, and central bank digital currency," Bank of Japan Working Paper Series no. 19-E-2, February 2019.

[143] Bank of Canada and Monetary Authority of Singapore, "Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies." Available: https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf.

[144] European Central Bank. "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures," ECB Occasional Paper Series No 223. May 17, 2019. Available: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223 3ce14e986c.en.pdf.

[145] Aurora Labs, "Aurora: A Decentralized Financial Institution Utilizing Distributed Computing and the Ethereum Network," Aurora Labs, 2018.

[146] 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.

[147] M. Bech and R. Garratt, "Central bank cryptocurrencies," BIS Quarterly Review. 55-70. September 2017 BIS. Available: https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

[148] Bank for International Settlements, "Central bank digital currencies," 2018. BIS. Available: https://www.bis.org/cpmi/publ/d174.pdf.

[149] Payments Canada, "High-Value System (LVTS) Participants," Available: https://www.payments.ca/our-directories/high-value-system-lvts-participants.

[150] Payments Canada, "What We Do," Available: https://www.payments.ca/about-us/what-we-do.

[151] Payments Canada, the Bank of Canada, TMX Group, Accenture and R3, "Jasper Phase III: Securities Settlement Using Distributed Ledger Technology," Available: https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf.

[152] TMX Group, "TMX Group Companies," TMX Group. Available: https://www.tmx.com/tmx-group/tmx-group-companies.

[153] TMX Group, "The Canadian Depository for Securities," TMX Group. Available: https://www.cds.ca/.

[154] Deutsche Bundesbank, "Organization," Available: https://www.bundesbank.de/en/bundesbank/organisation.

[155] Binance Academy, "Proof of Authority Explained," Available: https://www.binance.vision/blockchain/proof-of-authority-explained.

[156] Digital Asset, "Meet DA," Available: https://digitalasset.com/company/.

[157] ZILLIQA Team, "The ZILLIQA Technical Whitepaper," ZILLIQA Team. August 10, 2017. Available: https://docs.zilliqa.com/whitepaper.pdf.

[158] Central Bank of Brazil, "Gitlab Repository," Central Bank of Brazil. Available: https://gitlab.com/bacen.

[159] Central Bank of Brazil, "GitHub Repository," Central Bank of Brazil. Available: https://github.com/bacen.

[160] MAS, "Project Ubin: SGD on Distributed Ledger," Monetary Authority of Singapore. Available: https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin–SGD-on-Distributed-Ledger.pdf.

[161] MAS, "Project Ubin Phase 2 Report: Re-imagining RTGS," Monetary Authority of Singapore. Available: https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin–SGD-on-Distributed-Ledger.pdf.

[162] MAS, " Delivery versus Payment on DLT," Monetary Authority of Singapore. Available: https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-DvP-on-Distributed-Ledger-Technologies.pdf?la=en&hash=2ADD9093B64A819FCC78D94E68FA008A6CD724FF.

[163] MAS and ABS, "Ubin Docs," Available: https://github.com/project-ubin/ubin-docs.

[164] MAS and ABS, "Project Ubin," Available: https://github.com/project-ubin.

[165] R3. "Nodes-R3 Corda Master Documentation." Available: https://docs.corda.net/releases/release-V3.3/key-concepts-identity.html.

[166] ECB, "ECB, ESCB and the Eurosystem," European Central Bank. Available: https://www.ecb.europa.eu/ecb/orga/escb/html/index.en.html.

[167] ECB, "TARGET2," European Central Bank. Available: https://www.ecb.europa.eu/paym/target/target2/html/index.en.html.

[168] M. Herlihy, "Atomic Cross-Chain Swaps," Available: https://arxiv.org/pdf/1801.09515.pdf.

[169] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," Available: https://lightning.network/lightning-network-paper.pdfpage=30.

[170] Interledger Project, "JavaScript reference implementation of the Interledger protocol stack," Available: https://github.com/interledgerjs.

[171] Interledger Project, "Open-source reference ledger optimized for use with the Interledger protocol," Available: https://github.com/interledger-deprecated/five-bells-ledger.

[172] Bank of Thailand, "Project Inthanon Phase II," Available: https://www.bot.or.th/English/FinancialMarkets/ProjectInthanon/Documents/Inthanon_Phase2_Report.pdf.

[173] WAMI, "WAMZ Agreement," WAMI. Available: http://www.wami-imao.org/sites/default/files/WAMZ%20Agreement.docx.

[174] West African Monetary Agency, "ABOUT WAMA," [Online]. Available: https://amao-wama.org/aboutus/.

[175] 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.

[176] 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.

[177] G. Alagic et al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," 2020. Accessed: August 10, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

[178] ITU, "Global Cybersecurity Index 2018," 2018. Accessed: December 17, 2020. [Online]. Available: https://www.itu.int/dm_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[179] WAMI, "WACB Statutes",2000. Accessed: October 25, 2018. [Online]. Available: http://www.wami-imao.org/sites/default/files/WACB%20Statutes.docx

[180] KPMG, "Payment Developments in Africa," vol. 2, November 2016. Accessed: July 25, 2018. [Online]. Available: https://assets.kpmg/content/dam/kpmg/ng/pdf/dealadvisory/ng-KPMG-Payment-Developments-in-Africa-Volume-2.pdf

[181] UNCTAD, "Economic Development in Africa Report 2019: Made in Africa – Rules of Origin for Enhanced Intra-African Trade", October 29, 2019. [Online] Available: https://unctad.org/system/files/official-document/aldcafrica2019_en.pdf

[182] AFDB, "African Union Commission inaugurates AfCFTA permanent secretariat as launchpad for Africa's economic transformation," August 18, 2020. [Online] Available: https://www.afdb.org/en/news-and-events/press-releases/african-union-commission-inaugurates-afcfta-permanent-secretariat-launchpad-africas-economic-transformation-37379

[183] AfCFTA Secretariat, "About AfCFTA," [Online] Available: https://www.africancfta.org/aboutus

[184] Karahanna, Elena, et al. “Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs.” MIS Quarterly, vol. 23, no. 2, 1999, pp. 183–213., www.jstor.org/stable/249751. Accessed 27 Dec. 2020.

[185] The Law Library of Congress, ”Regulation of Cryptocurrency Around the World,” June 2018

Acknowledgments in Korean

I am thankful to God for his guidance and mercies throughout my doctoral degree program. I could do nothing without the help of the Lord Almighty.

I would like to sincerely thank Prof. Kwangjo Kim for suggesting that I do my PhD at his lab, the Cryptology and Information Security Lab, in the first place. I had many other plans after my Master's graduation at KAIST. This journey has been full of many interesting experiences. Many new networks and relationships have been built in and outside of KAIST, which experiences will be meaningful for the next stage of my career. I would also like to thank my current lab mates Jeeun Lee and Harry Chandra Tanuwidjaja; and former lab mates Rakyong Choi and Seunggeun Baek; and many others whom I had the privilege of meeting and working with throughout my PhD research period. I am indebted to you all for your numerous support and help throughout my PhD studies.

I am grateful to my beloved wife, Gertrude Opare, without whose support and encouragement I would not have made it this far. I am the one getting the doctoral degree, but you are the rockstar who made it happen. You have diligently and gracefully raised our two sons Edwin Opare and Ervin Opare almost single-handedly since the beginning of my Korean experience. I am eternally grateful.

I am thankful to Edwin and Ervin as well for being understanding and accepting that their father had to be away from home for a while. It has been a tough and uncomfortable process for all of you but you have preserved. I will make it up to you guys!!

I am thankful to my parents, parents-in-law, my siblings and siblings-in-law for the numerous ways they supported my family whiles I was away from Ghana pursuing my Master and PhD studies in Korea.

My sincere gratitude to Mr. Kwame Tawiah Wilson for taking me under his wings, mentoring me and providing me several opportunities in the world of business and politics. You have been many things to me including a father, a friend and a mentor. I am eternally grateful to you Sir.

Lastly, to Sharon Nabwire my former KAIST classmate; Sooman Park, my friend and business partner; Mujin Cheon my last surviving friend at KAIST; and all the many wonderful friends and acquaintances I made throughout my stay in Korea, I thank you enormously for your constant support and prayers all the way through.

Curriculum Vitae in Korean

이 름: Edwin Ayisi Opare

생 년 월 일: 1984년 10월 23일

본 적 지: Accra, Ghana

전 자 주 소: edwin.opare@kaist.ac.kr

학 력

1999. 01. – 2001. 07. Okuapemman Senior High School, Akropong-Akuapem, Ghana

2003. 09. – 2004. 08. Tver State Technical University, Tver, Russia (Russian University Entrance Program)

2004. 09. – 2009. 06. Southwest State University, Kursk, Russia (B.S.)

2011. 03. – 2013. 08. Korea Advanced Institute of Science and Technology, Daejeon, Korea (M.S.)

2016. 09. – 2021. 02. Korea Advanced Institute of Science and Technology, Daejeon, Korea (Ph.D.)

경 력

2009. 10. – 2010. 10. National Service Personnel, National Information Technology Agency, Ghana

2010. 11. – 2011. 07. Technical Consultant, CourtBridge Consulting Group, Ghana

2011. 05. – 2012. 05. Lecturer, Sikkim Manipal University, Ghana

2011. 08. – 2014. 12. CERT Manager, National Information Technology Agency, Ghana

2012. 04. – 2014. 12. Technical Lead, Ghana Open Data Initiative, Ghana

연 구 업 적

1. **Edwin Ayisi Opare** and Kwangjo 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.*.

2. **Edwin Ayisi Opare** and Kwangjo 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.

3. **Edwin Ayisi Opare** and Kwangjo 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.

4. **Edwin Ayisi Opare** and Kwangjo Kim, "Preliminary Design Considerations and Characteristics of Afkoin", *KAIST CAISLAB Technical Report No.TR-CIS-08/2019,)*, Last Revision: June 23, 2020, Daejeon, Korea. Available: https://caislab.kaist.ac.kr/publication/technicalreport/2019/Preliminary_Design_Considerations_and_Characteristics_of_Afkoin__c.pdf.

Appendix - Review of Relevant W-CBDC Research

Central banks' interest in CBDCs dates back to 2012 [98], with Bitcoin having only been invented in 2009. Central banks are generally the last entity in the FSI to adopt new technologies. This is because central banks must ensure that FMIs in their respective jurisdictions are secure, efficient, safe, and resilient [50]. The early demonstration of interest in blockchains and CBDCs by central banks within just three years of Bitcoin's invention is therefore very significant and requires close examination.

Although central banks' interest in CBDCs began in 2012, major attempts at developing CBDC PoC prototypes only began around 2015.

As this dissertation is focused primarily on W-CBDCs, excerpts of our major research publication on CBDCs [146] published in the peer-reviewed IEEE Access journal is provided as an appendix to this dissertation.

Selected CBDC Experiments

In the paper, [146], we surveyed CBDC research initiatives with completed PoCs from across the world. The key W-CBDCs experiments discussed in our paper [146] are presented in Table 7.1 and discussed in the subsequent section.

Table 7.1: Selected CBDC Experiment List

Jurisdiction	**Responsible Institution**	**Experiment Name**	**Type of CBDC**
Canada	Bank of Canada	Project Jasper	W-CBDC
Germany	Deutsche Bundesbank	BLOCKBASTER	W-CBDC
Brazil	Banco Central do Brasil	Project SALT	W-CBDC
Singapore	MAS	Project Ubin	W-CBDC
EU & Japan	ECB & Bank of Japan	Project Stella	W-CBDC
South Africa	SARB	Project Khokha	W-CBDC
Thailand	Bank of Thailand	Project Inthanon	W-CBDC
Canada & Singapore	Bank of Canada & MAS	Project Jasper–Ubin	W-CBDC

Broadly, we refer to all CBDC research initiatives as *CBDC research*, and specifically, all CBDC research initiatives with completed PoC prototypes as *CBDC experiments*. However, we use the terms interchangeably where applicable.

Project Jasper

Project Jasper [111], a W-CBDC experiment was launched in Canada in March 2016 through the partnership of Payments Canada, the Bank of Canada, a selected number of Canadian CMBs and R3, a blockchain-based company.

The motivation for Project Jasper was to build and evaluate the applicability of DLT for domestic wholesale interbank payments settlement in Canada [112].

Canada's wholesale interbank payments settlement system is called the *LVTS* [112].

The LVTS processes approximately 32,000 large-value interbank transactions per day or ten transactions per second at peak hours [111].

The LVTS is made up of seventeen participating FIs including the Bank of Canada [149]. It is owned and operated by Payments Canada [150], with the Bank of Canada providing oversight for its operation in accordance with international PFMIs [111]. All the CMB participants in Project Jasper were participants in Canada's LVTS.

Implemented over three phases, Project Jasper sought to understand how DLT could transform the future of payments in Canada [18].

Phase I and II of Project Jasper realizes the implementation of a DLT-based RTGS FMI that enables the domestic interbank transfer of a W-CBDC asset in Canada on Ethereum and Corda respectively.

Phase III of Project Jasper implemented a DLT-based prototype for integrated securities and payments settlement in Canada using Corda.

Jasper Phase I

Jasper Phase I was launched in March 2016 through the collaboration of Payments Canada, the Bank of Canada, five Canadian CMBs and R3.

The goal of Jasper Phase I was to build a DLT-based PoC prototype for domestic wholesale interbank payments settlement in Canada [111].

The transaction lifecycle of Jasper Phase I is presented in Figure 7.1.

In Jasper Phase I, distributed nodes were created for each participating entity on Ethereum.

The Bank of Canada was responsible for issuing digital depository receipts (DDRs); creating wallets for each CMB to hold DDRs; and approving or rejecting transactions through an autonomous *transaction agent* smart contract.

CMB nodes encompassed capabilities for creating accounts, initiating and executing transactions. All transactions on the Jasper Phase I platform were updated and synchronized onto each participating node regardless of whether a CMB is a counterparty to a transaction or not [111].

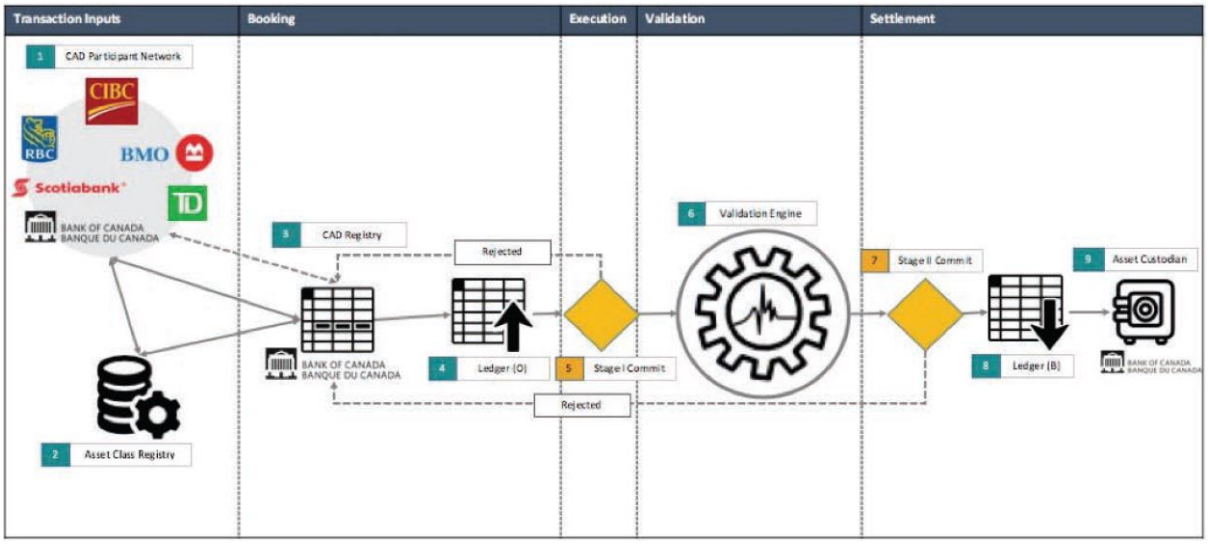


Figure 7.1: Project Jasper Phase I Transaction Lifecycle [111]

Payments Canada observed transactions on the Jasper platform in accordance with its mandate as the owner and operator of the LVTS.

The R3 node was responsible for accepting and recording all transactions onto a single shared ledger in Jasper Phase I.

In Jasper Phase I, a W-CBDC asset for interbank payments settlement was created to settle interbank transactions among participating CMBs of the project. The W-CBDC asset was called a DDR. Interbank payments on the Jasper platform were settled in DDR assets.

A DDR is a digital representation of the Canadian dollar. In Project Jasper, DDRs were issued by the Bank of Canada and backed one-for-one by cash pledged to the Bank of Canada by Jasper participating CMBs. DDRs therefore represented a claim on the assets of the Bank of Canada [53].

As part of Phase I, a DLT-based LVTS was built on Ethereum to provide the mechanism and capabilities for the transfer of DDRs among participating CMBs [53].

To conduct transactions on the Jasper platform, capabilities for pledging, generating, exchanging, redeeming and archiving DDRs were built into the Ethereum-based LVTS platform.

The capabilties enabled the:

- CMB node to *pledge* Bank of Canada money to the Bank of Canada for DDRs.
- Bank of Canada node to *generate* DDRs and send them to a requesting CMB.
- Recipient CMB to *fund* its DDR wallet with DDRs received from the Bank of Canada.
- CMB node to *exchange* DDRs with a transaction counterparty.
- CMB to *redeem* DDRs for Bank of Canada money.

- Bank of Canada to *archive* redeemed DDRs.
- Bank of Canada *return* new net balance of DDRs on-ledger.

The pledge of Bank of Canada money for DDRs and the redemption of DDRs for Bank of Canada money by the participating CMBs meant that there was no increase in money circulating in the Canadian banking system [17].

The consensus mechanism used in Jasper Phase I was PoW built into Geth [111]. To validate a transaction between two transacting parties, all members of the R3 Consortium (forty-two nodes) were required to validate the transaction before it was accepted and recorded onto the transaction ledger although only participating Canadian CMBs (five nodes) could transact DDRs on the Jasper platform [111].

Following the development of the Jasper Phase I PoC, the prototype was tested in a non-production environment with the following evaluation results.

- *Throughput*: The Jasper Phase I prototype was able to process approximately fourteen transactions per second. This throughput was sufficient to handle current LVTS peak hour throughput requirements [111]. However, in the event of transaction volume spikes, the prototype may not be able to support the throughput requirements due to the fact that R3's forty-two distributed nodes would each be required to validate transactions before they are committed to the ledger. The platform may therefore not be able to deliver the LVTS' newly heightened volume requirements.
- *Data Privacy*: The Jasper Phase I prototype did not fully support participating entities requirements for *data privacy*. Ethereum is a permissionless DLT platform, therefore all transaction data on the Jasper Phase I prototype could be viewed by all system participants, thereby violating the data privacy requirement (*Principle 17 - Operational Risk*) of the PFMIs.
- *Settlement Finality*: The Ethereum prototype did not provide for settlement finality. The PoW consensus algorithm is probabilistic, therefore there was always a small chance that a confirmed payment in Phase I could be reversed, invalidating the settlement irrevocability requirement (*Principle 8 - Settlement Finality*) of the PFMIs.

Jasper Phase II

To address the limitations of Jasper Phase I, Jasper Phase II [111] was launched in September 2016 to rebuild the Phase I prototype on a different DLT platform. Jasper Phase II was implemented on Corda.

Jasper Phase II attracted two more participating CMBs in addition to the original participants from Phase I.

In addition to the Phase I rebuild, Jasper Phase II implemented a Corda-based *atomic settlement* capability and an *LSM settlement* option. The transaction capabilties supported in Phase I were thus extended to include support for atomic and deferred net settlement options in Phase II.

In Jasper Phase II, distributed nodes were created for each participating entity on Corda. Three types of nodes were created: *a supervisory node, a notary node and a participant node* [111].

The Bank of Canada was designated as both the notary node and the supervisory node. The notary and supervisory nodes were combined into one system since both roles were performed by the same Bank of Canada entity. In its role as the supervisory node, the Bank of Canada had access to the entire transaction ledger with capabilities to query the ledger for monitoring and oversight purposes.

CMBs were each assigned a *participant node*. CMB nodes were updated and synchronized with only transactions records they were counterparty to.

Consensus on Jasper Phase II was achieved through the implementation of two Corda functions: a *validation function* and a *uniqueness function*.

Corda's validation function ensures that all details of a given transaction are verified and validated by the transacting parties and that the sender has the requisite amount of DDRs in their wallet to effect the transaction. In Jasper Phase II, the validation function was performed by CMB nodes that were counterparties to a transaction [111].

The uniqueness function was performed by the Bank of Canada in its role as the notary. Corda's uniqueness function ensured that DDRs proposed for exchange by CMBs had not been previously spent by the sender. The uniqueness function, thus prevents double spending by counterparties in Corda.

Following the development of the Jasper Phase II prototype, the platform was tested in a non-production environment with the following evaluation results:

- *Settlement Finality*: The introduction of a notary node ensured that settlement finality was achieved in Jasper Phase II.

- *Single Point of Failure*: The use of a trusted party to achieve settlement finality; however, introduced a *single-point-of-failure* problem into Jasper Phase II prototype. In the event that the Bank of Canada node was unavailable, no transactions could be processed on the Jasper Phase II platform.

- *Scalability*: Consensus was achieved much faster on Jasper Phase II as only counterparties to a transaction and the Bank of Canada node were required to establish consensus on a given transaction. This ensured that the problem of transaction scalability at peak hours was eliminated.

- *Data Privacy*: The use of a notary node also ensured that counterparty data privacy requirements

were met as transaction data were accessible by only the Bank of Canada and the CMBs involved in the given transaction.

- *Resiliency*: The resiliency of the Jasper Phase II prototype was diminished compared to Phase I. This is because participant nodes in Jasper Phase II recorded only transactions they were counterparty to. In the event that a participant node is unavailable or corrupted, the given node may incur extra costs to replicate its lost data from the Bank of Canada node. Participating CMBs may therefore have to invest in a high-availability system to mitigate against the impact of a corrupted node. Investment for high-availability node is also required for the Bank of Canada node to ensure that transactions can be processed on the Jasper Phase II platform at all times.

In conclusion, the participants of Project Jasper I and II emphasized that the true benefits and potential of DLT may only be realized if system reuse for the settlement of multiple asset classes is prioritized in CBDC experiment efforts.

Jasper Phase III

The Bank of Canada initiated Jasper Phase III [151] in October 2017 with the objective to leverage DLT for the exchange of multiple asset types.

Participants of Jasper Phase III were the Payments Canada, the Bank of Canada, TMX Group, Accenture and R3.

TMX Group is a Canadian financial services company that operates various securities exchanges. It is the owner of the Canadian Depository for Securities (CDS) [152].

The CDS is the national clearing and settlement hub for securities depository in Canada [153]. It administers the *CDSX*, Canada's securities settlement infrastructure. The Ontario Securities Commission, Quebec Securities Commission and the Bank of Canada have oversight responsibility over the CDS. The goal of Jasper Phase III [97] was to implement a DLT-based PoC prototype for an integrated securities settlement infrastructure that allows for the exchange of multiple asset types on a shared ledger.

Jasper Phase III developed capabilities for the atomic settlement of tokenized financial assets on an integrated LVTS-CDSX platform. The prototype was implemented on Corda v2.0 and hosted on Microsoft Azure.

Six types of nodes were established for the Jasper Phase III platform as follows:

- *Bank of Canada node*: Responsible for the tokenization of cash.
- *Notary node*: Responsible for the performance of the uniqueness function in order to achieve transaction consensus and eliminate double spending.

- *Payments Canada node*: Observer of cash transactions on the LVTS.
- *LVTS-member node*: Responsible for extending on-ledger credit to non-LVTS CDS members (such as broker-trader in the case of Jasper Phase III) for transaction settlement.
- *CDS node*: Responsible for the tokenization of equity. Additionally, it performs the role of central counterparty (CCP) in Jasper III in accordance with its legal mandate in Canada's FSI.
- *Broker-Trader node*: Participant in securities settlement transactions.

Overall, one node each were established for the Bank of Canada, Payments Canada and CDS respectively in accordance with the operational requirements of each entity. Additionally, fourteen broker-trader nodes and one LVTS-member node were established. The cumulative nodes established depict the relevant roles in Canada's equity settlement process [97]. Each node was hosted on a separate Microsoft Azure VM.

Jasper Phase III created role-based permissions and restrictions for a number of processes required for securities settlement to reflect participants access rights in a real-world securities settlement scenario. These included processes for: *creating, pledging, transferring and redeeming* equity or cash tokens.

Collectively, cash and equity tokens are referred to as DDRs. Individually, cash DDR refers to cash tokens and equity DDR refers to equity tokens respectively.

Jasper Phase III included the development of the following deliverables:

- Tokenized cash asset issued by the Bank of Canada and tokenized equity asset issued by the CDS for DvP settlement. Tokenized cash represents a claim on central bank money held at the Bank of Canada. Analogously, tokenized equity represents a claim on equity held at the CDS.
- Corda-based integrated settlement platform for the settlement of tokenized equity and cash assets.
- Capabilities for DvP settlement of tokenized equity assets against cash assets on the integrated security settlement system (SSS) with the CDS acting as the central counterparty (CCP).
- Capabilities for credit extension to broker-dealer by the LVTS-member participant.

The process for *pledging*, *transferring*, *redeeming* and *archiving* cash and equity DDRs follows a similar pattern as in Jasper Phase I and II.

The happy path for the tokenization of cash in Jasper Phase III is presented in Figure 7.2 and described as follows:

- *Step 1*: Bank1 initiates an on-ledger transaction to *pledge* cash to the Bank of Canada for cash DDR.

- *Step 2a*: The Bank of Canada reviews Bank1's on-ledger *pledge* request and verifies if Bank1 has sufficient funds in their off-ledger accounts. On successful verification, the Bank of Canada *transfers* the pledged amount from Bank1's off-ledger accounts on the Bank of Canada's books into an off-ledger "pool" account.
- *Step 2b*: The Bank of Canada *transfers* the corresponding cash DDR amount to Bank1's on-ledger wallet.
- *Step 3*: Bank1 *transfers* its on-ledger cash DDR to Bank2. Bank2 receives cash DDR in its on-ledger wallet.
- *Step 4*: Bank2 initiates a cash DDR *redeem* request and sends cash DDR to the Bank of Canada for redemption.
- *Step 5a*: The Bank of Canada verifies the cash DDR redemption request and issues an on-ledger receipt to Bank2 to confirm receipt of cash DDR.
- *Step 5b*: The Bank of Canada *transfers* the corresponding cash DDR amount in Bank of Canada money from the off-ledger pool account to Bank2's off-ledger account held at the central bank.

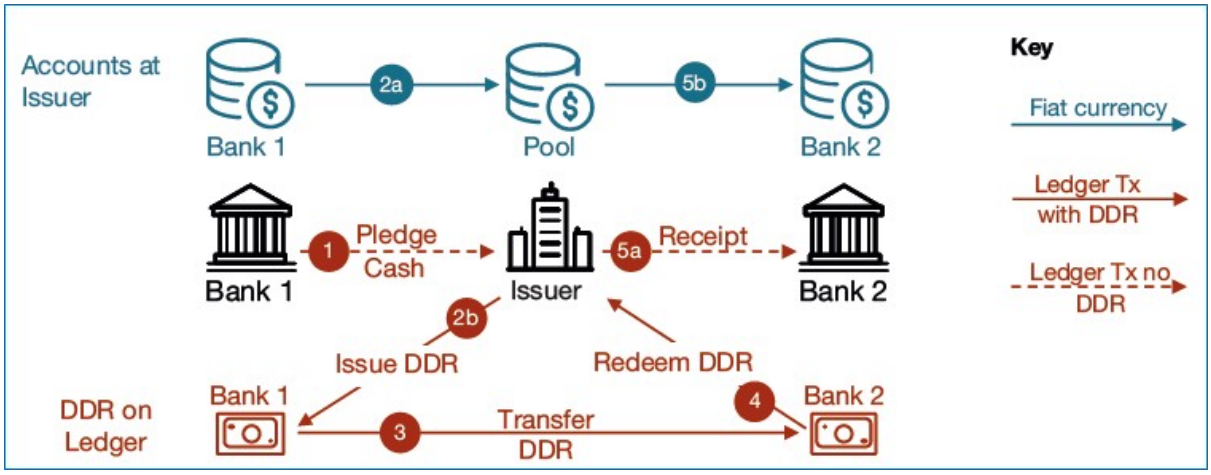


Figure 7.2: Project Jasper Phase III Asset Tokenization Process [151]

Following the development of the Jasper Phase III prototype, the platform was integrated with both the LVTS and the CDSX.

Further, system testing was conducted for the integrated FMIs from three efficiency perspectives: technical efficiency, operational efficiency and cash efficiency. The observations from each efficiency perspective are presented as follows:

- *Technical Efficiency*: a) Using DLT enabled the integration of the LVTS and CDSX FMIs for securities settlement without a large increase in the number of LVTS transactions processed per

day and without Payments Canada and CDS losing control and ownership of their respective FMIs. b) The shared ledger DvP settlement approach adopted for Jasper Phase III enabled a better cash-equity interactions among transaction parties compared to the existing securities settlement arrangement in Canada. c) A cloud-hosted non-enterprise version of Corda was used to implement the Jasper Phase III integrated SSS prototype with a minimal set of functions in order to quickly evaluate the applicability of DLT for securities settlement functions in Canada. As a result, a detailed assessment of system performance, resiliency, availability and security were out of scope for the project. However, the platform was used to settle 35,000 trade positions in a timely manner.

- *Operational Efficiency*: Due to the scope limitation of the Jasper Phase III experiment, cost savings related to the use of DLT for an SSS deployment could not be examined.

- *Cash Efficiency*: The atomic settlement functionality built into Jasper Phase III brought about immediate settlement finality in the securities settlement process, thereby enabling the reuse of equity and cash DDRs once a transaction was completed.

We present Jasper Phase III's end-to-end equity and cash settlement process in Figure 7.3.

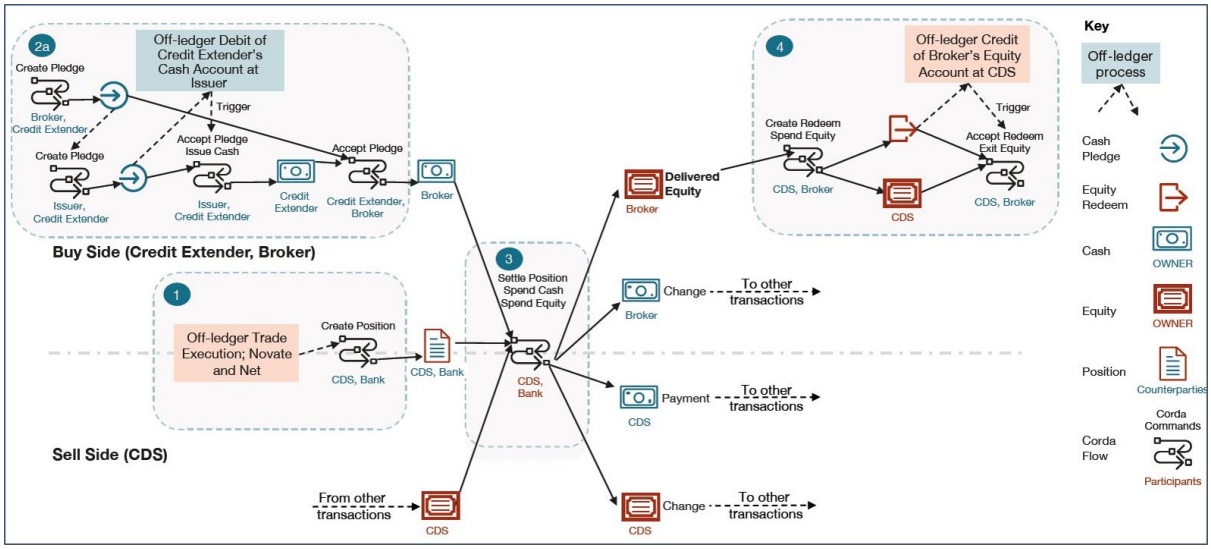


Figure 7.3: Project Jasper Phase III End-to-End Security Settlement Process [151]

The Jasper Phase III platform did not implement capabilties for posttrade activities.

Due to the limited scope and functionality of the Jasper Phase III integrated SSS prototype, a number of open questions on scope, business models and production readiness of DLT for FMIs remain that needs to be explored in future CBDC research.

Project BLOCKBASTER

Motivated by advancements in emerging technologies and their applicability to the FSI, the Deutsche Börse Group and Deutsche Bundesbank started Project BLOCKBASTER [113] in March 2016 to explore the possibility of leveraging blockchain to improve back office services in Germany's securities settlement FMI.

Deutsche Bundesbank is the central bank of Germany [154].

Deutsche Börse Group is one of the world's largest securities exchange centers [106]. It is the owner and operator of Clearstream, a securities clearinghouse based in Luxembourg.

The goal of Project BLOCKBASTER was to create a DLT-based SSS prototype for the settlement of securities for cash.

Project BLOCKBASTER implemented a full interbank bond issuance and lifecycle management prototype on two DLT platforms: Hyperledger Fabric and Digital Assets.

A high-level overview of Project BLOCKBASTER is presented in Figure 7.4.

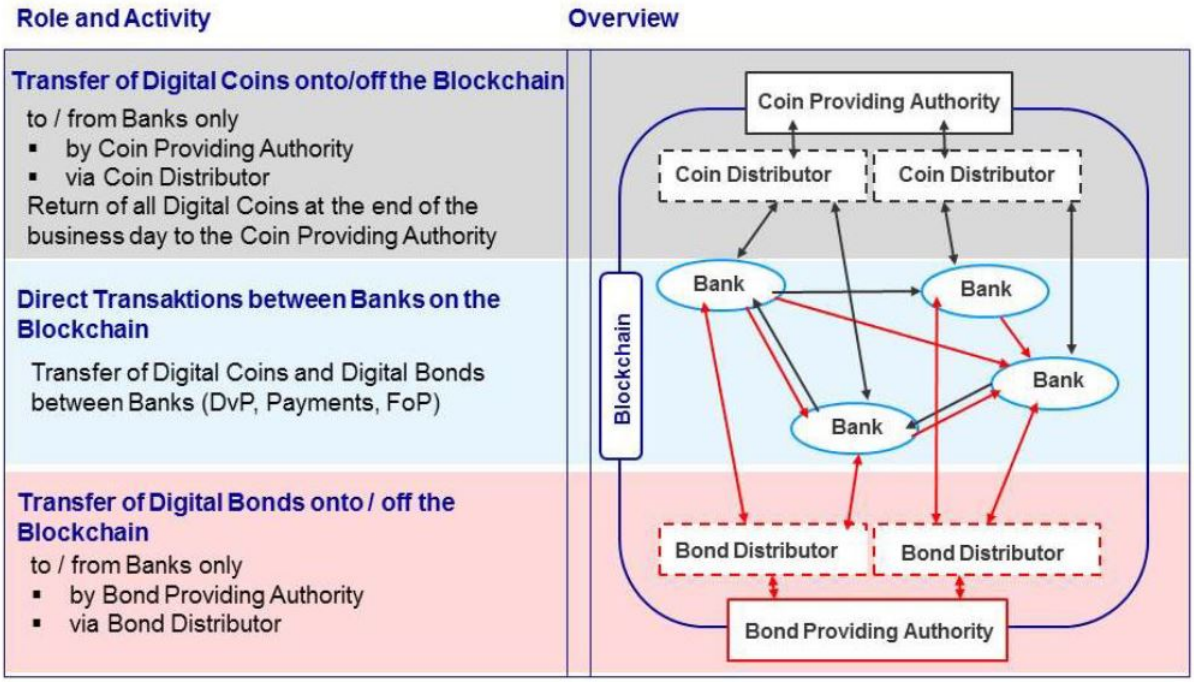


Figure 7.4: Project BLOCKBASTER High Level Overview [113]

The securities settled on Project BLOCKBASTER were tokenized bond and cash assets.

In order to enable rapid prototyping and assessment of the applicability of DLT for securities settlement, the scope of Project BLOCKBASTER was limited to the DLT-based settlement of matched trades in cash or securities only. Capabilities for interest rate payments to users (banks) were also built into the BLOCKBASTER platform.

Capabilities for bond pricing, market making and LSM settlement options were out of scope for Project BLOCKBASTER.

Project BLOCKBASTER established five key entities with the following responsibilities within the PoC prototype:

- *Coin Providing Authority* - The CPA was responsible for the issuance of *digital coins* used for settlement in Project BLOCKBASTER. Only the CPA could issue digital coins in Project BLOCKBASTER.

- *Coin Distributor* - The CD was an entity (bank) with capabilties to *pledge* and *transfer* money to the CPA in exchange for digital coins. CDs could transfer their digital coins to banks or back to the CPA for redemption for cash.

- *Bond Providing Authority* - The BPA was a central securities depository with responsibility for the issuance of *digital bonds* used for settlement in Project BLOCKBASTER. Only the BPA could issue digital bonds in Project BLOCKBASTER.

- *Bond Distributor* - A BD was an entity (bank) with capabilties to receive digital bonds issued by the BPA. BDs could transfer their digital bonds to banks or back to the BPA for redemption for actual securities.

- *Corporate Action Executor* - The CAE was an entity responsible for executing a corporate action such as interest payment in Project BLOCKBASTER.

Three types of settlements were supported on the Project BLOCKBASTER platform: payments (only transfer of digital coins), FoP security settlement (only transfer of digital bonds) or DvP security settlement (concurrent exchange of digital bonds and digital coins).

Digital coins circulating on the BLOCKBASTER platform were returned to the CPA's account at the end of the business day, therefore there was no increase in money circulating in the German banking system.

Digital bonds on the BLOCKBASTER platform, however remained there until they were consumed in subsequent transactions or returned to the BPA for redemption [113].

We discuss the experimental results of the Fabric and Digital Asset prototypes developed in Project BLOCKBASTER in the subsequent subsections.

Fabric-based Prototype

The Fabric-based BLOCKBASTER prototype was initially developed on Fabric v0.6, the current version of Fabric at the time of the prototype development. The prototype was later reconstructed on

Fabric v1.0 as that version became available.

Fabric provides for a pluggable consensus mechanism, therefore the PBFT-based consensus mechanism in Fabric was replaced with a proof-of-authority (PoA) [155] consensus mechanism in the BLOCKBASTER Fabric-based prototype.

Leveraging the PoA consensus mechanism, transactions in the Fabric v0.6 BLOCKBASTER prototype were validated by only the CPA and BPA nodes, providing for high transaction scalability. The Fabric v1.0 BLOCKBASTER prototype adopted Fabric's endorsement policy and ordering service to further improve transaction performance.

Both Fabric prototypes implemented two types of nodes: validator nodes and non-validator nodes. Validator nodes were the CPA and BPA nodes with responsibility for validating transactions and preventing double spending. Non-validator which were the CD and BD nodes were responsible for publishing transactions onto the shared ledger.

Nodes for the Fabric v1.0 prototypes were individually deployed in an EC2 instance hosted within one Availability Zone on AWS.

Subsequently, the performance of the Fabric v1.0 prototype was evaluated from the *throughput* and *latency* perspectives using the following base dataset:*1,000 bank-user profiles*, *500 bond instruments* and *200,000 transactions*. The 200,000 transactions were broken down into *100,000 DvP transactions*, *50,000 FoP transactions* and *50,000 cash transactions*.

The Fabric-based prototype was instantiated with the base dataset and allowed to ran for 35 minutes with the following key observations:

- *Throughput*: Transaction throughput and latency were functions of the chaincode. The simpler the chaincode, the higher the throughput and the lower the latency. The more complex the chaincode the lower the transaction throughput and the higher the latency.

- *Transaction Conflicts*: Significantly high throughput and minimal latency were recorded for all the transactions. However, several transaction conflicts were observed due to architectural changes between the Fabric v0.6 and v1.0 platforms. These conflicts were rectified in future versions of Fabric.

Digital Asset-based Prototype

Project BLOCKBASTER was rebuilt on the Digital Asset [156] (DA) DLT platform to evaluate the performance of the SSS prototype on a different DLT platform. The DA-based prototype was hosted on a DA in-house production environment hosted on AWS [113].

The DA DLT platform is made up of three layers; the application layer, the business logic layer,

and the distributed ledger (DL) layer. The platform also comprises of two key roles; the operator role and the participant role.

A high-level overview of the DA platform is presented in Figure 7.5.

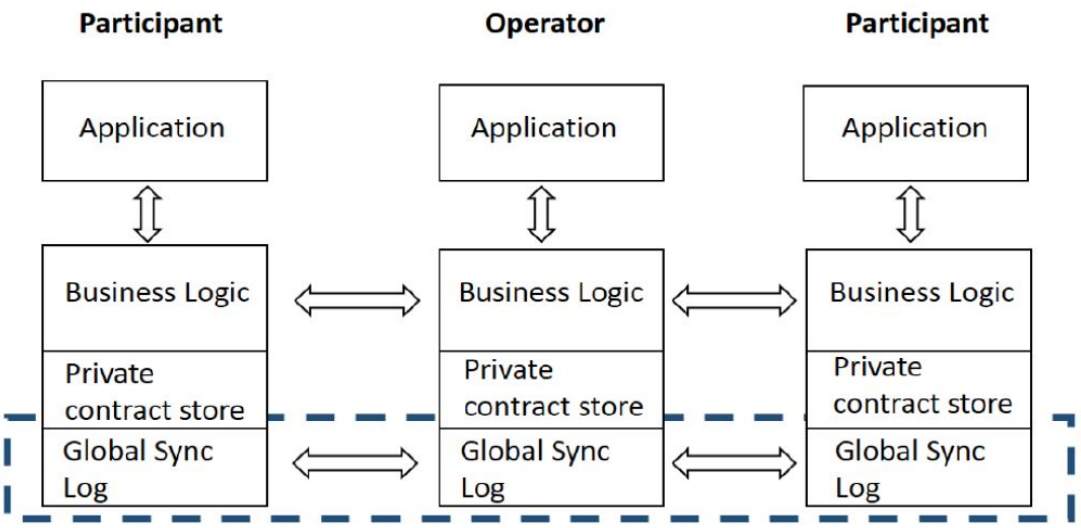


Figure 7.5: Digital Asset DLT Platform High Level Overview [57]

In Figure 7.5, the *application layer* provides capabilities for user-defined software interaction with other layers of the DA platform.

The *business logic layer* contains the business rules and smart contracts defined for a given DA network.

The *DL layer* stores transaction data in a DA network. It is made up of a *private contract store* (PCS) and a *global sync log* (GSL). The PCS is used to store all validated transaction data for which a given DA participant is counterparty to. The GSL records commitments and notifications across the entire DA network to guarantee platform auditability and integrity [57]. The GSL is the shared ledger in a given DA network.

The *operator* role in the DA DLT platform is responsible for defining, implementing and enforcing the rules of the DA network. In Project BLOCKBASTER, the operator function was performed by a special node called the *commiter node*. The committer node was responsible for verifying and writing all transactions to the GSL shared ledger.

The *participant* role refers to any entity that participates in activities on the DA DLT network. The CPA, BPA, CD, BD and CAE roles were all participant roles in the DA network.

Overall, three types of nodes were deployed for the DA-based BLOCKBASTER prototype: an *application node* that facilitates interactions between user-defined applications and the DA platform; a *participant node* which corresponds to DA platform's *participant role*; and a *committer node* which corresponds to the *operator role*.

An application node has a one-to-one relationship with a participant node.

In addition to the three types of settlements supported in the Fabric prototype, the DA-based prototype supported one more settlement type, *coupon payment*.

Following the rebuild of the DA-based BLOCKBASTER prototype, a functional assessment of the prototype was conducted from the throughput, latency and resource utilization perspectives using 30 different test scenarios and a varied number of bank-user profiles for each scenario.

All tests were ran for 30 minutes each with the base scenario ran over a 20 hour period to examine the platform performance consistencies over the period.

The node composition of the DA prototype experimental setup was as follows:

- *Operator node setup*: three DA nodes deployed on an in-house cloud environment hosted on AWS.
- *Participant node setup*: one CPA node; one BPA node; one CAE node; three CD nodes; three BD nodes; and 150 bank-user nodes.
- *Dataset*: 2,500,000 DvP transactions; 1,000,000 FoP transactions; 250,000 payment transactions; and 10,000 coupon payment transactions.

The following evaluation results were recorded for the functional testing of the DA prototype:

- *Throughput*: An increase in the number of transactions resulted in an increase in transaction throughput with a less than proportional increase in latency and memory usage.
- *Network Size*: An increase in participant nodes resulted in a less than proportional increase in latency and memory usage per node.
- *Scalability*: The DA-based prototype was able to meet stress testing and scalability benchmarks defined for the project.

Project SALT

The Banco Central do Brasil initiated Project SALT [115] in September 2016 with the objective to identify central bank use cases that could be implemented on DLT.

The Bank identified four potential use cases and elected to implement one of the use cases, the *Alternative System for Transactions Settlement* (SALT) on multiple DLT platforms as a backup to Brazil's RTGS system.

Participants of Project SALT included the Central Bank of Brazil and a selected number of CMBs.

Phase I of Project SALT included the use case identification and the PoC implementation on BlockApps, a fork of the Ethereum platform over a sixty day period beginning September 2016 [115].

Phase II of Project SALT implemented SALT on Fabric and Quorum over a forty-five day period beginning January 2017T [115].

Additionally, Project SALT implemented a tokenized Brazilian Real (BRL) W-CBDC asset. We refer to the tokenized BRL asset as BRL-DDR.

SALT Phase I

Having identified and selected one use case for implementation, the Central Bank of Brazil implemented Phase I of Project SALT, a backup RTGS system for wholesale interbank payment settlement with a minimal set of functionalities on BlockApps [115].

In SALT Phase I, both the central bank node and the CMB nodes were validating nodes. Consequently, both node types were equally responsible for achieving transaction consensus [115]. As it was implemented on BlockApps, the consensus mechanism used in SALT Phase I was the PoW consensus mechanism.

The SALT prototype had capabilities (smart contracts) that enabled CMBs to exchange BRL-DDR in a decentralized manner and achieving transaction consensus without relying on a central authority. Smart contracts implemented on SALT provided mechanisms to prevent double-spending by system participants. The Ethereum prototype is hosted at the Central Bank of Brazil's GitLab page [158].

Following the development and instantiation of the BlockApps prototype, the Central Bank of Brazil node generated the full quantity of BRL-DDRs to be transacted on SALT as well as digital wallets with corresponding balances for each CMB node [115]. All BRL-DDRs on the SALT Phase I platform were returned to the central bank once the system was terminated.

Testing and evaluating the SALT Phase I prototype, it was observed that the platform could not fully provide for system participants' requirements for data privacy.

The central bank adopted an inefficient mechanism to address the data privacy challenge which introduced further bottlenecks into the SALT Phase I platform. Adopting an alternative mechanism to resolve the data privacy limitation rendered the system inefficient in mitigating against double-spending. Additionally, transaction key protocol arrangements in SALT Phase I lacked strong forward secrecy unless keypairs were changed periodically [115].

SALT Phase II

The Central Bank of Brazil began Project SALT Phase II in January 2017 to examine the suitability of alternative DLT platforms for the selected SALT use case scenario implemented in Phase I. Additionally, SALT Phase II sought to address the data privacy challenge encountered in Phase I [115].

SALT Phase II was implemented on Fabric and Quorum.

a. Fabric

The first iteration of SALT Phase II was implemented on Fabric v0.6.

Consensus on the Fabric prototype [109] was achieved using the PBFT consensus mechanism. Overall, two types of nodes were supported on the Fabric prototype: validating nodes and non-validating nodes. Validating nodes were responsible for achieving transaction consensus while non-validating nodes only maintained a copy of the shared ledger.

The Fabric prototype had data privacy challenges similar to the BlockApps implementation in SALT Phase I.

The central bank attempted an implementation of SALT on Corda but discontinued the effort due to immaturity of the Corda platform at the time. Instead, the central bank implemented a Quorum prototype as part of SALT Phase II [22].

b. Quorum

The second iteration of Project SALT Phase II was implemented on Quorum.

The consensus mechanism used in the Quorum implementation was QuorumChain.

A major advantage with the Quorum implementation was code reuse from the BlockApps-based prototype as both BlockApps and Quorum are a fork of the Ethereum DLT platform.

The Quorum implementation provided stronger guarantees for data privacy and weaker guarantees for double-spending prevention.

Project Ubin

Project Ubin [117], Singapore's CBDC initiative has been implemented over multiple phases by MAS, Singaporean FSPs and industry collaborators since November 2016 to explore the potential benefits of DLT and its applicability to Singapore's FMIs.

MAS is the central bank and financial regulator in Singapore. MAS is the owner and operator of Singapore's RTGS system, the MAS Electronic Payment System (MEPS+). MEPS+ is the FMI used for domestic wholesale interbank payments settlement in Singapore as well as the settlement of Scriptless Singapore Government Securities (SGS) between MEPS+ participants [160].

Project Ubin Phase I [160] implemented a W-CBDC for domestic wholesale interbank payments settlement on the Ethereum DLT platform while Phase II [161] rebuilt the Phase I prototype with additional functionalities on Corda, Fabric and Quorum to address data privacy and settlement finality challenges encountered in Phase I.

In Phase III [162], Project Ubin implemented DvP capabilities for interbank securities and payments settlement on multiple DLT platforms.

The ultimate goal of Project Ubin was to provide capabilities for the exchange of a tokenized Singapore Dollar (SGD) asset on DLT and to evaluate the implications of such an exchange on Singapore's FMIs. The SGD asset was represented as a depository receipt (DR) similar to DDRs in Project Jasper. We use the term tokenized SGD asset and SGD-DR interchangeably.

Ubin Phase I

Project Ubin Phase I began in November 2016 through the collaboration of MAS, eight Singapore-based CMBs, the Singapore Exchange (SGX), Deloitte, R3 and BCS Information Systems [160].

The goal of Ubin Phase I was to implement an RTGS PoC prototype on Ethereum for the exchange of SGD-DR among Project Ubin participants.

To achieve the objectives of Project Ubin in a timely manner, Ubin Phase I was divided into two workstreams; a *technical workstream* responsible for implementing Project Ubin's DLT-based RTGS prototype for domestic interbank payment settlement; and a *research workstream* responsible for concurrently analyzing and documenting the implications of DLT on Singapore's FMIs in a production environment.

The Phase I prototype developed by the technical workstream included capabilities for the: issuance of SGD-DR by MAS; creation of wallets by MAS for CMBs; pledging and transferring of SGD-DR among Ubin Phase I participating CMBs and redemption of SGD-DR for central bank money on the Ethereum DLT platform.

The DLT-based RTGS prototype was further integrated with MEPS+ to examine its implications for Singapore's FMIs.

The consensus mechanism used in the Ubin Phase I prototype was the PoW consensus mechanism.

We present the high level architecture for Project Ubin Phase I in Figure 7.6.

In order for participating CMBs to pledge central bank money in their RTGS accounts held at MAS in exchange for SGD-DR, a special *DR Cash Custody* account was created by MAS. Pledged central bank money were stored in the DR Cash Custody accounts and the corresponding SGD-DR issued to the *pledging CMB*. Unlike Project Jasper which used "pool" accounts to store pledged central bank money, individual DR Cash Custody accounts were created for each participating CMB.

SGD-DR issued to a pledging CMB could be held on-ledger overnight [110] unlike Project Jasper which required the redemption of all DDRs intraday [17]. By holding on-ledger SGD-DR balances overnight, Project Ubin participants could conduct interbank transactions 24/7, independently of the operating hours of MEPS+ [110].

Project Ubin Phase I was completed with the achievement of the following deliverables:

- Development of an SGD-DR for domestic interbank payments settlement on an Ethereum network.

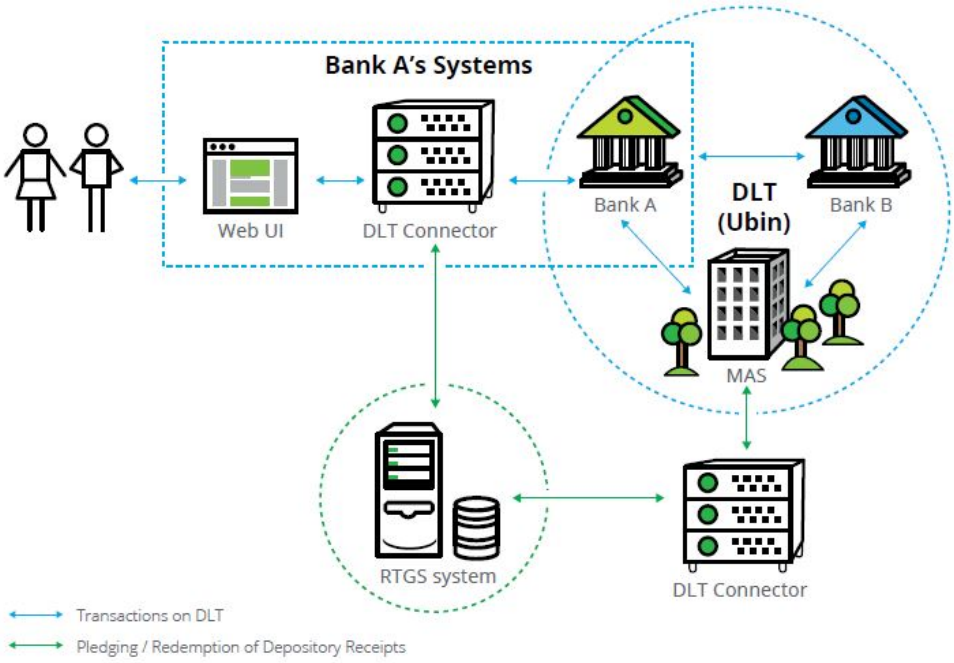


Figure 7.6: Project Ubin Phase I High Level Architecture [160]

- Implementation of an Ethereum-based RTGS prototype for settlement of domestic wholesale interbank transactions.
- Development of a new Smart Contract codebase and an evolution of Project Jasper's monetary model to allow for overnight storage of SGD-DR on the DL network.
- Successful end-to-end integration of the Ethereum-based RTGS prototype with MEPS+ in a test environment for the transfer of funds from participating CMBs' RTGS accounts to DR Cash Custody accounts and vice versa.

As it was implemented on Ethereum, Ubin Phase I could not provide for participants requirements for data privacy. Additionally, settlement finality could not be achieved on the Ethereum prototype as the PoW consensus mechanism is probabilistic.

Ubin Phase II

Project Ubin Phase II [161] was launched in July 2017 by MAS, the Association of Banks in Singapore (ABS), a consortium of eleven FSPs and five technology providers.

The goal of Project Ubin Phase II was to leverage alternative DLT platforms to address the data privacy and settlement finality challenges encountered in Ubin Phase I and to extend the functionality of the Phase I prototype to include capabilities for *gridlock resolution* and *LSM settlement* options [161].

Consequently, Ubin Phase II was concurrently developed on Corda, Fabric and Quorum with a detailed design specification document for each prototype published on MAS' GitHub page [163]. All

three prototypes were deployed on the Microsoft Azure cloud infrastructure. Overall, forty-one DLT-based nodes were deployed in VMs hosted on Microsoft Azure [161].

Project Ubin Phase II's codebase has been publicly released by MAS under Apache License Version 2.0. and hosted at [164].

A basic design concept employed in Ubin Phase II was the tokenization of cash assets (SGD-DR) to be settled immediately and the tokenization of *obligation* assets (OBL-DR) to be settled in cash in the future.

Project Ubin Phase II's functional architecture is presented in Figure 7.7.

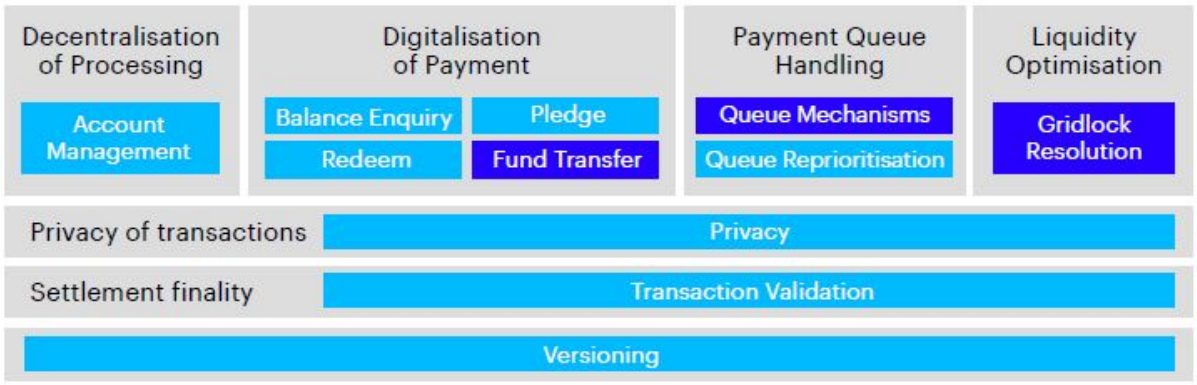


Figure 7.7: Project Ubin Phase II Functional Architecture [111]

Overall, core capabilities implemented in Ubin Phase II were organized under six functional categories: *Decentralization of Processing, Digitization of Payment, Payment Queue Handling, Liquidity Optimization, Privacy of Transactions and Settlement Finality.* The six functional categories were further decomposed into eleven epics or capabilities and implemented in each DLT prototype.

Ubin Phase II focuses on the assessment and evaluation of the *Fund Transfer, Queue Mechanisms and Gridlock Resolution* epics built into each of the three DLT-based prototypes via smart contracts.

a. Quorum

The Ubin Phase II Quorum prototype was implemented on Quorum v1.5.

Transaction consensus was achieved in the Quorum prototype using Quorum's Raft consensus mechanism.

Transaction privacy was achieved using a combination of Quorum Constellation and ZKP.

b. Corda

The Ubin Phase II Corda prototype was implemented on Corda v1.0.

Double spending prevention on the Corda platform was achieved through the use of a notary node, similar to other Corda prototype implementations examined in this paper.

Exchange of value between counterparties were initiated through the use of *confidential identities* [165] to guarantee counterparty transaction privacy. Using confidential identities, only the parties involved in a transaction were aware of the details of the transaction.

Each Corda node was allocated a vault where SGD-DR and OBL-DR states were stored. The UTXO model was used to represent SGD-DR and OBL-DR states in the Corda implementation of Ubin Phase II.

c. Fabric

The Ubin Phase II Fabric-based prototype was implemented on Fabric v1.0.1.

Double-spending prevention on the Fabric-based prototype was achieved through the use of endorsement policy, similar to previous Fabric-based prototype implementations examined in this paper.

Transaction privacy on the Fabric-based prototype was achieved through the use of channels which were provisioned by the ordering service.

Ubin Phase III

Project Ubin Phase III [162] commenced in August 2018 through the partnership of MAS, ABS, SGX, Anquan Capital, Deloitte and Nasdaq.

The goal of Ubin Phase III was to extend the experience gained in Project Ubin Phase I and II to implement DvP settlement capabilities for the cross-ledger settlement of tokenized securities in Singapore.

The securities settled were tokenized cash assets (SGD-DR) issued by MAS and tokenized SGS assets (SGS-DR) also issued by MAS.

The SGD-DR and SGS-DR assets were exchanged on a trade-by-trade basis over DLT-based SSS' implemented on multiple DLT platforms [162] .

The DLT platforms used to implement the Ubin Phase III prototypes were Ethereum, Fabric, Quorum, Chain and Anquan permissioned blockchain.

Overall, three interledger prototypes for cash and securities comprising of Quorum-Anquan, Ethereum-Fabric and Fabric-Chain were developed by Anquan Capital, Deloitte and Nasdaq respectively.

The prototypes were developed to fulfil Ubin Phase III's objectives to leverage DLT to:

- Facilitate interledger trading of tokenized securities in Singapore.
- Guarantee investor confidence in trading MAS-issued securities.
- Minimize counterparty risks in trading MAS-issued securities through the use of smart contracts to fulfil DvP trade obligations.
- Achieve DVP settlement finality.

In order to achieve Ubin Phase III's defined objectives, each cash-securities prototype implemented five core capabilities, namely *contract locks, account controls, secure secrets, dispute resolution* and *time boundaries*.

The *contract locks* capability provided mechanisms to *lock* SGD-DR and SGS-DR involved in an ongoing transaction (*Tx1*) so that they were not used in new transactions (*Tx2*) until *Tx1* was completed, thus, preventing double-spending and minimizing counterparty risks.

The *account controls* capability provided mechanisms to achieve settlement finality through the use of signatures under the ownership of the seller, buyer and MAS.

The *secure secrets* capability provided an extra layer of security for posttrade activities to achieve DvP finality. Secure secrets were generated by the RMO and sent separately off-chain to each of the transacting parties as a PDF file. Secure secrets were a function of the digital signatures of the counterparties involved in a given transaction.

The *dispute resolution* capability provided mechanisms for MAS in its role as *Arbiter* to autonomously arbitrate counterparty trade issues, thereby guaranteeing investor protection and confidence in trading MAS-issued securities.

The *time boundaries* capability provided mechanisms for trades to be concluded within pre-defined time windows as a way to minimize counterparty risks and achieve settlement finality.

We present the high-level architecture of Project Ubin Phase III in Figure 7.8.

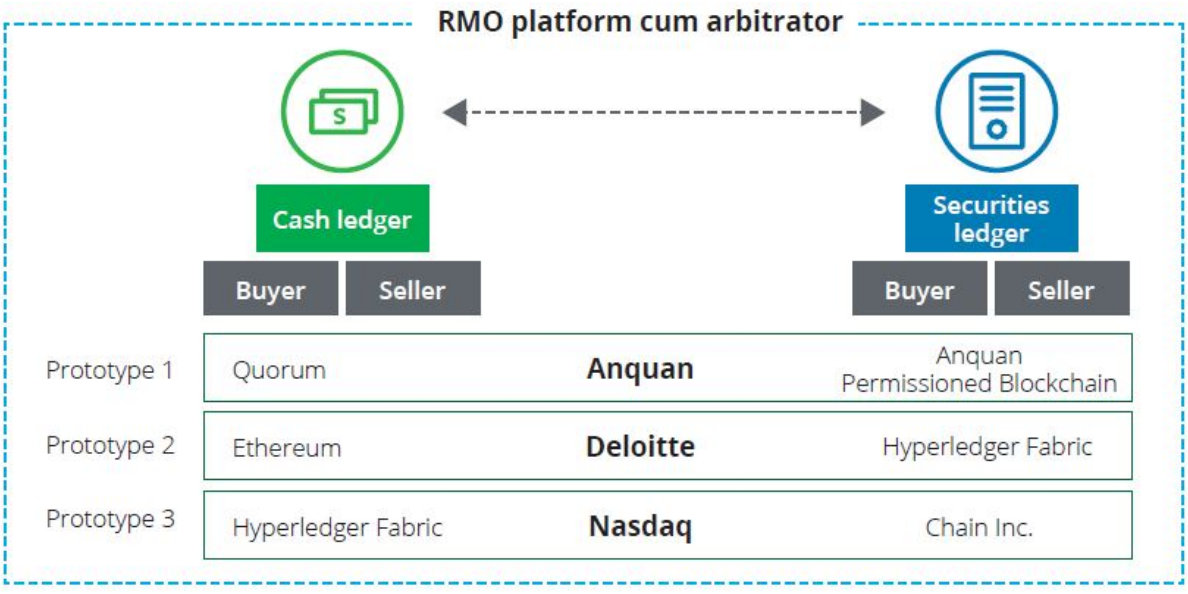


Figure 7.8: Project Ubin Phase III High Level Architecture [162]

Five key entities were established for the Ubin Phase III platform. The entity composition of the Ubin Phase III prototypes were as follows:

- *Recognized Market Operator (RMO)* - The RMO role was the owner and operator of the Ubin Phase III platform. This role was responsible for the smooth and efficient operation of the Ubin Phase III platform. At all times, the RMO was able to view all transactions on the Ubin Phase III platform and also act as an Arbiter for dispute resolution among system participants. The RMO holds one keypair each for the cash ledger and securities ledger. In Ubin Phase III, MAS performed the RMO role.
- *Cash Ledger* - The cash ledger was used for the issuance, storage and transfer of SGD-DRs. This ledger was managed by MAS.
- *Securities Ledger* - The securities ledger was used for the issuance, storage and transfer of SGS-DRs. This ledger was managed by SGX.
- *Buyer* - The buyer role was an exchange-registered trader who held accounts on both the cash and securities ledger as well as one keypair for each ledger.
- *Seller* - The seller role was an exchange-registered trader who held accounts on both the cash and securities ledger as well as one keypair for each ledger.

Having completed the development of the Ubin Phase III prototypes, the following DLT-based DvP securities settlement scenarios were executed and evaluated.

- *Scenario I*: Successful settlement.
- *Scenario II*: Failed settlement with automatic recovery.
- *Scenario III*: Failed transaction requiring arbitration.
- *Scenario IV*: Failed transaction with arbitration.

The Ubin Phase III prototype was able to successfully confirm the above scenarios.

We highlight some of the characteristics of the solutions developed by Anquan Capital, Deloitte and Nasdaq in the subsequent subsection.

a. Anquan Solution

Anquan Capital implemented its Ubin Phase III DLT prototypes using Quorum for the cash ledger and the proprietary Anquan [55] permissioned blockchain platform for the securities ledger respectively.

The Anquan DLT platform is a permissioned implementation of ZILLIQA [157], a high-throughput DLT platform developed from the ground up to address the limitations of the Ethereum DLT platform.

The consensus mechanism used on the securities ledger was the PBFT consensus mechanism while transaction privacy on the cash ledger was achieved through the use of ZKP.

Interledger exchange of value and transaction scalability was achieved through the use of the sharding technique and atomic swaps. Leveraging atomic swaps enabled the efficient exchange of the underlying securities across ledgers without the need for an Arbiter [161].

Additionally, the Anquan solution was integrated with the Ubin Phase II prototype.

b. Deloitte Solution

Deloitte implemented its Ubin Phase III DLT prototypes using Ethereum for the cash ledger and Fabric for the securities ledger respectively.

Transaction privacy on the securities ledger was achieved by leveraging channels, similar to the Fabric-based prototype examined in Chapter 7.2.

The Fabric prototype also provided a centralized key management service that allowed buyers and sellers to store their private keys in an escrow. The centralized key escrow service was provided by MAS. MAS would then use its digital signature to sign transactions on behalf of system participants using its key management service.

To enable transaction arbitration, the Deloitte solution leveraged smart contracts to implement a semi-centralized DVP settlement process.

c. Nasdaq Solution

Nasdaq implemented its Ubin Phase III DLT prototypes using Fabric for the cash ledger and the Chain Core DLT platform for the securities ledger respectively.

Chain Core [56] is an FSI-focused DLT platform developed from the ground up to enable a secure and efficient transfer of tokenized financial assets.

Nasdaq decoupled the DvP settlement processes from the underlying DLT platforms using smart contracts. The DvP settlement capability in the Nasdaq solution was therefore DLT-neutral, allowing it to be integrated with different DLT platforms other than the platforms leveraged by Nasdaq in its Ubin Phase III solution.

Transaction privacy in the Nasdaq solution was achieved through a combination of multi-level encryption mechanisms, one-time addresses and channels.

Nasdaq's Ubin Phase III solution provided capabilities for:

- A *smart contract engine* that enabled the creation and execution of DLT-agnostic smart contracts;
- A modular, containerized, elastic and configurable infrastructure that could be securely deployed on a variety of cloud platforms;

- *Role-based APIs* for the DvP settlement process. Role-based APIs enabled Ubin Phase III system participants to initiate and execute multiple interledger transactions using a single API interface.

Project Stella

The Bank of Japan and the ECB initiated Project Stella in December 2016 to assess the applicability of DLT to FMIs in both jurisdictions [118].

The ECB is responsible for the administration of monetary policy within the Eurozone [166]. TARGET2, the high-value interbank settlement system in the euro area is used to perform monetary policy operations in the Eurozone [167]. The Eurosystem, which comprises of the ECB and National central banks of all EU member States, is the owner and operator of TARGET2 [166].

The Bank of Japan, Japan's central bank is responsible for administering monetary policy in Japan. It is the owner and operator of the BOJ-NET, Japan's wholesale LVTS [119].

Project Stella has been implemented in three phases using multiple DLT platforms.

Project Stella Phase I [119] implemented a W-CBDC and core RTGS functionalities on the Fabric DLT platform.

Project Stella Phase II [120] implemented DvP functionalities for the settlement of tokenized securities on Corda, Elements and Fabric.

Project Stella Phase III [121] focused on the potential of improving the efficiency of cross-border transactions using DLT. Stella Phase III was implemented on Fabric.

In all three phases of Project Stella, fictitious virtual CMBs were created to test the developed prototypes.

Additionally, IBM, DG Labs and R3 provided technical advice for Stella Phase II.

Stella Phase I

Project Stella Phase I began in December 2016 through the partnership of the Bank of Japan and the ECB.

Project Stella Phase I evaluated the potential of DLT to deliver specific RTGS functions for domestic wholesale interbank payments settlement in the Eurozone and Japan.

In Stella Phase I, two separate DLT-based RTGS prototypes with LSM settlement capabilities were developed on Fabric v0.6.1 [119]. One prototype satisfied core RTGS functional requirements of TARGET2 as defined by the ECB while the other satisfied key requirements of BOJ-NET as defined by the Bank of Japan.

The Stella Phase I ECB prototype was developed to meet TARGET2's daily transaction volume requirement of 343,729 payments per day (PPD) while the Bank of Japan prototype was developed to

meet BOJ-NET's daily transaction volume requirement of 67,326 PPD. On the average, the ECB and the Bank of Japan process between 10 and 70 transaction requests per second (RPS) daily.

Transaction consensus in Stella Phase I was achieved using the PBFT consensus mechanism.

To test the performance of the Stella Phase I prototypes, the Bank of Japan and the ECB created simulated data which were used as experiment inputs.

Participant nodes for the ECB DL network were deployed on VMs in an in-house network infrastructure hosted at the ECB while Bank of Japan participant nodes were deployed on a commercial cloud platform.

Performance tests for the Stella Phase I prototypes were conducted in parallel by the ECB and the Bank of Japan with the following evaluation results:

- *LSM Settlement*: Generally, LSM functionalities performed as required.
- *Latency*: Transaction latency increased as the number of nodes on the network increased.
- *Throughput*: Both prototypes met the ECB and the Bank of Japan's daily RTGS PPD requirements; however, increasing transaction volumes to 250 RPS led to an overall decrease in system performance.
- *Distance*: Network performance was enhanced the closer the nodes required to achieve transaction consensus were to each other. However, an increase in distance between *consensus nodes* resulted in a decreased system performance.

The ECB and the Bank of Japan further tested the reliability and resiliency of the Stella Phase I prototypes using three base scenarios.

- *Scenario I*: Temporary failure of an authoritative node used to authenticate and approve transaction requests.
- *Scenario II*: Temporary failure of one or more validating nodes.
- *Scenario III*: Sending incorrect data formats.

In *Scenario I*, a single-point of failure problem was encountered when the authoritative node responsible for transaction authentication and approval was temporarily unavailable.

In *Scenario II*, it was observed that system availability and performance were not impacted as long as the number of validating nodes required for achieving consensus were operational.

In Scenario III, the system was able to accurately detect and eliminate transactions with incorrect data formats, therefore system performance was not impacted.

Stella Phase II

The Bank of Japan and the ECB launched Project Stella Phase II in November 2017 to examine the potential of using DLT for interledger DvP settlement of tokenized financial assets [120].

Stella Phase II defined three DLT-based DvP settlement approaches. They were; *single-ledger DvP settlement*, *cross-ledger DvP settlement with connection between ledgers* and *cross-ledger DvP settlement without connection between ledgers* [120].

The three DLT-based DvP settlement approaches are presented in Figure 7.9.

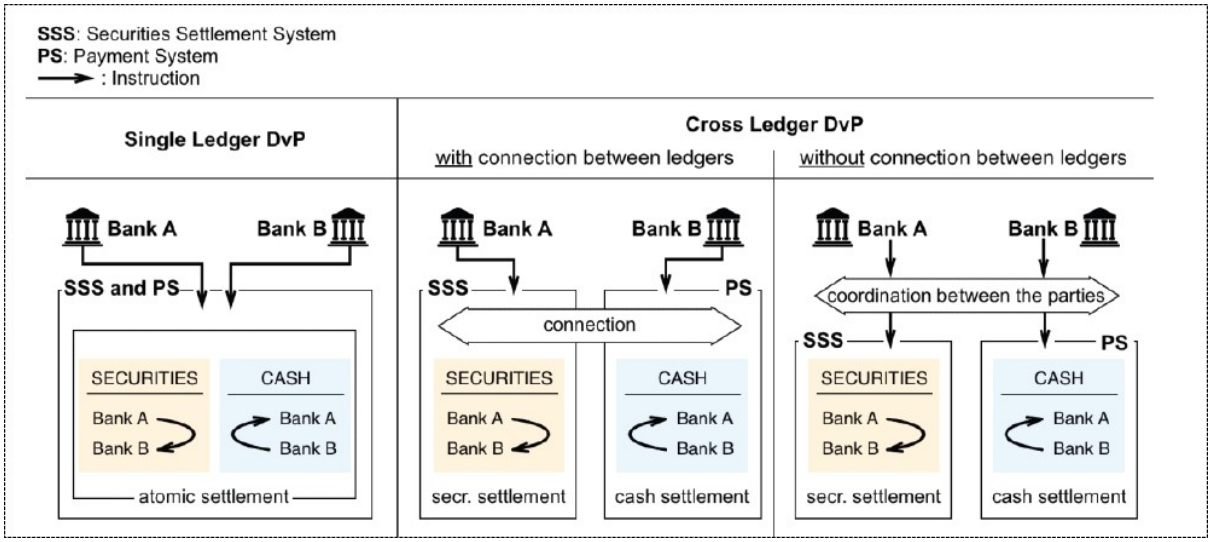


Figure 7.9: Project Stella Phase II DLT-based DvP Settlement Approaches [120]

Stella Phase II implemented DvP settlement prototypes for two of the approaches: the *cross-ledger DvP settlement without connection between ledgers* and the *single-ledger DvP settlement* on Fabric, Elements and Corda.

To achieve interledger asset transfer without a direct interaction between the underlying ledgers, Stella Phase II leveraged cross-chain atomic swaps [168] using HTLC [169].

In this paper, we refer to the cross-ledger DvP settlement prototype without connection between ledgers as *HTLC-based cross-ledger DvP settlement* prototype.

The atomic swap protocol enables the transfer of assets between multiple ledgers without the need for a trusted third-party [168].

In HTLC-based cross-ledger DvP settlement, HTLC uses hashlocks to conditionally block the transfer of assets and timelocks to deliver the assets when settlement conditions are satisfied. Analogically, timelocks recovers the assets back to the sender if settlement conditions are not satisfied.

HTLC works as follows: firstly, counterparties to a transaction must each generate a secret S. Secondly, counterparties generate a hash digest for their respective secrets, S, that is $H(S)$. Counterparties

then send *H(S)* and *S* to each other off-chain in accordance with pre-determined securities settlement conditions.

The ECB and Bank of Japan established two base scenarios to test both the single-ledger and the HTLC-based cross-ledger DvP settlement prototypes. The base scenarios examined the viability of DLT for DvP settlement of securities between two counterparties, *Bank A* and *Bank B*. In the base scenarios, *Bank A* was the seller of securities and *Bank B* was the buyer of securities. The base scenarios were as follows:

- *Scenario I*: Successful settlement.
- *Scenario II*: Failed settlement due to one counterparty not satisfying settlement conditions.

We highlight the experimental results of the HTLC-based cross-ledger DvP settlement prototype. All tests were conducted in a non-production environment.

- *Scenario I*: Tokenized financial assets could be transferred between ledgers using HTLC. Using, cross-chain atomic swaps with HTLC, settlement finality could be achieved if all asset transfer conditions were satisfied.
- *Scenario II*: The experiment identified a major limitation with HTLC. DvP settlement requires time asymmetry for the settlement of one leg (obligation) of the transaction, usually the cash leg before the securities leg. During the simulation of *Scenario II*, *Bank B* did not submit its transfer instructions within the specified *timelock* leading to *Bank A* retaining its securities asset and still receiving cash payment for the securities from *Bank B*. This HTLC design flaw exposed *Bank B* to principal risk.

We present a summary of the DvP settlement prototypes developed on Elements, Corda and Fabric in the next subsection.

a. Elements

Stella Phase II implemented one single-ledger DvP settlement prototype on Elements as well as one Element-Element HTLC-based cross-ledger prototype.

Additionally, one Element-Fabric HTLC-based cross-ledger prototype was implemented.

b. Corda

Stella Phase II implemented one Corda-based single-ledger DvP settlement prototype. A Corda-Corda HTLC-based cross-ledger prototype was also implemented.

No HTLC-based implementations were made between Corda and other DLT platforms.

c. Fabric

Lastly, Stella Phase II implemented one single-ledger DvP settlement prototype on Fabric as well as a Fabric-Fabric HTLC-based cross-ledger prototype.

Stella Phase III

The value of cross-border payments and settlements is expected to reach USD 30 trillion by the year 2022 [140]. However, existing cross-border payments settlement arrangements are complex, expensive and inefficient, thereby affecting the safety and security of such payments [121].

Figure 7.10 depicts a simplified cross-border payments settlement credit risk scenario that arises upon intermediary *Entity B* failing (e.g. going bankrupt) after receiving 1 million from *Entity A* meant for onward transmission to *Entity C* in Japanese Yen. *Entity B* goes bankrupt before it could fulfil the transfer obligation to *Entity C*, thereby exposing *Entity A* to principal risk.

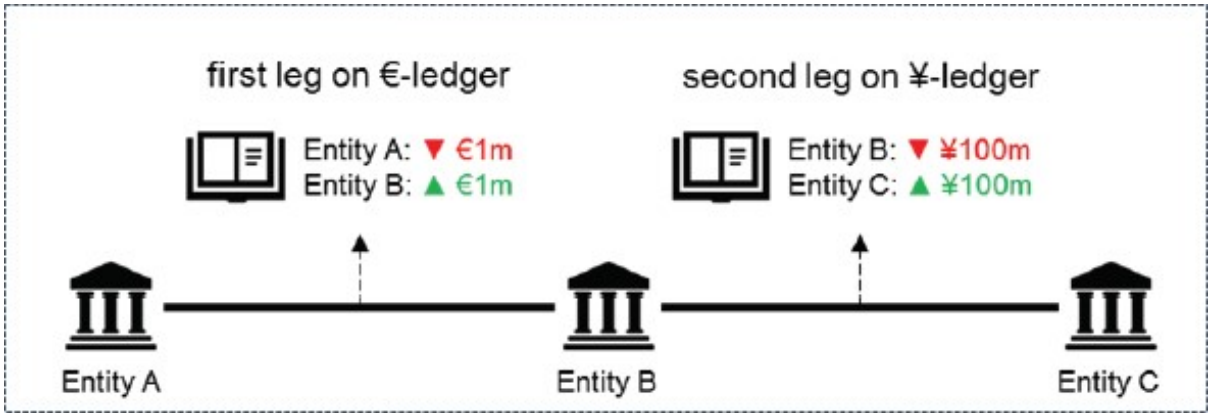


Figure 7.10: Project Stella Phase III Cross-Border Payments Settlement Credit Risk Scenario [121]

The report on Project Stella Phase III [121] published in June 2019 by the ECB and the Bank of Japan examined the feasibility of synchronously improving cross-border payments settlement security and efficiency with and without DLT as well as with and without the use of the interledger protocol (ILP) [122].

In Stella Phase III, prototypes were developed to examine the following base scenarios:

- *Scenario I*: Non-DLT-based centralized interledger cross-border settlement with ILP.
- *Scenario II*: DLT-based ledger vs. non-DLT-based centralized ledger cross-border settlement with ILP.
- *Scenario III*: DLT-based interledger cross-border settlement with ILP.
- *Scenario IV*: DLT-based interledger cross-border settlement without ILP.

The DLT-based ledger prototype was developed on Hyperledger Fabric v.1.2.1.

The non-DLT-based centralized ledger used in Stella Phase III was the *Five Bells Ledger* [171].

In Scenarios I-III, *Interledger.js* [170], the open-source JavaScript implementation of ILP was leveraged.

To eliminate the credit risk scenario presented in Figure 7.10, an on-ledger escrow-lock mechanism with HTLC was implemented on the prototypes. The on-ledger escrow-lock mechanism provided capabilities to conditionally lock funds transferred by counterparty *Entity A* in an escrow until counterparty *Entity C* satisfied the terms and conditions of the contract for which funds were being transferred.

We present the experimental results of the cross-border settlement scenarios involving the DLT-based prototype, that is Scenarios II-IV in the subsequent subsection.

Entity B, which held accounts on both the Euro and Yen ledgers acted as an intermediary in all the given scenarios.

- *Scenario II*: Funds transfer from counterparty *Entity A* which held an account on the Fabric-based ledger to counterparty *Entity C* which held an account on the Five Bells Ledger was successful, demonstrating the viability of ILP.

- *Scenario III*: Synchronized cross-border payments settlement between two Fabric-based ledgers with ILP was successful.

- *Scenario IV*: DLT-based interledger payments settlement without ILP was achieved. Using the Euro ledger and Yen ledger analogy in Figure 7.10, funds on the Euro ledger were locked between *Entity A* and *Entity B* using the on-ledger escrow with HTLC service. The same mechanism was used to lock funds on the Yen ledger between *Entity B* and *Entity C*. Funds on the Euro ledger and funds on the Yen ledger were synchronized and released to *Entity B* and to *Entity C* respectively once all settlement conditions were met.

Stella Phase III confirmed that ILP is ledger-agnostic as the protocol was successfully leveraged on both DLT and non-DLT-based ledgers.

Project Khokha

Project Khokha [130], South Africa's W-CBDC experiment was launched in January 2018 by the SARB, seven South African CMBs, PricewaterhouseCoopers and ConsenSys to explore the use of DLT for domestic wholesale interbank payments settlement in South Africa.

The Khokha participant ecosystem is presented in Figure 7.11.

The goal of Project Khokha was to build a DLT-based RTGS prototype for interbank payments settlement using a tokenized South African Rand asset. The prototype was built on the Quorum DLT

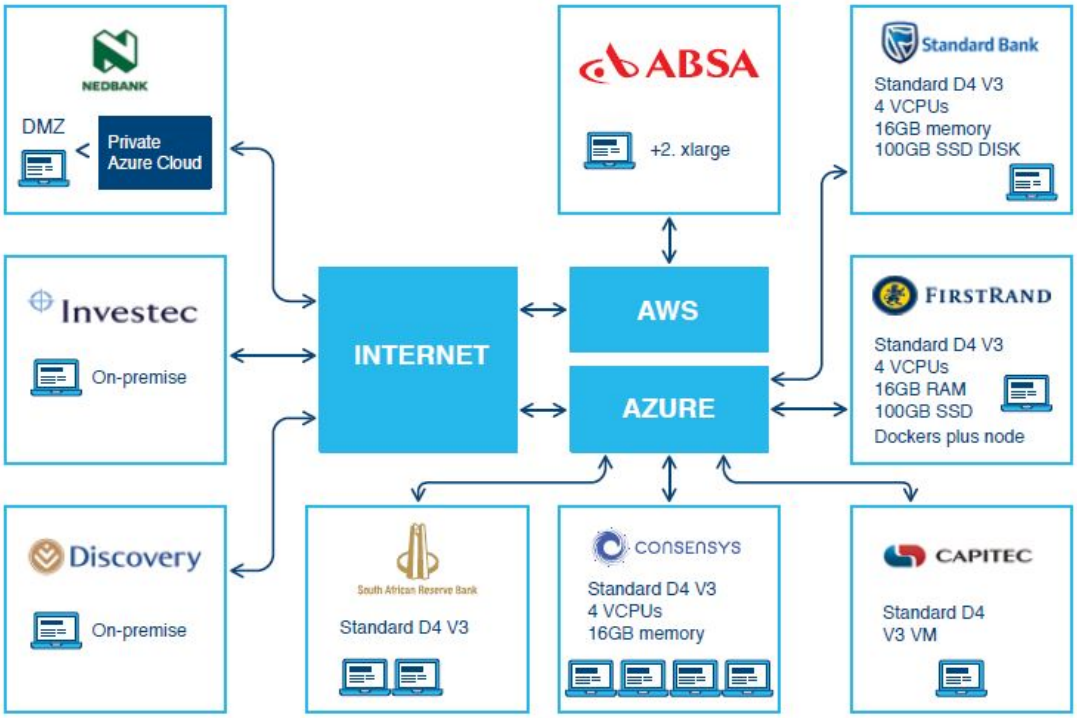


Figure 7.11: Project Khokha Participant Ecosystem [130]

platform.

The RTGS system in South Africa is called the South African Multiple Option Settlement system (SAMOS). SAMOS, which is owned and managed by the SARB is used to process high-value interbank payments, interbank retail payment obligations and securities settlement in South Africa.

SAMOS processes 70,000 wholesale interbank payments intraday on RTGS basis with capabilities to process a whole day's transaction within two hours in the event that the system is unable to operate in the course of the day due to system outage [130].

In order to compare the functionality and performance of the DLT-based RTGS prototype to the existing SAMOS FMI, the following performance metrics were defined for the Khokha prototype.

- Except the SARB, counterparty transaction data in the DL network should be fully confidential to all system participants.
- The system should adhere to the settlement finality (*Principle 8*), money settlement (*Principle 9*) and operational risk (*Principle 17*) requirements of the PFMIs.
- The system should settle up to 70,000 wholesale interbank payments intraday.
- The system should scale and settle up to 200,000 wholesale interbank payments intraday.
- In emergency situations, the system should settle up to 70,000 interbank payments within two hours.

- At least 95% of blocks containing transactions should be propagated throughout the entire DL network under one second.
- At least 99% of blocks containing transactions should be propagated throughout the entire DL network within two seconds.

In Project Khokha, participating entities deployed Quorum-based distributed nodes using a combination of VMs, on-premise private and public cloud hosting platforms with varying network resources as shown in Figure 7.11. The SARB was responsible for issuing tokenized Rand assets and creating wallets for each participating CMB to hold tokenized Rand assets.

Transaction consensus on the Khokha platform was achieved using the IBFT consensus mechanism. Additionally, Pedersen commitments and range proofs were leveraged to guarantee transaction privacy, settlement finality, scalability and system resiliency in Khokha [130].

Capabilities to pledge, transfer, redeem and track tokenized Rand balances were built into the Khokha platform.

At all times, the SARB node had full visibility of transactions on the Khokha platform.

Khokha was implemented over four iterations as follows:

- *Iteration 1*: Capabilities for the issuance of tokenized Rand assets and the creation of on-ledger wallets by the SARB were implemented. Capabilities for CMBs to pledge, transfer and redeem tokenized Rand assets for central bank money were also implemented in this iteration.
- *Iteration 2*: Capabilities for transaction approval by the SARB without guarantees for data privacy were implemented.
- *Iteration 3*: Mechanisms for the exchange of keypairs among counterparties as well as capabilities for data privacy and settlement finality using Pedersen commitments were implemented.
- *Iteration 4*: Mechanisms to achieve system resiliency were implemented through a combination of Pedersen commitments and range proofs. Capabilities for counterparties to verify and validate transactions were also implemented in this iteration.

Following the development of the Khokha platform, the prototype was tested in a non-production environment against the defined performance metrics with the following results. The platform:

- Settled a minimum of 70,000 transactions intraday.
- Achieved the scalability requirement of up to 200,000 transactions intraday.
- Settled 70,000 transactions in two hours in line with the emergency performance metric.

- Achieved 95% block propagation throughout the entire DL network in one second and up to 99% block propagation throughout the entire network within two seconds.
- Adequately provided for counterparty data privacy requirements.
- Adhered to the defined settlement finality, money settlement and operational risk requirements of the PFMIs.

Project Inthanon

The Bank of Thailand together with R3 and eight Thai CMBs initiated Project Inthanon [138] in August 2018 to examine the potential of DLT for Thailand's FMIs. Project Inthanon has been implemented over two phases.

Project Inthanon Phase I [138] implemented a DLT-based distributed RTGS prototype for domestic wholesale interbank payments settlement in Thailand.

Project Inthanon Phase II [172] focused on the implementation of a securities settlement platform for the issuance, management and settlement of Bank of Thailand-issued tokenized bond and tokenized cash assets.

Inthanon Phase I

Project Inthanon Phase I [138] commenced in August 2018 through the collaboration of the Bank of Thailand, eight Thai CMBs and R3.

Project Inthanon Phase I [138] implemented on Corda, a distributed RTGS prototype with LSM settlement options for domestic wholesale interbank payments settlement in Thailand. Inthanon Phase I was implemented on Corda v3.2.

We present the design architecture of Inthanon Phase I in Figure 7.12.

Key deliverables in Inthanon Phase I included the development of a Corda-based distributed RTGS prototype with LSM settlement capabilties and the issuance of tokenized Bank of Thailand-issued bond and cash assets.

Similar to previously examined CBDC experiments, capabilities for pledging central bank money for Bank of Thailand-issued tokenized securities were implemented in Inthanon Phase I. Analogically, mechanisms for the transfer and redemption of tokenized assets (e.g. Chapter 7.2) for central bank money were implemented in the Inthanon Phase I prototype.

Three types of nodes were deployed in Inthanon Phase I, namely *supervisory node*, *notary service node* and *participant nodes*.

Similar to previous Corda implementations examined in this paper, the supervisory node and notary node functions were performed by the Bank of Thailand whiles CMBs were assigned participant nodes.

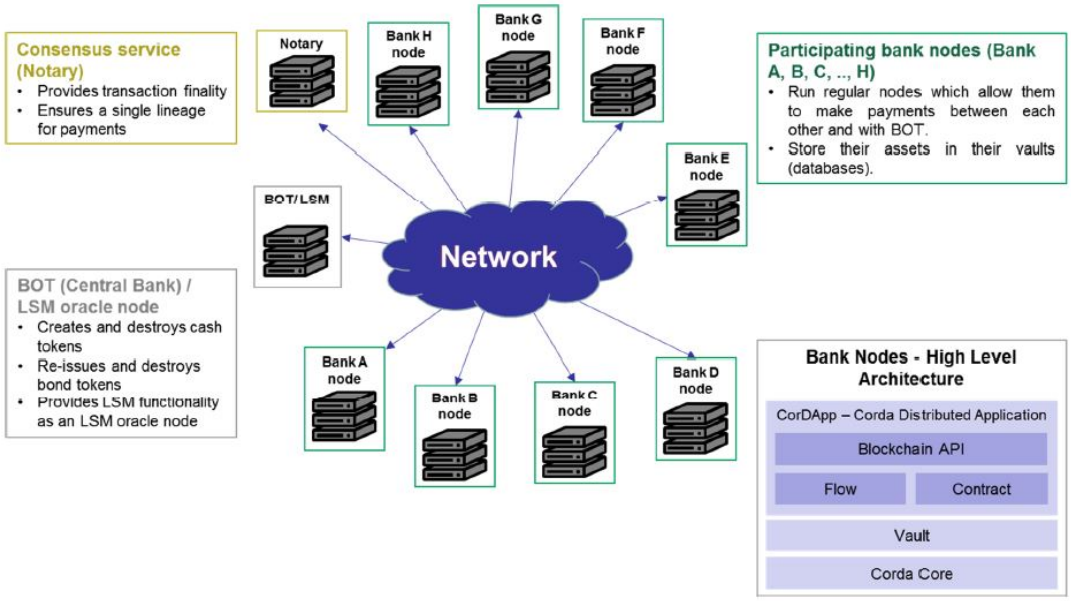


Figure 7.12: Project Inthanon Phase I Design Architecture [138]

All nodes in Inthanon Phase I were deployed on separate Microsoft Azure cloud-hosting platforms.

Tokenization of Bank of Thailand-issued cash assets in Inthanon Phase I follows a similar pattern as in Figure 7.2.

The consensus mechanism used in Inthanon Phase I follows previous Corda-based CBDC prototypes examined in this paper, such as in Chapter 7.2.

A key difference between Inthanon Phase I and the other CBDC experiments with LSM capabilties (e.g. Chapter 7.2, Chapter 7.2 and Chapter 7.2) examined in this paper is that, the Inthanon Phase I prototype enabled banks with liquidity shortages to pledge tokenized bond assets to the Bank of Thailand in exchange for tokenized Baht assets. The experiments referenced did not provide for pledging of bond assets as collateral.

The Inthanon Phase I prototype was tested in a non-production environment with the following evaluation results:

- *Settlement Success*: Inthanon Phase I participants were able to exchange value among each other with guaranteed data privacy and settlement finality.
- *Enhanced LSM Capability*: The Inthanon Phase I platform implemented an enhanced LSM settlement option that enabled participating CMBs to pledge tokenized bond assets to the Bank of Thailand as collateral in exchange for tokenized cash assets.

Inthanon Phase II

Project Inthanon Phase II [172] was launched in February 2019 through the partnership of the Bank of Thailand, R3 and eight Thai CMBs.

Project Inthanon Phase II [172] implemented on Corda, a securities settlement platform for the issuance, management and settlement of Bank of Thailand-issued tokenized bond assets and tokenized cash assets. Project Inthanon Phase II was implemented on Corda v4.0.

The securities settlement infrastructure implemented in Inthanon Phase II was an integrated single-ledger DvP settlement platform similar to the single-ledger DvP model presented in Figure 7.9.

Similar to Inthanon Phase I, three types of nodes were deployed in Inthanon Phase II, namely participant nodes, supervisory node and notary node. Participating CMBs were each assigned participant nodes. The Bank of Thailand was responsible for the supervisory and notary node functions.

Tokenized cash and bond assets in Inthanon Phase II were represented on-ledger using Corda's UTXO state model.

The consensus mechanism used in Inthanon Phase II was similar to the mechanism used in Inthanon Phase I.

Key capabilities implemented in Inthanon Phase II included capabilities for:

- DvP settlement of Bank of Thailand-issued tokenized bond and cash assets;
- Tokenized Bank of Thailand-issued bond and cash assets;
- Bond issuance and full lifecycle management;
- Multi-asset LSM settlement options; and
- Third-party funds transfer fraud prevention.

Following the development of the Inthanon Phase II prototype, the platform was tested in a non-production environment.

An evaluation of the Inthanon Phase II prototype demonstrated that:

- DLT-based DvP settlement of securities for cash was feasible in Thailand.
- Inthanon Phase II enabled the on-ledger exchange of multiple tokenized assets in real-time.
- Multi-asset LSM capabilties implemented on Inthanon Phase II enabled the efficient use of liquidity across the Inthanon Phase II securities settlement infrastructure.

Project Jasper - Ubin

The report on Project Jasper-Ubin [143], a cross-border CBDC experiment between the Bank of Canada, MAS, Accenture and JP Morgan was published in November 2019.

The goal of Project Jasper-Ubin was to examine the feasibility of a cross-border interledger payments settlement denominated in different currencies using DLT.

Intermediaries Approach	Direct widened access	Direct multiple-currencies
• also known as asset swap via intermediary • needs intermediary for foreign exchange and transfer	• also known as direct access • does not involve an intermediary	• also known as asset transfer • allows for multiple currencies within the same network • still need intermediary (which could be the central banks) for transfer

Figure 7.13: Cross-Border Payments Settlement Approaches and Characteristics [143]

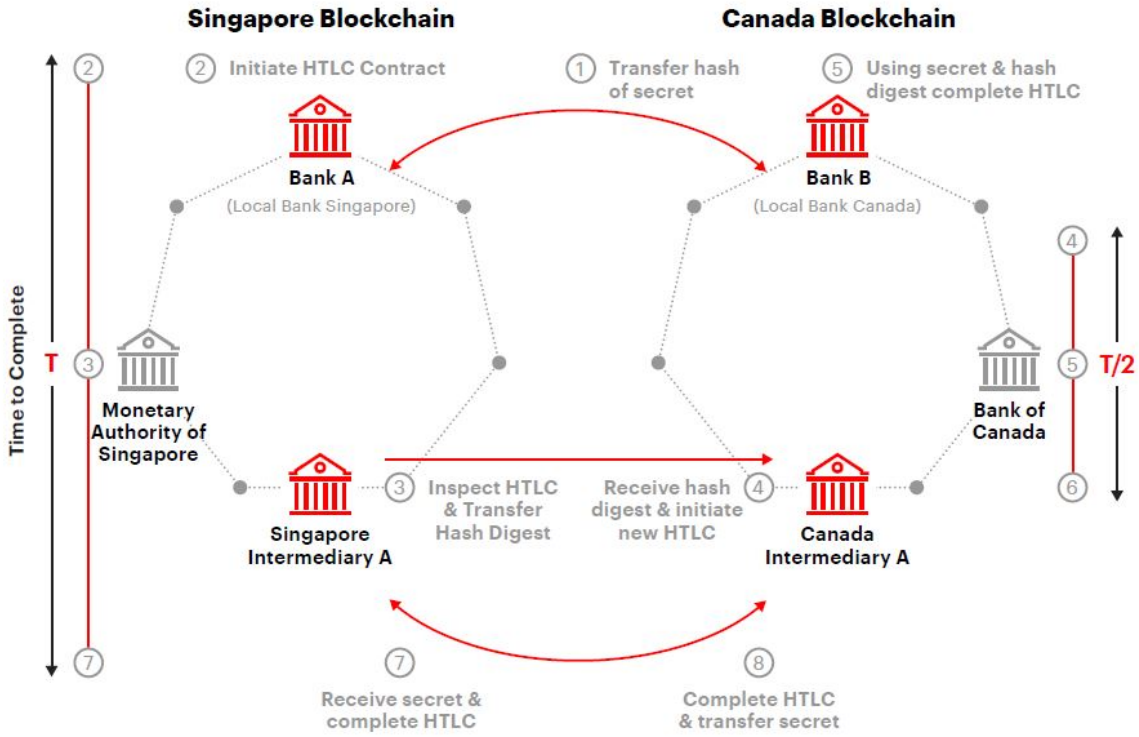


Figure 7.14: Project Jasper-Ubin Cross-Border Interledger Value Exchange Transaction Flow [143]

The Jasper-Ubin prototypes were developed on Corda and Quorum for the Bank of Canada and the MAS respectively.

The Jasper-Ubin prototypes were a DLT-based implementation of cross-border payments approaches proposed by the Bank of Canada, the Bank of England and the MAS in their joint CBDC research report

on cross-border payments settlement [140].

In the Jasper-Ubin report [143], three cross-border settlement approaches were discussed, the *intermediary approach*, the *widened access approach* and the *multicurrency approach*.

In Project Jasper-Ubin, a prototype for only one approach, the *intermediary approach* was implemented. Figure 7.13 describes the characteristics of the three cross-border payments approaches discussed in the Jasper-Ubin report.

Similar to Project Stella Phase II, cross-chain atomic swaps with HTLC was used for the cross-border interledger exchange of value between the Jasper-Ubin prototypes.

The experimental setup for the Jasper-Ubin PoC consisted of one intermediary bank (*Intermediary A*) with accounts in both Canada and Singapore, one local bank (*Bank A*) in Singapore and one local bank (*Bank B*) in Canada respectively. *Intermediary A* and *Bank B* were assigned one node each in Canada while the same *Intermediary A* and *Bank A* were assigned two nodes each in Singapore.

We present the transaction flow of the cross-border interledger value exchange between the Jasper-Ubin prototypes in Figure 7.14.

Following the development of the Jasper-Ubin Quorum and Corda prototypes for Singapore and Canada respectively, a cross-border interledger high-value transfer denominated in SGD was executed from *Bank A* in Singapore to *Bank B* in Canada with the following results:

- *HTLC Transfer*: HTLC enabled a successful atomic transfer of SGD$ 105 from *Bank A* through *Intermediary A* to *Bank B*. *Bank B*'s account was credited with CAD$ 100 by *Intermediary A* in accordance with pre-agreed exchange rates between the transaction parties.

- *HTLC Limitation*: The HTLC protocol requires the exchange of hash digests and secrets off-chain. *Intermediary A* in Canada may incur a principal risk in the event that it loses the original secret it received from *Bank B* after crediting *Bank B*'s account.

We present a summary of the goals, stakeholders, use cases and DLT platforms used to implement each of the CBDC experiments discussed in this research in Table 7.2 and Table 7.3.

Table 7.2: CBDC Experiment Practices Summary-A

Experiment Name/ Jurisdiction	**Phase/Year**	**Goals**	**Stakeholders**	**Use Case**	**DLT used**
Project Jasper (Canada)	Phase I (Mar - June 2016)	Build a DLT-based PoC prototype for domestic wholesale interbank payments settlement in Canada.	Payments Canada, Bank of Canada, R3, CIBC, TD Bank, Scotiabank, BMO and RBC.	UC2, UC3	E
	Phase II (Dec 2016 - Apr 2017)	Rebuild the Phase I PoC on an alternative DLT platform with extended RTGS functionalities.	Payments Canada, Bank of Canada, R3, CIBC, TD Bank, Scotiabank, BMO, RBC, NBC and HSBC	UC2, UC3	C
	Phase III (Oct 2017 - May 2018)	Implement a DLT-based PoC prototype for an integrated SSS that allows for the exchange of multiple asset types on a shared transaction ledger.	Payments Canada, Bank of Canada, TMX Group, Accenture and R3.	UC2, UC6	C
BLOCKBASTER (Germany)	Phase I (Mar - Nov 2016)	Evaluate the potential of blockchains for interbank securitiessettlement for DvP.	Deutsche Bundesbank, Deutsche Börse Group and Digital Asset.	UC2, UC6, UC7	F, D
Project SALT (Brazil)	Phase I (Sept - Nov 2016)	Explore CB use cases that could benefit from the potential of DLT and implement a prototype for one of the identified use cases.	Central Bank of Brazil and selected CMBs.	UC2, UC3	B
	Phase II (Jan - Feb 2017)	Evaluate competing DLT platforms for their suitability for wholesale interbank payments.		UC2, UC3	F, Q
Project Ubin (Singapore)	Phase I (Nov - Dec 2016)	Explore the use and potential benefits of DLT for key RTGS functionalities.	MAS, Deloitte, Bank of America Merrill Lynch, Credit Suisse, DBS Bank Ltd, Hongkong and Shanghai Banking Corporation Ltd, J.P. Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, SGX, UOB, BCS Information Systems and R3.	UC2, UC3	E
	Phase II (July - Nov 2017)	Rebuild the Phase I PoC on multiple DLT platforms with extended RTGS functionalities.	MAS, ABS, Bank of America Merrill Lynch, Citi, Credit Suisse, DBS Bank Ltd, HSBC Limited, J.P. Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, SGX, Standard Chartered Bank, UOB, Accenture, R3, IBM, ConsenSys and Microsoft	UC2, UC3	C, F, Q
	Phase III (Aug - Nov 2018)	Evaluate the use of DLT for the development of an interbank SSS for the settlement of tokenized assets.	MAS, ABS, SGX, Anquan Capital, Deloitte and Nasdaq.	UC2, UC6	E, F, H, N, Q
Note: B-BlockApps, C-Corda, D- Digital Asset, E-Ethereum, F-Fabric, H-Chain, L-Elements, N-Anquan and Q-Quorum.					

Table 7.3: CBDC Experiment Practices Summary-B

Experiment Name/ Jurisdiction	**Phase/Year**	**Goals**	**Stakeholders**	**Use Case**	**DLT used**
Project Stella (EU & Japan)	Phase I (Dec 2016 - Sept 2017)	Implement a DLT-based RTGS prototype with LSM capabilites.	ECB, Bank of Japan and virtual CMBs	UC2, UC3	F
	Phase II (Nov 2017 - Mar 2018)	Implement DvP functions on multiple DLT platforms for interbank settlement of securities for cash.	ECB, BOJ, R3, IBM and DG Lab.	UC2, UC6	C, F, L
	Phase III (June 2019)	Explore the potential to improve the safety of crossborder transactions using DLT.		UC2, UC9	F
Project Khokha (South Africa)	Phase I (Jan - June 2018)	Explore the use of DLT for wholesale interbank payments settlement in South Africa.	SARB, Absa, Capitec, Discovery Bank, FirstRand, Investec, Nedbank, Standard Bank, ConsenSys and Pricewaterhouse Coopers Inc.	UC2, UC3	Q
Project Inthanon (Thailand)	Phase I (Aug 2018 - Jan 2019)	Implement a decentralized RTGS prototype with LSM functionalities on DLT for wholesale interbank payments settlement.	Bank of Thailand, Bangkok Bank, Krung Thai Bank, Bank of Ayudhya, Kasikornbank, Siam Commercial Bank, Thanachart Bank, Standard Chartered Bank, Hongkong and Shanghai Banking Corporation Limited and R3.	UC2, UC3	C
	Phase II (Feb - June 2019)	Implement a DLT-based DvP system for interbank bond trading and bond lifecycle management.	Bank of Thailand, Bangkok Bank, Krung Thai Bank, Bank of Ayudhya, Kasikornbank, Siam Commercial Bank, Thanachart Bank, Standard Chartered Bank, Hongkong and Shanghai Banking Corporation Limited and R3.	UC2, UC7	C
Project Jasper-Ubin (Canada & Singapore)	Phase I (Nov 2019)	Enable cross-border high value transfer between different DLT platforms that settle in different currencies.	Bank of Canada, MAS, Accenture and J.P. Morgan.	UC2, UC9	C, Q
Note: B - BlockApps, C - Corda, D - Digital Asset, E - Ethereum, F - Fabric, H - Chain, L - Elements, N - Anquan and Q - Quorum.					