
fime
GREYC

Offline payment requirements for Central Bank Digital Currencies

Atangana Olivier

09/10/2022

Introduction

FIME (`https://www.fime.com/`), a world leader in electronic payment, offers a comprehensive suite of services in the field of testing and certification of transactions and payment methods. This suite specifically includes consulting, support, technical training, assistance in product design, and test tools, in addition to laboratory certification services. Furthermore, FIME operates in the telecommunications, transportation, and digital identity sectors, and invests in emerging areas such as M2M, IoT, and biometrics. Thus, leveraging over 20 years of experience and expertise, the group offers a myriad of services, allowing its clients to effectively and confidently meet their market's expectations with secure embedded solutions. This particularly includes smart cards, mobile, Cloud Computing, or any other medium by incorporating recent technologies and payment methods, such as Central Bank Digital Currencies (CBDCs).

Chapitre 1

Context and Motivation

Central Bank Digital Currencies are evolving in correlation with the technological transition movement inherent in the global economy, marked by a preferential option for digital transactions. Following the emergence of the coronavirus pandemic, numerous countries and organizations have accelerated their digital transformation to align with electronic payment systems. In China, nearly 80

1.1 GREYC Laboratory

The GREYC laboratory (`http://www.greyc.fr/`), a long-term partner of FIME, is a research unit (UMR 6072) in digital sciences, composed of distinct but complementary teams. The Architecture and Security Models team specializes in computer systems security. For several years, it has worked in the field of network security (IoT, SDN, 5G), applied and random cryptography, and information protection. The laboratory has notably developed numerous software solutions and mobile applications for transaction security.

1.2 Supervision

— Prof. Lyes Khoukhi (`mailto:lyes.khoukhi@ensicaen.fr`)
— Dr. Morgan Barbier (`mailto:morgan.barbier@unicaen.fr`)
— Willy Royer (`mailto:willy.royer@fime.com`)

Chapitre 2

Projet Description

According to the electronic money directive of the Monetary and Financial Code, electronic money is "a monetary value stored in electronic form, including magnetic, representing a claim on the issuer, issued against the delivery of funds for the purpose of payment operations [...] and accepted by a natural or legal person other than the electronic money issuer" [3]. It can maintain a link with traditional currencies (Dollar, Yuan, Euro), provided that the funds are also expressed in the same unit of account and that the currency is also accepted by other actors besides the issuer. Thus, from this perspective, the digital currency issued by central banks is a digitization of fiat money. Clearly, the widespread emergence of cryptocurrencies, with historical turning points such as Szabo's design of "Bit Gold" in 1998 and the advent of bitcoin 10 years later as a peer-to-peer digital currency, has accelerated the research and development of CBDCs [4]. Indeed, CBDCs are a credible alternative to the volatility of cryptocurrencies and a complementary option for electronic payment in an economic context undergoing full digital transition.

A plethora of serious work has been carried out to define the characteristics, issuance terms, reception, and recording of CBDCs, as well as their deployment infrastructure. It goes without saying that the main motivations inherent to the adoption of this digital currency are the reduction of issuance costs, security, robustness, and efficiency of payments, transparency, improvement, and facilitation of transactions [5]. However, while the use of CBDCs offers great promises, its implementation faces a multitude of challenges on technical, technological, legislative, and social levels that intertwine with each other. Among others, interoperability with existing payment systems, cross-

border payment, security guarantee of digital wallets, traceability, the definition of a legislative code... Although some countries are already deploying their digital currency, not without difficulty and hesitation, most, like the European community, are still in the pilot phase.

In this thesis, the goal is to ensure an optimal level of security for CBDC payment transaction flows, even in offline mode. The research methodology will reside in the dynamics of these three action verbs : understand, analyze, implement. In other words, it involves immersing oneself in the latest research advances on CBDC projects through literary studies and participation in conferences on the subject, followed by technological monitoring. Then, it is necessary to examine the relevance and shortcomings of current CBDC technologies. Finally, it will involve implementing a viable payment solution for the CBDC ecosystem. Subsequently, through this research, FIME aims to define the technical characteristics of an electronic currency based on a secure and resilient infrastructure. In other words, to define an operational system capable of ensuring offline payment when the central infrastructure is unavailable or when network quality is degraded, while guaranteeing the transaction's security, its traceability, and the authenticity of the issuer [6].

Chapitre 3

Research Axes

This thesis proposes to make a contribution scaffolded on three research axes :

3.1 Features of the Digital Wallet

Definition of the characteristics of the electronic wallet, the matrix of electronic money, in all its aspects and with its security constraints. This presupposes, at the base, first ensuring the security services of a traditional computer system. In particular, integrity, non-repudiation, access control, confidentiality, availability, identity, and authentication [7]. This last service will be particularly important insofar as it will be necessary to ensure the identity of the buyer or prove that of the payment issuer. At this level, the experience of the FIME biometrics laboratory in collaboration with the Monetics and Biometrics team of the GREYC laboratory specialized in the evaluation of behavioral biometrics will be of great contribution. Indeed, biometric authentication tied to payment is increasingly popular in the market and even required by new regulations on electronic payment. In addition, it will be appropriate to integrate a functionality to protect against double-spending and a hardware and/or software privacy protection module. This is one of the reasons why research on CBDCs in connection with distributed ledger technologies (originally DLT for Distributed Ledger Technology), which are very respectful of privacy, is developing significantly [8].

3.2 Communication Protocol

Establishment of the communication protocol between two electronic wallets. Knowledge in cryptography will inevitably be necessary because whatever the envisaged protocol, it must ensure the authenticity of the transaction (obviously without burdening the execution of the transaction itself) by means of encryption. Encryption tools such as asymmetric encryption, elliptic curve cryptography, cryptographic signature are very interesting leads in this respect. Also, the development of quantum computing units also implies foreseeing, if not implementing, the possible integration of a post-quantum algorithm. Moreover, for the transmission of payment data (account-based or token-based) itself, a study of protocols such as the NFC protocol, the BLE protocol, or the use of QR code with simple or mutual authentication will have to be taken into account. As an illustration, the payment card provider Visa is currently implementing the OPS protocol (offline payment system) which allows point-to-point authorization during offline payments using open-source technology and a public key infrastructure [9].

3.3 Synchronization with the Central Network

Synchronization with the central network. This is, for the occasion, the central bank, the trusted third party, providers of funds, and guarantor of the financial stability of the system [10]. The main challenge will be to make offline and online electronic wallets coexist, to combine their exchanges in such a way that the transfer and recovery of funds are carried out properly, in a simple and transparent manner for the actors. Many CBDC-based architectures take into account the integration of an API to ensure the link between payment actors and central banks.

Chapitre 4

Conclusion

Finally, the research will be completed by the study of the impact of an embedded artificial intelligence solution on fraud prevention. Cyber attackers and cyber fraudsters are competing in skill to compromise cryptocurrency systems [11]. Consequently, as their techniques develop, innovation must provide a significant response. In particular, to deal with fraud techniques such as double-spending, double-incoming, replay (transaction replay)...

To carry out this work, the doctoral student, keen on emerging Fintech technologies and passionate about technological challenges, has good knowledge in cryptocurrencies, network security, cryptography, and AI. His work time, divided between two parts, is put to good use in the FIME laboratory and the GREYC laboratory. He has a range of material, computer, and literary resources to conduct his research, carry out his experiments, and test his solution.

Chapitre 5

Bibliography

[1] Knoerich. "China's new digital currency : implications for renminbi internationalization and the US dollar. In : The (Near) Future of Central Bank Digital Currencies : Risks and Opportunities for the Global Economy and Society" Global Politics and Security (2021) : 145-166.

[2] Ahmet Faruk Aysan, Farrukh Nawaz Kayani. "China's transition to a digital currency : does it threaten dollarization ?" Asia and the Global Economy (2022).

[3] Transposed definition from Article L.315-1 of the Monetary and Financial Code.

[4] Huaqun Guo, Xingjie Yu. "A survey on blockchain technology and its security." Blockchain : Research and applications (2022).

[5] Tao Zhang, Zhigang Huang. "Blockchain and central bank digital currency." ICT Express (2022) : 264-270.

[6] Fabio Panetta. "The digital euro : our money wherever, whenever we need it." Introductory statement (2023).

[7] Guy Pujolle. "Networks in the age of cloud and 5G" (2020).

[8] Paul Wong, Jesse Leigh Maniff. "Comparing Means of Payment : What role for a Central Bank Digital Currency ?" FEDS Notes (2020).

[9] Mihai Christoderescu al. "Towards a Two-Tier Hierarchical Infrastructure : An Offline Payment System for Central Bank Digital Currencies." Visa Research (2020).

[10] Dashkevich et al. "Blockchain Application for Central Banks : A Systematic Mapping Study." IEEE ACCESS (2020).

[11] Guglielmo Maria Caporale et al. "Non-linearities, cyber-attacks, and cryptocurrencies." Finance Research Letters (2020).