Detailed Report on Offline CBDC Technical Considerations

Personal Account by Olivier Atangana

8-9 November 2023, Basel, Switzerland

Author's Note

This report is a personal account of the presentation by Ben Dovey and Gary Munro, as interpreted and compiled by Olivier Atangana. It reflects my understanding and perspective on the topics discussed during the event.

1 Introduction

This detailed report covers the presentation by Ben Dovey, Adviser at BIS Innovation Hub-Nordic Centre, and Gary Munro, CTO at Consult Hyperion,

on "Offline CBDC Technical Considerations". The presentation was part of the conference "Securing the Future Monetary System Cybersecurity for Central Bank Digital Currencies" held in Basel, Switzerland.

2 Context and Significance

2.1 Emergence of CBDCs

The presentation began with an overview of the evolving landscape of digital currencies, emphasizing the emerging trend of Central Bank Digital Currencies (CBDCs).

3 Central Bank Perspectives

3.1 Motivations for Adoption

The driving factors behind central banks' interest in integrating offline functionalities into CBDCs were explored. This included discussions on financial inclusion, security, and operational resilience.

3.2 Importance of Offline Capabilities

The need for offline functionalities in CBDCs was underscored, highlighting its significance in ensuring resilience and accessibility in various transaction scenarios.

4 In-Depth Analysis of Security and Cash-like Issues in Offline CBDCs

4.1 Security in Offline CBDC Environments

The presentation delved deeply into the security challenges inherent in offline CBDC transactions. A significant concern highlighted was the risk of offline devices being compromised or used maliciously. The discussion emphasized the need for robust hardware and software security solutions. This

includes secure storage of keys and values, transmission of secure data, and maintaining device integrity over extended periods.

4.2 Cash-like Properties and Risks

The notion of cash-like use cases in CBDCs was explored, considering the unique characteristics and risks associated with offline CBDCs. The presenters discussed how a purely offline CBDC system might face challenges such as extended security validity and the potential for currency manipulation, like counterfeiting and double-spending activities.

4.3 Risk Management and Mitigation Strategies

The presenters provided insight into the various risk management strategies that could be employed in offline CBDC systems. These include both preventative measures for detecting and reacting to fraudulent activities, and corrective measures for managing the impacts of such activities.

4.4 Physical and Digital Security Measures

The role of physical elements such as secure elements in payment cards and smartphones, and their relevance in an offline CBDC context was discussed. The importance of a Zero Trust architecture in software security for managing offline transactions was also highlighted.

4.5 Implementation Barriers

The presenters identified and discussed various barriers to implementing offline CBDC systems, including technical, regulatory, and infrastructural challenges.

5 Design Considerations

5.1 Architectural Requirements

Details were provided on the required security architecture for offline CBDCs, encompassing both hardware and software components to ensure transaction integrity and prevent fraud.

5.2 User-Centric Design

The importance of a user-centric approach in the design of offline CBDC systems was highlighted. This section emphasized the need for accessibility and ease of use, ensuring inclusivity for all users.

6 Concluding Thoughts

6.1 Future Trends and Innovations

The presentation concluded with a forward-looking perspective, discussing upcoming trends and potential innovations in the offline CBDC space. The importance of adaptability to future technological advancements was emphasized.

6.2 Final Remarks

The presenters summarized their insights and encouraged ongoing research and collaboration in the field.

7 References

A list of references and recommended readings on offline CBDCs was provided for further exploration of the topic.

8 Legal Notices

8.1 Copyright

8.2 Terms of Use

8.3 Disclaimer

The opinions expressed in this report are those of Olivier Atangana and do not necessarily reflect the views of any associated organizations.

8.4 Contact Information

For inquiries or additional permissions, please contact Olivier Atangana at olivier.atangana@fime.com.