# Comprehensive Report on Project Tourbillon Presentation

Analysis by Mike Alonso and Robert Oleshak

Presentation at BIS, Basel, Switzerland

## Author's Note

This report is a personal account of the presentation by Robert Oleschak and Mike Alonso, as interpreted and compiled by Olivier Atangana.. It reflects my understanding and perspective on the topics discussed during the event.

## Introduction

The "Tourbillon Project" report presents a complex and innovative approach to integrating privacy in Central Bank Digital Currencies (CBDCs). The

project explores the feasibility of maintaining cash-like privacy in digital transactions without facilitating illicit activities.

# 1 Project Overview

**Title:** Project Tourbillon
**Objective:** To demonstrate the feasibility of cash-like privacy in Central Bank Digital Currencies (CBDCs) while preventing illicit transactions.
**Context:** With over one trillion digital payments processed in 2021, the need for privacy in digital transactions has become increasingly crucial.

# 2 Key Concepts

## 2.1 Understanding Privacy in Digital Transactions

The project underscores that CBDCs can offer a choice for making digital payments with enhanced privacy, differing from current trends. Privacy is categorized into anonymity, pseudonymity, and confidentiality.

## 2.2 Types of Privacy in Payments

- **Anonymous Transactions:** Similar to cash transactions where the parties involved are not recorded.
- **Pseudonymous Transactions:** Illustrated by blockchain transactions where identities are behind addresses.
- **Confidential Transactions:** Credit card transactions that are confidential but not necessarily private.

# 3 Challenges and Solutions

## 3.1 Anonymity and Security

The main challenge is achieving the anonymity of cash payments without supporting illegal activities.

### 3.2 Balancing Privacy, Security, and Scalability

Addressing the trade-offs between these aspects is a complex yet essential task for the project.

## 4 Technical Approach and Prototypes

- Development of two e-cash prototypes, adapting original e-cash designs and proposing new advancements with eCash 2.0.
- Implementation of privacy using one-way anonymity and advanced cryptographic methods.
- Consideration of quantum security to safeguard against future quantum computing threats.

## 5 Demonstration and Q&A Session

A live demonstration showcased the proposed system's functionality. The Q&A session included discussions on the role of central and commercial banks, transactional processes, and technical features like the absence of a deposit back to bank account option in the app demonstration.

## 6 Conclusion

The Tourbillon Project presents a pioneering approach in developing a CBDC system that harmonizes privacy, security, and scalability. The project aims to establish a new paradigm in digital payments, leveraging advanced cryptographic techniques and considering the challenges posed by quantum computing.