Project Hamilton

Conceptual Analysis

Ahto Buldas and Märt Saarepera

8. September 2022

1. Introduction

The Hamilton Project, conducted by the Federal Reserve Bank of Boston together with the Massachusetts Institute of Technology Digital Currency Initiative, is a concept study on implementing central bank digital currency (CBDC).

This report is based on the information presented in the technical paper [1] of the Hamilton project, where two possible CBDC designs are described.

In Section 2, we present basic engineering principles of CBDC design. In Section 3, we analyze both designs in the framework of the engineering principles and compare them with the KSI-Cash [3] and Bitcoin [2].

2. Engineering Principles of Designing a CBDC

Designing a CBDC implementation involves the following design choices:

1. Mathematical model of the money scheme
2. Security model related to machine implementation
3. System architecture of the service

Selection of the money scheme. The following desicions have to be made:

1. *Money units* — representation of money units: accounts, fixed-value tokens (coins, bills), etc.
2. *Payment types* — how payments change the representation of money. For example, in the account scheme, payments change the valuse of two accounts, while in the bill/coin scheme, payments change the owners of bills/coins.
3. *Emission and destruction* — how money is issued and destructed by the central bank.

Selection of the security model. There are the following two options for the security model:

- *Trusted Third Party (TTP)* — Trusted party implements the money scheme. Perimeter defence is used. Insider threats addressed with non-technical (organisational) means. Such model is used in commercial banking today.
- *Distributed Ledger Technology (DLT)* — Untrusted third party service implementing a verifiable money scheme solution. The state of money and its evolution is represented as a unique (publicly) verifiable ledger. Prevents both external and internal threats. Such model was first introduced in Bitcoin [2] and is the basis of all blockchain solutions.

Selection of architecture to guarantee the Service Level Agreement (SLA). There are the following options for implementing the SLA:

- *Single server* — the money scheme is implemented as a single server solution.
- *Server farm* — the money scheme is implemented as a network of servers.

SLA defines the following parameters:

Payment processing:

1. Payments per second
2. Payment processing (settlement) time in seconds

Payment verification:

1. Verifications per second
2. Verification complexity (computational, communicational, etc.)

In CBDC solutions, it may be necessary that both payment processing and payment verification are scalable to millions of operations per second.

Scalability means that the selected architecture should enable to increase the payment processing and verification capacity by increasing the computational/communicational power of the single server or by adding more servers to the farm.

3. Project Hamilton: Design Decisions

The CBDC solutions proposed in the Hamilton project technical paper [1] use the **UTXO money scheme** that was first proposed in Bitcoin. The UTXO representation is somewhat modified for better scalability of payment processing. Two different architectures are investigated:

- *Atomizer architecture* — a DLT solution (Figure 1)
- *Two-phase commit (2PC) architecture* — a TTP solution (Figure 2)

Atomizer architecture is a DLT solution that relies on sharded UTXO processing aming to speed up payment processing.

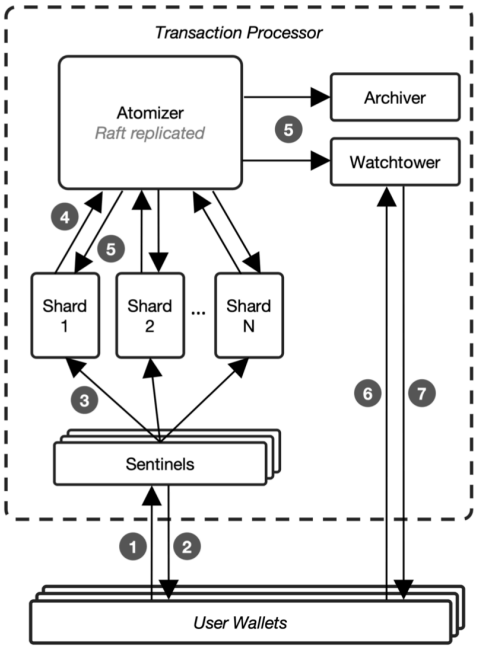

Figure 1. Atomizer architecture.

The central component of the architecture is the atomizer, which is responsible for collecting validated payments from payment processing shards and creating blocks, introducing an essential bottleneck to the overall system. Hence, payment processing as a whole is not sharded.

2PC architecture is a TTP solution where both payment processing and verification are scalable.

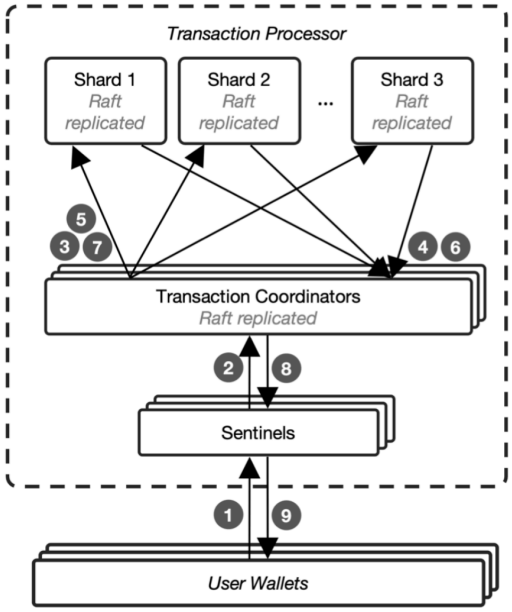

Figure 2. Two-phase commit architecture.

Comparison of the two architectures, the KSI-Cash solution [3] and Bitcoin [2] is summarized in Table 1 below:

	Atomizer	**2PC**	**KSI-Cash**	**Bitcoin**
Money scheme	UTXO	UTXO	Bill	UTXO
Security model	**DLT**	**TTP**	**DLT**	**DLT**
Payment processing	Not scalable	Scalable	Scalable	Not scalable
Payment verification	Not scalable	Scalable	Scalable	Not scalable

Table 1. Comparison of the two Hamilton architectures, KSI-cash, and Bitcoin.

References

[1] Federal Reserve Bank of Boston and Massachusetts Institute of Technology Digital Currency Initiative. Project Hamilton Phase 1—A High Performance Payment Processing System Designed for Central Bank Digital Currencies. Federal Reserve Bank of Boston. Accessed: Mar. 26, 2022. [Online]. Available: https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/61fc25f91a0df903748 8eb7d/1643914745989/Hamilton.Whitepaper-2022-02-02-FINAL2.pdf

[2] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Apr. 20, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] A. Buldas *et al*.. An Ultra-Scalable Blockchain Platform for Universal Asset Tokenization: Design and Implementation. In *IEEE Access*, vol. 10, pp. 77284-77322, 2022, doi: 10.1109/ACCESS.2022.3192837