Boom
A peer-to-peer online commerce ecosystem, independent of the banking system

Peter Alfred-Adekeye, Founder Boom

July 6, 2023

Contents

1 Abstract

Boom is fulfilling Bitcoin's original mission of using crypto for day-to-day commerce, without the need for financial institutions as trusted third party intermediaries for payment processing. At the minimum, Boom is an all-inclusive alternative and backup, to the current global commerce infrastructure.

2 The Vision

To democratise commerce and connect all humans to the global digital economy.

3 The Problem

(a) 1.7 Billion adults worldwide have no bank accounts and are financially excluded from the global digital economy. As such, they have never bought, sold or paid for anything online, despite having an annual purchasing power of over $5 Trillion. They are called the unbanked.

(b) The ongoing systemic failures in the banking system as seen with the recent failure of Credit Suisse, one of Switzerland's oldest banks, Silicon Valley Bank, Signature bank and others, continues to erode the credibility of the entire banking system. Consequently, this has led to (1) vast amounts of capital outflow from banks to safe haven assets, such as cash, the most liquid asset of all, and (2) individuals and businesses to seek an alternative way of transacting, where they can transparently monitor and access their assets round-the-clock and where settlements are instant.

4 The Solution

After years of development, Boom launched in October 2022 as an e-commerce ecosystem that enables everybody to buy, sell and pay for all goods and services online, and in-person, without needing a bank account. Boom is disrupting the way we transact globally for the better by enabling financial inclusion for all, real-time transaction settlements and asset transparency, powered by its proprietary TransactionChain technology and advanced cryptography.

5 The Technology

(a) **Boom Ledger**

All transactions on Boom are stored in its proprietary ledger, where they are cryptographically chained together forming a TransactionChain. The process of chaining transactions together involves linking each new transaction to the previous one using a cryptographic hash. This creates a chain of transactions that is extremely difficult to alter or tamper with, as any attempt to modify a transaction would require altering all of the subsequent transactions in the chain as well.

To ensure the security of communication between the client and the ledger, the Boom Ledger uses a system of authentication that combines two different technologies: TOTS (Time-based One-Time Signatures) and DAKC (Dual Asymmetric Keys Communication). The TOTS system is used to authenticate each request made to the ledger. It works by generating a unique signature for each request that is valid only for a certain period of time. This helps to prevent replay attacks, where an attacker captures a valid request and resends it to the ledger at a later time. The signature is calculated using the Edward curve digital signature algorithm (ed25519), which provides strong security.

Algorithm 1 TOTS algorithm

```
  $y \leftarrow data$
  $y \leftarrow \frac{t}{v}$
  $y \leftarrow sha512(y)$
  $y \leftarrow hex(y)$
  $y \leftarrow ed25519.signature(y)$
```

The Dual Asymmetric Keys Communication (DAKC) system is a method of ensuring secure communication between two parties, in this case the proxy API and the Boom Ledger. In DAKC, each party holds one public key and one private key. The private key is used to create a TOTS which is then verified by the other party using the corresponding public key to ensure that each communication is authentic and cannot be intercepted or tampered with by a third party.

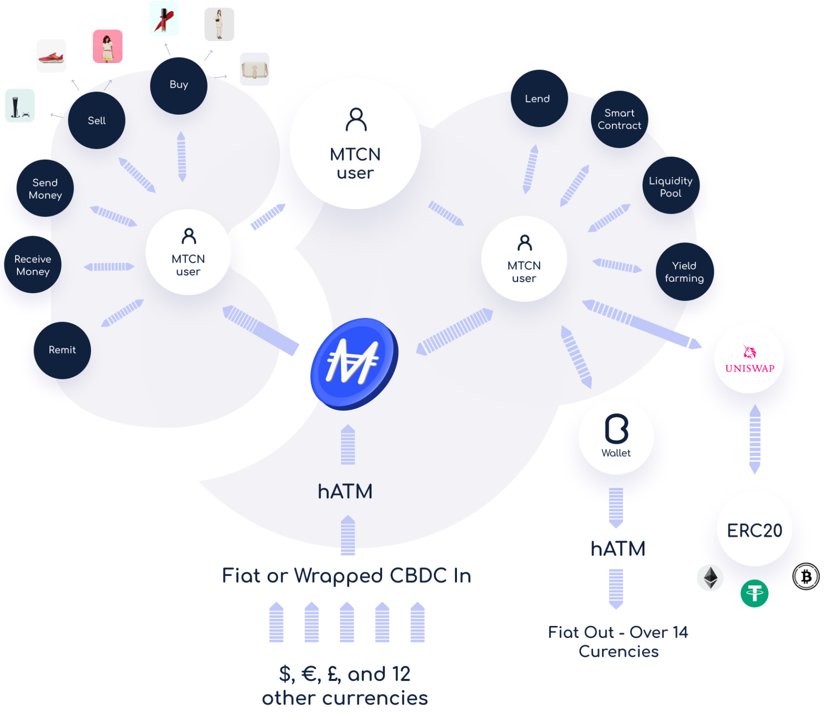
The Boom TransactionChain can currently process in excess of 1 million transactions per hour with a single node. All transactions on the Boom Ledger can be viewed on the Boom TransactionChain Explorer at (`https://boom.market/explorer`)

(b) **The Medium-of-Exchange**

The Multicoin ("MTCN") is Boom's native token and global medium-of-exchange. It enables everybody to transact internationally in their local fiat currencies.

Boom achieves this by converting fiat currencies into Multicoin, which is then delivered to the other party's Boom wallet and swapped back into fiat. Because its supply is limited and no new Multicoins can be minted, it can also be a store-of-value that can be used to hedge against inflation. The Boom wallet, which currently supports 14 fiat currencies in-app, can be funded with fiat, crypto and CBDCs. All fees on Boom are payable only in Multicoins. Total Multicoin supply is 2 Billion tokens, of which up to 700 million is earmarked towards the Boom Liquidity Pool, 300 million is allocated to the team and investors and 1 billion is held in reserve.

In March 2023, Boom was selected (along with 20 other organisations including Amazon, Cardano Blockchain, Revolut and others) by the Bank of International Settlements (which represents 63 Central Banks worldwide) via the Bank of England Rosalind Project, to create a global proof-of-concept ("PoC") framework for CBDC utility. Boom's PoC showed how CBDCs can be used to buy and sell MTCN to fund and defund the Boom Wallet. Interestingly, in the BIS model, retail CBDCs are issued directly by Central Banks to Payment-Interface-Processors like Boom, bypassing Banks.



6 The Products

The Boom super-app consists of following four applets:

- **Boom Marketplace**: A one-stop-shop and the simplest way to sell goods, (including luxury, B2B, secondhand and handmade) and services online to a global audience.
- **Boom Wallet**: Send and receive money instantly, collect money and scan-to-pay in-wallet with Boom PoS. Fund and withdraw peer-to-peer via the Boom human ATM network. The Boom Wallet can be funded / defunded in cash, in crypto and in CBDC.
- **Boom Talks**: Military-grade encrypted messaging where the private keys to encrypt/decrypt messages and sign all operations are stored only locally in the user's phone.
- **Boom Hose**: In-app social media for community engagement.

7 The Business Model

Boom monetises as follows:

- Boom charges Merchants fees on all transactions
- Boom charges fees on all remittances above €1,500
- Boom charges swap fees on all currency swaps
- Boom will introduce subscription plans for marketplace-specific value added features and functionalities. For example, Boom on-chain proof-of-ownership history verification for luxury goods.
- **All fees on Boom are payable only in Multicoins (MTCN)**.

8 References

1) S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

2) The World Bank, "The Global Findex Database", 2017

3) NPR.org, "The demise of Credit Suisse", 2023

4) Daniel J. Bernstein, "EdDSA" , 2011

5) Hayden Adams, "Uniswap", 2018

6) Boom x Bank of International Settlements, "Project Rosalind", June 2023

7) Multicoin, ”MTCN”

8) Peter Alfred-Adekeye, Bio