WHITE PAPER

Michael Blaize
CTO Mic-Apps Ltd
20th March 2018

1. INTRODUCTION

This document details the purpose, structure and implementation of **bitmore coins**, a newly created cryptocurrency aimed at mobile devices and based on a centralised and agile multi-layer blockchain for fast and secure transactions.

2. THE NEED

Conventional peer-to-peer, decentralized cryptocurrency like the well-known **bitcoins** have recently grown in popularity, but have failed to offer a real tangible alternative to conventional bank currencies for 3 fundamental reasons.

Thrustworthiness

The level of autonomy provided by the decentralised approach of regular peer-to-peer blockchains and the possibility of an illicit fork in the digital ledger (whereby a non-genuine branch is created in parallel to the real chain), like the one that required the Bitcoin blockchain to be rolled back in 2016, has undermined the trustworthiness of this type of currencies.

Suistainability

The decentralised and shared blockchain of conventional cryptocurrencies calls for a computationally expensive proof of work. The limited number of blocks (typically a handful per hour) has led to an "arms race" and miners have resorted to high-performance computers. The energy required for this mining process is significant and has been openly criticised as unsustainable and unfit to our modern energy challenges.

Speed & Flexibility

The difficult and long mining activity results in a juddered cumbersome process. Transactions are stacked in large blocks that are mined slowly. Transactions are only really accepted once they have proven to be part of a genuine branch and it can therefore take hours before being fully acknowledged by the recipient as genuine.

3. BITMORE CONCEPT

Bitmore brings a timely evolution of regular cryptocurrency, using a centralised, multi-layer blockchain system offering:

- A centralized and open but trustworthy, secure and controlled transaction ledger;
- A reduced-difficulty proof of work to minimise energy requirements while still ensuring robustness of the digitally encrypted chain;
- A fast and flexible process where blocks, each containing a single transaction, can be mined in parallel by all users.

Bitmore coins are devised to be managed uniquely on mobile devices (smart phones and tablets running iOS or Android). Transactions are mined directly by the user performing the

transaction, meaning anyone who creates, buys or sends coins to another user. The proof-of-work takes an average of 30 seconds on a modern smartphone.

4. BITMORE BLOCKCHAIN ARCHITECTURE AND BLOCK STRUCTURE

The blockchain is organised in levels, with each level holding up to a pre-set number of blocks (currently up to 1,000). A new level is created every time the maximum number of transaction has been reached, or if the same user is involved in a bilateral transaction (one user gives coins to another). This ensures that all transactions on one level are all independent from one another.

Each block within one level is directly woven to the blocks in the preceding level using a Merkel root. The whole blockchain forms a tight matrix being extended continuously by users mining their own transactions into new blocks.

The block structure is defined by a 160 bytes input sequence, as described in figure 1 below. Block details include the id of the two users taking part in the transaction, the amount of coins being transferred and finally a 256-character information or content sequence (this can be anything defined by the user initiating the transaction). These details are hashed together.
The block input sequence is encrypted through SHA2-256. The proof-of-work consist in finding a nonce that will result in the block hash being lower than a predefined threshold (currently starting with at least 5 zeros).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
		VERSION									Difficulty				
Merkel Previous Level Blocks															
Block details hash [block id, id1, id2, amount, content)															
		TIMESTAMP											NONCE		

Figure 1 – block structure

5. TRANSACTION PROCESS

All transactions follow a simple and robust process: the user defines the transaction, gets a slot in the chain and has up to 5 minutes to complete its mining process on his device to validate the transaction and tie the block into the chain. At which point, the block is registered successfully within the chain as valid and funds are allocated accordingly. If the user has already been involved in a bilateral transaction then the network waits for the mining operations already registered on the current level to be completed before initiating a new level where the user can finally mine his new transaction.

From the genesis block seating at level 0, successive levels of blocks are generated every time the pre-set number of blocks has been reached, or a user registers a second bilateral transaction.

6. COINS ACQUISITION

In addition to being sent coins by another user (as a payment for goods or services), users can create new coins by mining them or buying them.

New coins mining

A simple mining operation will allocate a number of coins to the user performing the mining. This can be done directly on the user's mobile device and as with any other type of transactions, take an average of 30 seconds. The number of coins is set centrally. It is currently set to 10 new coins.

New coins purchase

New coins can be bought at a value that is calculated based on the number of coins in circulation as defined in the following paragraph (7. Value Management). As per mining new coins, buying new coins works in a similar fashion to any other transactions. After the user has chosen the number of coins he would like to purchase, the transaction is mined by the user and tied into the chain. Once payment has been received, the purchase transaction is fully validated and will appear as successful in the ledger, with the new coins allocated to the user.

7. VALUE MANAGEMENT

The majority of cryptocurrencies are not recognised on trading markets. Bitmore offers 2 mechanisms to protect value and foster user to user trading.

Any user can generate a number of coins by simply mining a new allocation. Each mining operation will create a pre-defined number of coins (currently 10). As per normal transactions, the mining process will take an average of 30 seconds.

Coins can also be purchased directly from Mic-Apps Ltd. In this case, the purchase is also registered as a mined transaction. The value of each Bitmore coin is calculated based on the number of coins in circulation. The more coins created by users, or purchased, the more the value Bitmore coins increases. A predefined algorithm targets an average of 10% increase in value every 4 weeks.

The Bitmore platforms also intend to open a trading system, whereby users will be able to offer their coins to other users for them to purchase at a price to be set by the seller.

8. AVAILABILITY

Bitmore coins is available to download for free from iOS App Store and Android Play Store.

iOS link: https://itunes.apple.com/us/app/bitmore-coins/id1355891102?ls=1&mt=8

Android link: https://play.google.com/store/apps/details?id=com.mic_apps.bitmore-coins