The e-Banknote as a ‘Banknote’: A Monetary Law Interpreted

Benjamin Geva, Seraina Neva Grünewald, Corinne Zellweger-Gutknecht

gqab019, https://doi.org/10.1093/ojls/gqab019
Published: 25 May 2021

(iv) BitMint

BitMint money, developed by BitMint, was identified as ‘the only candidate qualifying as a universal digital representation of worldwide currencies’.[128] A bit-minted currency, unlike all known cryptocurrencies, does not rely on algorithms that may be solved by quantum computers but rather on quantum-grade randomness.[129] Each coin has a unique identity; however, the identities of the bits do not determine the coin’s value. The value of the coin appears in a part of the coin called the payload string. The identity string and the payload string are based on pure randomness and are fused together inseparably.

Users receive a coin on their devices, similar to receiving a text message. They can then split the coin to make payments for any sum up to the sum of the coin. Payment is carried out by directly transmitting the bits that comprise the coin-split to the payee’s device under any communication method without the real-time intervention of any remote server. Thus, BitMint facilitates continuous payment made simultaneously in real time during the purchase—for example, when a buyer fills their car’s fuel tank at a gas station.

Having a unique identity, a coin can be designated as tethered money, so it is possible to tie to it terms of use, an expiration date, an intended purpose, a time of payment or a designated redeemer.[130] In addition, the BitMint digital money framework facilitates uninterrupted payment online and offline (the latter meaning that it is not dependent on network availability),[131] and allows peer-to-peer payments.

BitMint is centrally minted. Its rCBDC solution is a digital claim check to a defined quantity of a specific commodity, including a fiat currency.[132] It can be issued either directly by a central bank[133] or by a private issuer, such as a commercial bank,[134] ideally holding a 100% reserve.

BitMint digital currency may be operated either as a unified global digital money platform or decentralised in a system wherein each central bank operates its own CBDC mint. Central banks can, however, choose any distribution and/or authentication channel, whether of BitMint's delegated authentication solution or delegated to designated dealers, such as commercial banks, delegated mints and/or distributed ledgers network (eg blockchain, Ethereum). When authenticating on a distributed ledger, only the coin's identity is exposed; it is unnecessary to expose the value, such as when authenticating cryptocurrencies. When the central banks of various countries launch their own respective rCBDCs, or if one large country chooses to authorise several local mints, full interoperability will be facilitated through BitMint's InterMint.[135]

BitMint's technology enables controlled privacy, from full anonymity to full traceability and anything in between, in compliance with regulatory requirements in each jurisdiction. The coin itself can carry its chain of custody (optional), which can only be bypassed by court order.[136] Each coin is equipped with smart contract capabilities. Through its quantum randomness generation process, distribution management model and technical architecture, BitMint retains the basic characteristics of having quantum security,[137] resisting counterfeiting and discouraging money laundering.

(v) Assessment

The ECB Digital Euro Report stresses that the digital euro is neither a crypto-asset nor a stablecoin.[138] However, this statement ought to be regarded with some scepticism. We take the first part of the statement to indicate that the digital euro will not be a self-anchored cryptocurrency, as Bitcoin is. The second part suggests that the digital euro will not constitute a claim to the euro, but rather will be a euro in its own right.

However, this is analogous to stating that the paper banknote is not a promise to pay money but *is* money. Accordingly, we do not understand the ECB Digital Euro Report as rejecting an e-banknote that 'promises' to pay in euro. Nor do we take the Report to reject (or provide reasons for the rejection of) a cryptocurrency along the lines of Libra/Diem.

Our own assessment is that a public digital currency in the form of a cryptocurrency, even if it is a (sterile claim check) stablecoin, has a few drawbacks from both legal and technological perspectives. In a cryptocurrency, the coin consists of the total amount available in the wallet. Put otherwise, a coin is not handled as a unique and separate entity from the beginning of a payment transaction to its end. Finality of payment is also less clear on a blockchain. Furthermore, in a cryptocurrency, the sequence of the bits represents the value of the coin. Since it is unique to each coin, it is this sequence that gives the coin its identity. Accordingly, insofar as each coin in WingCash and BitMint has both an identity and a specific value, as separate functions and from the beginning of the transaction to its end, both stand closest to the paper banknote among the three designs that we have presented.

The WingCash coin, as a digital representation of the fiat currency banknote, is the closest to the paper banknote. At the same time, the BitMint payment transaction more closely assimilates payment in cash, as it does not require any intermediation. BitMint also facilitates continuous payment, coin splitting and tethering. Furthermore, a unique key feature of BitMint, which has not been shown to exist for the others, is the complete lack of dependence not only on the internet, but on any communication network. As such, it appears to meet a universal access requirement,[139] implying a degree of independence from communication networks, particularly the internet. This facilitates access by unbanked individuals and individuals without digital devices, as well as access in cases of network failure, particularly in disaster situations. Thereby, BitMint payment is closely assimilated to payment using physical banknotes.

Thus, while substantially enhanced through the use of smartphones and the internet, BitMint payments may be made using simple mobile phones over the cellular network. When using more sophisticated devices, proximity BitMint payments, which may be a necessity in emergency situations, can be made without any communication network. For example, the payer's device may generate a QR code[140] that the payee's device takes a picture of, thereby completing the payment. A payment may also be made via near-field communication (NFC),[141] which most smartphones are capable of. Finally, trust facilitating payment may be generated by the payee's inspection of a hard wallet containing the money. The hard wallet is a physical device that can dispense identity-bearing digital currency. It may be an independent device, serving unbanked or underbanked people as well as people without mobile phones, or a chip embedded in a smartphone that can work offline. Payment issued from the hard wallet can be taken in by a second hard wallet, which will forward the payment to another hard wallet, creating a payment ecology of digital money over long periods without the need for a communication network.[142] Therewith,

> All that the payee has to do is to attach a simple measuring device to the physical wallet, take instant measurements and compare them to the pre-loaded figures published by the manufacturer. If the two sources agree, the payee is satisfied and regards the bits that subsequently flow out from this wallet as bona fide money.[143]

Blockchain technology currently seems to be leading the way in CBDC research and projects.[144] Regardless of legal interpretation, however, it remains to be seen whether a blockchain-based CBDC can provide the required quantum security, speed and scalability to replace physical cash, become legal tender and enable fee-free, frictionless, instantaneous and unconditional money transfer with legal finality of value between any two parties.