4-22-2020

Payment in Virtual Currency

Benjamin Geva
Osgoode Hall Law School of York University, bgeva@osgoode.yorku.ca

Virtual Currencies and the State
B. Geva, Payment in Virtual Currency

April 22, 2020

Benjamin Geva, Osgoode Hall Law School of York University[1]

By reference to an analysis of the operation of payment in traditional forms of money, this essay explores the meaning of 'virtual currency'[2] and the mechanism for payment in it. Endeavoring to identify directions in which events will unfold, the essay sets the stage for a future detailed analysis of pertaining legal aspects.

Payment of money has traditionally been made in either currency or account balance. Payment in currency is by physical delivery from one person (payer) to another (payee) of banknotes and coins. Typically, this is a face-to-face process which does not require intermediaries. More specifically, 'payment' is "a bilateral act which requires the [payee] to accept the [payer]'s act of tender";[3] and is completed on the passage of possession in the money when the payee takes delivery, thereby manifesting the acceptance of the tender. Typically, banknotes and coins are denominated in the unit of account of a national currency and are legal tender in the country of issue.

Payment in account balance requires intermediation. It is carried out by having the payer's account debited and the payee's account credited. Typically, both accounts are held at regulated financial institutions, broadly speaking, banks. Both accounts are typically denominated in the unit of account of a national currency. Payment is performed by means of either the extinction or reduction of the debt owed to the payer by the payer's account-holding bank and either the creation or increase in the debt owed to the payee by the payee's account-holding bank. Where payer and payee hold their respective accounts at two banks that are correspondents, payment in account balance requires the debiting the account of the payer's bank by the payee's bank or crediting the account of the payee's bank by the payer's bank. In a domestic payment system, at least all major banks hold their accounts with the central bank so that the interbank component of payment between two such banks is carried out as part of the multilateral interbank settlement on the books of the central bank. Otherwise, payment in account balance requires a chain of settlements on correspondent accounts, with or without settlement on the books of the central bank, or alternatively, one settlement between correspondent banks followed by another settlement on the books of a central bank.

The architecture of the interbank payment system is centralized. Thereunder, a bank maintains accounts for customers. For its part, a large bank may also maintain accounts for correspondent banks. Finally, the central bank maintains settlement accounts at least for large banks. As a whole, the system can be visualized as a pyramid at whose head or apex stands the central bank with which at least large banks hold accounts, and possibly with small banks holding accounts with large banks. Individual and corporate customers are at the bottom or base of the pyramid holding their accounts in banks (whether large or small). Money denominated in the domestic fiat currency and held in bank accounts is redeemable in banknotes and coins which usually constitute 'legal tender'.

With the advent of electronic banking, it became possible to initiate, transfer and process payment instructions electronically. Payment in account balance so performed is known as an electronic funds transfer. It became also possible to 'load' monetary value (that is, value denominated in an official or, in fact, any unit of account) on a tamper-resistant stored-value device such as a card or personal computer.

In such a case, the value became known as ‘electronic money’ or ‘e-money’. Most e-money schemes have involved “balance-based” products. In such products, devices store and manipulate a numeric ledger, with transactions performed as debits or credits to a balance. Accordingly, this type of e-money is a monetary balance or value recorded electronically on and is available from a stored-value product (SVP), such as a chips card, or a hard drive in a personal computer, or a server. Such a record, accessible from the device without resort to the bank’s computer system, can be viewed as a decentralized bank account. E-money is said to “differ … from so-called access products, which are products that allow [customers] to use electronic means of communication to access otherwise conventional payment services” in and out bank accounts.[4] Alternatively, with a ‘pre-paid product’ variant, monetary value is available from a master account, belonging to the issuer or someone acting on the issuer’s behalf.

A minority of e-money products may still operate on devices that store electronic “notes” (sometimes called coins or tokens) that are uniquely identified by a serial number and are associated with a fixed, unchangeable denomination. In such a “note-based” model, transactions are performed by transferring notes from one device to another, and the balance of funds stored on a device is thus the sum of the denominations of all notes on the device. However, as in the “balance-based” products, transferability is typically restricted, and cardholders may usually make payments only to merchants who may clear these payments or deposit the accumulated balances exclusively through their acquiring banks.

E-money is ultimately a variant of ‘bank money’; thus, whether e-money is purchased in cash or by means of a debit to the purchaser’s bank account, the issuer has its own bank account credited with the amount sold to the purchaser. Where the e-money is purchased from a bank, the account credited is the reserve account of the selling bank. Payment in e-money is forwarded to the payee’s bank which credits the payee’s account with the amount of payment and forwards the e-money itself for redemption against the value previously credited to the seller’s account. In the final analysis, even where pre-paid value or e-money is not issued by a bank, a scheme must facilitate the purchase and redemption through banks.

Particularly outside the banking system, a balance-based payment product need not necessarily be provided in an official unit of account. For example, a balance-based payment product may be denominated in weight units of gold. As well, a balance-based product may be redeemed by specific product, usually the one in which it is denominated. Furthermore, a balance-based product may be backed – in whole or in part– by a reserve made of the product itself. In fact, any proposed ‘full reserve banking’ scheme will provide a balance-based bank product fully backed by central bank money.

For its part, digital currency consists of digital coins, and is a completely stand-alone category distinguished from both currency (cash) and balance- based (including e-money) products. A digital coin is a distinct entity consisting of data expressed in a unique string of bits which represent value.[5] Like physical coins and banknotes, digital coins are not paid out of bank accounts so that their payment does not appear to require intermediation by banks. And yet, exactly as the electronic funds transfers, they are paid over the cyber space. A privately issued digital currency is known as ‘virtual currency’ and may have its own unit of account, fluctuating by reference to the value of an official unit of account, in which case it is self-anchored. Alternatively, it may be a ‘claim check’ or stablecoin, either in a unit of account of an official currency, or in the value of a specific commodity, whether or not it is fully (or even partially) backed by a reserve of such currency or commodity. Each coin may be in the form of a total unspent amount in a wallet or a representation of what otherwise would be a physical banknote.

Virtual currency is frequently treated as a digitally-traded or transferrable digital representation of value.[6] In my view, a definition along such lines is too broad. It encompasses account balance represented and transferred digitally and entirely misses the fundamental feature of the separate identity of each digital currency coin, facilitating holding and transferring without an account.

An account as well as an undivided share in a stock of digital coins may however be held with an exchange or other depositary or virtual bailee. Controlling them, the latter may thus occupy a position analogous, or at least similar, to that of a bank in relation to the deposit of funds.

Unlike payment in account balance, payment in digital currency need not be recorded on a centralized ledger. However, in a given scheme, coins may be issued, transferred and redeemed under centralized protocol in which case the scheme is said to be centralized. Conversely, a scheme under which a digital currency is issued, transferred, and redeemed over a distributed ledger is decentralized. Finally, a digital currency transferable under a decentralized protocol – such as over a distributed ledger and yet issued by a centralized operator – is hybrid.

Centralized protocol does not require the intermediation of bank accounts and is thus entirely different from a centralized architecture in account-balance payment systems. At the same time, payment in digital currency, while being made from one digital device to another, requires the intermediation of an electronic network. Depending on its format, it may further require the intermediation of a custodian acting as a virtual storer or warehouse person for the coins.

The distributed ledger underlying decentralization is an asset database that can be shared across a network of multiple sites, geographies or institutions. Blockchain is an underlying technology, requiring the Internet to support and maintain its peer-to-peer network, that enables digital implementation of a distributed ledger. Being a computerized ledger on a distributed network, it generates a single version of the record on each computer. Its essence is:[7]

> *a type of a database that takes a number of records and puts them in a block … Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.*

Accuracy of the ledger is corroborated under a method determined under rules adhered to by participants. Record security and visibility to authorized users is ensured by cryptography.

A "*cryptocurrency*" denotes a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the execution of payment transactions on a decentralized network. Cryptography is thus used in cryptocurrencies to express and protect the value of the coins (the sequence of the bits), to prevent counterfeiting and fraudulent transactions, as well as to perform validation, execution and recording. These functions are carried out on a distributed ledger, such as a blockchain. Thereon, each block contains a cryptographic hash or algorithm that links it to the previous block along with a timestamp for the transactions from that block. The network allows online payments to be sent directly from one party to another without going through a bank or any other account holding centralized counterparty.

The mechanics of payment in a digital coin depends on the specific design of the coin and its underlying scheme. As stated, the mechanism requires the use of a telecommunication network. But to avoid double use of the same digital coin, it also requires some validating intermediary. Several options are available:

1. Being in control of a digital coin 'affixed' to a single internet domain, for which it attorns to the payer, a 'baliee' complies with the payer's instructions and executes them by attorning to the payee, thereby causing 'possession' in the coin to be transferred from the payer to the payee.
2. A 'coin' in the form of an unspent transaction output (UTXO)[8] in the payer's wallet, reflecting earlier transactions, is transformed into a new UTXO in the payee's wallet. Where the payer does not use up the entire UXTO, payment is carried out by splitting the payer's UXTO into two UTXO's: one in the sum of payment going to the payee's wallet, and the second, in the amount of the balance of the UXTO, remaining in the payer's wallet.

3. The payer sends from his or her digital device to the payee's device a 'coin' or any split of it. The payee may (but is not required to) validate the coin authenticity with the 'mint.'

Respectively, these are the methods of payment in WingCash, Bitcoin and BitMint. Among these three, only Bitcoin requires a blockchain and is a cryptocurrency. Neither WingCash nor BitMint are cryptocurrencies. No blockchain is required in BitMints or even exists in WingCash.[9]

Arguably, payment in digital coins is completed when the coins get under the full control of the payee. From this perspective, completion of payment in digital coins and the discharge of the debt paid by them are governed by rules that are fundamentally similar to those governing payment in cash as well as in account balance. This, however, does not resolve the question of loss allocation where something goes wrong by the intermediary, namely the blockchain, 'mint' or switch. In principle, between the payer and the payee, loss is to be allocated as agreed between them, except that the law should establish a preemption, one way or another.

Predicting the impact of digital currencies is beyond the scope of this essay. I will however conclude by pointing at two directions to watch for.

First, payment in a digital currency bypasses account intermediation which is at the heart of payment in account balance. In the struggle for market share, efficiency thus appears to side with digital currencies. However, use of the latter raises its own risks, relating to trust, financial stability and misuse. Certainly, to meet such risks, oversight and regulation are required. The challenge is to ensure such oversight and regulation will put both methods of payment on an equal footing.

A second perspective to be watched is the competition between 'self-anchored' and 'claim check' virtual currencies, or more specifically, those denominated in an official currency.[10] At the heart of this competition is the old controversy as to the concept of money, i.e. whether its value is based on the salability of the material from which it is made or on the power of its issuing authority. Having historically identified gold as the optimal material on the basis of its low stock-to-flow ratio,[11] the former is known as the metalist[12] approach. The latter is known as chartalist.[13] Not surprisingly, metalists anticipate the triumph of 'self-anchored' currencies with low stock-to-flow ratio, such as Bitcoin,[14] which may thus be characterized as 'digital gold.' For their part, chartalists are likely to anticipate the triumph of 'claim check' currencies denominated in an official currency unit.[15]

——

1. This essay draws on and yet builds on Benjamin Geva, "Cryptocurrencies and the Evolution of Banking, Money and Payments," in Chris Brummer (ed.) *Cryptoassets – Legal, Regulatory and Monetary Perspective* (Oxford University Press, 2019) 11-37 (+ 341-366 EN). ↑

2. For a detailed albeit earlier discussion see Benjamin Geva, "Disintermediating Electronic Payments: Digital Cash and Virtual Currencies", (2016), 31: 12 J.I.B.L.R, 661 at 664-65. ↑

3. David Fox, *Property Rights in Money* (Oxford: Oxford University Press, 2008) at 28. ↑

4. CPSS, *Implications for Central Banks of the development of electronic Money* (Basle, October 1996) at 1, emphasis in the original; online: https://www.bis.org/publ/bisp01.pdf, visited January 17, 2020. ↑

5. According to Gideon Samid, *Tethered Money: Managing Digital Currency Transactions* (Elsevier Academic Press, 2015) at 105-106, the unique string of bits should better experess both identity and value. ↑

6. See e.g. Section 102(23) Uniform Regulation of the Virtual-Currency Business Act, Drafted by the National Conference of Commissioners on Uniform State Law (NCCUSL) and approved and recommended by it for enactment in all the states in the United States at its Annual Conference Meeting in its 126th year in San Diego, California on July 14-20, 2017. So far it has been enacted in Rhode Island and introduced in California, Oklahoma and Hawaii. It is available online with Prefatory Note and Comments (and more information) at: https://www.uniformlaws.org/committees/community-home?communitykey=e104aaa8-c10f-45a7-a34a-0423c2106778&tab=groupdetails visited January 17, 2020. See also FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATS, 2019) at 13, online: http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf, visited January 16, 2020. ↑

7. UK Government Office for Science, "Distributed Ledger Technology: beyond block chain" (2016) at 17, online: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>, visited January 17, 2020. ↑

8. The term is explained e.g. in https://komodoplatform.com/whats-utxo/ , visited on January 16, 2020. ↑

9. These systems are set out in Geva, n.1 *supra*, where direct sources are cited. ↑

10. I assume that it is issued by a trusted, properly regulated entity so as to bear a similar risk to the officially issued currency. ↑

11. This is the relation between its existing supply and the extra production that will be made in the foreseeable future. A currency with a low ratio is 'hard' so as to maintain its value. ↑

12. See e.g. Carl Menger, "On the Origins of Money" (1892), 2 Economic Journal 239 (translation by CA Foley). ↑

13. For this theory see at length: L. Randall Wray, "From the State Theory of Money to Modern Money Theory: An Alternative to Economic Orthodoxy (Working Paper No. 72, March 2014, Levy Economic Institute of Bard College) ↑

14. See e.g. Saifdean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, (Hoboken NJ, Wiley, 2018) ↑

15. For an analysis preferring the chartalist approach in general see: Charles A. E. Goodhart, "The two concepts of money: implications for the analysis of optimal currencies areas" (1998), 14 European Journal of Political Economy 407. ↑