

4-14-2016

Virtual Currencies and Blockchains: A Primer

Benjamin Geva

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

Follow this and additional works at: http://digitalcommons.osgoode.yorku.ca/public_writing



Part of the [Law Commons](#)

Recommended Citation

Geva, Benjamin, "Virtual Currencies and Blockchains: A Primer" (2016). *News, Editorials, and Commentaries*. 140.
http://digitalcommons.osgoode.yorku.ca/public_writing/140

This News Article is brought to you for free and open access by the Faculty Scholarship at Osgoode Digital Commons. It has been accepted for inclusion in News, Editorials, and Commentaries by an authorized administrator of Osgoode Digital Commons.

Virtual Currencies and Blockchains: A Primer

April 14, 2016

Benjamin Geva

With the advent of virtual currencies and blockchain technologies the global payments landscape may be irreversibly transformed. This bulletin is designed to present basic concepts underlying this transformation.

What You Need To Know

A report published in February 2015 by the ECB,¹ defines a *virtual currency* to be:

a digital representation of value, not issued by a central bank, credit institution [i.e. "bank"] or e-money institution, which in some circumstances, can be used as an alternative to money

Similarly, according to an IMF study, virtual currencies are defined to be:

digital representations of value issued by private developers and denominated in their own unit of account²

Virtual currency schemes are predominantly decentralized, namely, have neither a central repository nor a single administrator. They use encryption techniques, particularly public-key cryptography,³ to regulate the generation of units of currency and verify payments.⁴

The currency of which the generation of units and verification of payments are regulated by cryptography is thus called cryptocurrency. It is a digital asset with verifiable mathematical properties that can be transferred directly between users on a distributed ledger without relying on a centralized protocol operator.

A distributed ledger is an asset database that can be shared across a network of multiple sites, geographies or institutions. Its underlying technology is the *blockchain*, which is:⁵

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 by consensus.

Participants in a cryptocurrency network hold their keys in digital wallets. A payer pays with his or her digital coins stored in the blockchain using his or her private key and the payee's public key. For virtual currencies, specialized trading platforms function as marketplaces while exchanges offer trading services.⁶

The emergence and rise of virtual currencies as cryptocurrencies has raised significant legal and regulatory questions. An overarching one is whether a virtual currency is "money" or "currency."⁷ This is a matter of importance for both private and public laws. A virtual currency is however certainly a means of payment so as to be of interest to central banks in relation to the stability of prices, the financial system, and the payment system. Central banks are also concerned with the lack of legal basis and the risk to their reputation.⁸ Other regulatory concerns include financial integrity, consumer protection, taxation, exchange controls and capital flow management.⁹ Underlying many of the concerns are both the fluctuating value of each virtual currency and the absence of central governance authority. And of course there are the "usual" payment system issues of transparency and fairness of terms and fees, hacking, finality of payment, and the allocation of losses caused by fraud, error or insolvency.¹⁰ In Canada there may also be an issue as to the appropriate level of government to address each issue.

In the United States a draft of the *Regulation of Virtual Currency Business Act* is currently emerging as a project of the National Conference of Commissioners on Uniform State Laws (NCCUSL).¹¹ The project covers licensing, examinations, reports and records, permissible investments, and enforcement. Subject to some refinements and express exclusions, Section 103(24) of the present draft defines "Virtual currency" as "any digital unit of value that is used as a medium of exchange or that substitutes in transaction for money but that is not money." "Money" is defined in Section 103(8) by reference to its issue or designation by a government body.

Bitcoin¹² is both the originator of the blockchain technology and at present the predominant cryptocurrency scheme. It is a peer-to-peer payment network and virtual currency based on an open source protocol, which makes use of a public transaction log. Another innovative player to be mentioned is Ripple. Besides for a native currency, its protocol also provides for currency-agnostic payment rails for multi-currency payments in both other virtual and fiat currencies across the world.¹³ In the UK, other than over Ripple rails, a privately funded venture called SETL intends to develop a specialized blockchain that will allow the settlement of securities transactions on a peer-to-peer basis in central bank money.¹⁴

In the final analysis, sooner or later regulatory and legislative measures will have to take place to accommodate the quickening pace in which virtual currencies and blockchain applications evolve.

¹ See European Central bank/Eurosystem, *Virtual Currency Schemes- a Further Analysis*, February 2015, at 25 available online at: <https://www.ecb.europa.eu/pub/pdf/other>

[/virtualcurrencyschemesen.pdf](#).

² See IMF Staff Discussion note *Virtual Currencies and Beyond: Initial Considerations*, January 2016, at 7, available online at: <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>.

³ https://en.wikipedia.org/wiki/Public-key_cryptography.

⁴ See: https://www.google.ca/search?q=crypto+currency&sourceid=ie7&rls=com.microsoft:en-CA:IE-Address&ie=&oe=&gfe_rd=cr&ei=hf3iVpLqJlfdswSny6OAAg&gws_rd=ssl.

⁵ See UK Government Office for Science, *Distributed Ledger Technology: beyond the block chain* (2016) at 17.

⁶ Voluminous information on the mechanics of a cryptocurrency payment is available in the reports and studies cited herein as well as in a Report of the Standing Senate Committee on Banking, Trade and Commerce (Canada), *Digital Currency: You Can't Flip This Coin!* (June, 2015).

⁷ Both "currency" and "money," together with other relevant terms, are defined in the 2015 ECB Report, above note 1 at 33.

⁸ See European Central bank/Eurosystem, *Virtual Currency Schemes*, October 2012, at 22-46 available online at: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Further discussion including a summary of national responses is available in the 2015 ECB Report, *ibid.* at 26 – 33.

⁹ See e.g. IMF Report above note 2 at 24-34.

¹⁰ See e.g. Sarah Jane Hughes, and Stephen T. Middlebrook, "Advancing Framework for Regulating Cryptocurrency Payments Intermediaries" (2015), 32 *Yale J. on Reg.* 495.

¹¹ The most recent Draft is that of the Drafting Committee Meeting of February 19-21, 2016, available online at: http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2016feb_RVCBA_Mtg%20Draft.pdf. For a review see e.g.: http://www.sidley.com/news/2016-02-26_banking_and_financial_services_update_

¹² Conventionally "Bitcoin" capitalized refers to the technology and network whereas "bitcoins" lowercase refers to the currency itself.

¹³ Jessie Cheng and Benjamin Geva, "Understanding Block Chain and Distributed Financial Technology: New Rails for Payments and an Analysis of Article 4A of the UCC," *Business Law*

Today 25 no. 7 (March 2016), http://www.americanbar.org/publications/blt/2016/03/05_cheng.html.

¹⁴ The UK Government Report, above note 10 at 60.

To discuss these issues, please contact the author(s).

This publication is a general discussion of certain legal and related developments and should not be relied upon as legal advice. If you require legal advice, we would be pleased to discuss the issues in this publication with you, in the context of your particular circumstances.

For permission to republish this or any other publication, contact [Janelle Weed](#).

© 2017 by Torys LLP.

All rights reserved.