Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/CLSR
ELSEVIER
Computer Law & Security Review

Cryptocurrencies are (smart) contracts

Simon Geiregat[*]

Financial Law Institute, Ghent University, Belgium

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Bitcoin
Block
Blockchain
Chain
Cryptocurrency
Coin
Smart contract

ABSTRACT

The functioning of cryptocurrencies like *Bitcoin* ultimately depends on participants' agreements to selectively disclose or conceal information. Various arguments suggest that those agreements amount to a large multilateral contract to which all participants are parties. That multilateral agreement is automatically enforced through smart contract technology. Therefore, cryptocurrency "wallet holders" are simultaneously creditors and debtors of smart contract claims vis-à-vis their cryptocurrency community.

Cryptocurrencies and smart contracts are based on the same technology: blockchain (also spelled "block chain"). Thus far, legal literature seems to have ignored that both phenomena share more than their technical backbone.[1] Cryptocurrencies and smart contracts can fit in one and the same private-law classification. More specifically, the former is a specific subtype of the latter. This Comment paper seeks to prove that claim in three steps. First, Section 1 examines the technical aspects of cryptocurrencies, which are briefly explained. Next, Section 2 analyses cryptocurrencies from a private-law perspective. Lastly, the findings from that analysis are tested in Section 3 against the doctrinal concept of smart contracts.

1. Cryptocurrencies technically

1.1. *Origins*

Cryptocurrency systems are implementations of a theoretical model described in a pseudonymously published paper

[*] Corresponding author: Faculty of Law and Criminology, Ghent University, Universiteitstraat 4, 9000 Ghent, Belgium.
E-mail address: simon.geiregat@ugent.be

[1] see e.g. Christoph Simmchen, 'Blockchain (R)Evolution: Verwendungsmöglichkeiten und Risiken' [2017] MMR 162, 164; Joachim Schrey and Thomas Thalhofer, 'Rechtliche Aspekte der Blockchain' [2017] NJW 1431, 1431; T F E Tjong Ting Tai, 'Blockchain en smart contracts' [2017] Tijdschrift voor Privaatrecht 563, 577 para 20; Christoph Van der Elst and Anne Lafarre, 'Blockchain and the 21st Century Annual General Meeting' (2017) 14 ECLJ 167, 172 ch 3; Klaus Eschenbruch and Robert Gerstberger, 'Smart Contracts: Planungs-, Bau- und Immobilienverträge als Programm?' [2018] NZBau 3, 4.

https://doi.org/10.1016/j.clsr.2018.05.030
0267-3649/© 2018 Simon Geiregat. Published by Elsevier Ltd. All rights reserved.

by Satoshi Nakamoto.[2] The basic idea is to create a money transfer system that does not require interventions by governments, financial institutions or other third parties. Such systems inevitably require participants to put their trust in those third parties, and are therefore inherently flawed. Cryptocurrency users instead put faith in the power of computers to crunch numbers, as well as in a high degree of transparency that allows anyone to monitor all other users' actions.[3] People from all over the world have collectively implemented that model in practice by creating the *Bitcoin* system. Later, other cryptocurrency systems emerged.[4] All cryptocurrency systems are nonetheless derived from the very same model.[5]

1.2. *Coins, wallets and signatures*

Participants in a cryptocurrency system trade in cryptographic units sometimes called "coins". A coin consists of an extremely long code made up of a combination of digital signatures. Each coin transfer requires a digital signature that pertains to the person who previously held that coin in his cryptocurrency "wallet". This person can only insert this signature with the help of a unique, secret code: his highly confidential "private key".[6] All of this allows consenting participants to transfer coins via the Internet.[7]

1.3. *Blockchains and miners*

Cryptocurrency systems fully depend on the existence of blockchains. These chains make up a shared public ledger[8] that allows anyone to see all transfers[9] subject to any given coin.[10] "Miners" provide for control. These actors check whether all transfers are duly accompanied by a technically valid electronic signature and whether the blockchain of the coins is uninterrupted.[11] As this verification process requires extremely difficult calculations, miners need powerful computers to comply with their monitoring task. The system therefore rewards them with new coins in exchange for their verification effort. This incentive is intended to be a stimulus for them to make all investments necessary for future verifications.[12] As long as the majority of the miners fulfil this task in good faith,[13] blockchain technology ensures that a wallet-holder cannot successively spend one and the same coin multiple times.[14]

1.4. *Summary*

The technical details of cryptocurrencies are described in depth in doctrine and on the Net.[15] This paper instead requires stepping back and abstracting from those details. Looking at cryptocurrencies from a distance, two aspects prove to

[2] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' <https://bitcoin.org/bitcoin.pdf> accessed 1 May 2018.

[3] ibid 1-2 ch 1-2; see Jens Ekkenga, 'Bitcoin und andere Digitalwährungen – Spielzeug für Spekulanten oder Systemveränderung durch Privatisierung der Zahlungssysteme?' (2017) 11 CR 762, 762-763 <https://doi.org/10.9785/cr-2017-1113>.

[4] Paolo Tasca, 'Digital Currencies: Principles, Trends, Opportunities, and Risk' (2015) ECUREX Research Working Paper 2015/7, 5 and 78-79 <https://ssrn.com/abstract=2657598> accessed 1 May 2018.

[5] cf Tasca (n 4) 14; see eg X, 'What is Ethereum?' <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html#a-next-generation-blockchain> accessed 1 May 2018; X, 'BitcoinCash' <https://www.bitcoincash.org/en/> accessed 1 May 2018.

[6] Franziska Boehm and Paulina Pesch, 'Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung: Eine erste juristische Einordung' [2014] MMR 75, 76; J Boersma, 'Cryptocurrencies: exploring a revolutionary technology' in R A Wolf, J Boersma, W A K Rank et al, *Bitcoins. Civiele en fiscale aspecten in beeld* (Kluwer 2015), 25; W A K Rank, 'Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten' in R A Wolf, J Boersma, W A K Rank et al, *Bitcoins. Civiele en fiscale aspecten in beeld* (Kluwer 2015), 27; T Spaas and M Van Roey, 'Quo vadis Bitcoin?' [2015] Computerrecht 113, 115 ch 2.5.1; Markus Kaulartz, 'Die Blockhain-Technologie: Hintergründe zur Distributed Ledger Technology und zu Blockchains' [2016] CR 474, 475; Tjong Ting Tai (n 1) 569-570 para 7; Albert Schlund and Hans Pongratz, 'Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung' [2018] DStR 598, 599.

[7] Satoshi Nakamoto (n 2) 2 ch 2.

[8] X, 'How does Bitcoin work?' <https://bitcoin.org/en/how-it-works> accessed 1 May 2018; Sue McLean and Simon Deane-Johns, 'Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero?' (2016) 4 CRi 97, 97 <https://doi.org/10.9785/cri-2016-0402>; Mark Giancaspro, 'Is a "smart contract" really a smart idea? Insights from a legal perspective' (2017) 33 CLSR 825, 826; Van der Elst and Lafarre (n 1) 171-172 ch 3; Schlund and Pongratz (n 6) 598.

[9] cf Spaas and Van Roey (n 6) 114 ch 2.2, 122, nr. 7; Schrey and Thalhofer (n 1) 1431.

[10] Satoshi Nakamoto (n 2) 3 ch 4; see Boersma (n 6) 22; Tasca (n 4) 12; Giancaspro (n 8) 826; Tjong Ting Tai (n 6) 569 paras 6-7.

[11] Merih Erdem Kütük and Christoph Sorge, 'Bitcoin im deutschen Vollstreckungsrecht: Von der „Tulpenmanie" zur „Bitcoinmanie"' [2014] MMR 643, 643; Spaas and Van Roey (n 6) 115 ch 2.5.2; María Nieves Pacheco Jiménez, 'Payment services evolution: from the European Directive of 2007 to the Digital Single Market and the European Directive of 2015′ [2016] EuCM 219, 219; Schrey and Thalhofer (n 1) 1432.

[12] Satoshi Nakamoto (n 2) 4 ch 6; Boehm and Pesch (n 6) 76; Kütük and Sorge (n 11) 643; Tasca (n 4) 11-12; Rank (n 6) 27; J Baukema, 'Virtuele valuta: (toezichtrechtelijke) stand van zaken' in R A Wolf, J Boersma, W A K Rank et al, *Bitcoins. Civiele en fiscale aspecten in beeld* (Kluwer 2015) 48 para 2; Spaas and Van Roey (n 6) 115 para 2.5.2; Tjong Ting Tai (n 6) 571-573 para 10; Van der Elst and Lafarre (n 1) 172 ch 3; Ekkenga (n 3) 763.

[13] Schrey and Thalhofer (n 1) 1432; H Schuringa, 'Enkele civielrechtelijke aspecten van blockchain' [2017] Computerrecht 372, 375.

[14] Kütük and Sorge (n 11) 643; Rank (n 6) 27-28; Kaulartz (n 6), 476; D De Jonghe and V I Laan, 'Blockchain in de realiteit' [2017] Computerrecht 347, 347; Jean-Luc Verhelst, 'Zijn cryptomunten munten? Een analyse van Bitcoin' in Matthias E Storme and Frederic Helsen (eds), *Innovatie en disruptie in het economisch recht* (Intersentia 2017) 44 paras 66-67; Schlund and Pongratz (n 6) 598-599.

[15] see inter alia Boehm and Pesch (n 6) 75-76; Kütük and Sorge (n 11) 643-644; A W Jongbloed, 'Bitcoins: virtueel geld, beslag op gebakken lucht?' [2015] Tijdschrift voor de Procespraktijk 77, 77-78; Rank (n 6) 27-28; Tasca (n 4) 10-14; Sean Greenwalt, 'Bitcoin: The Conflicting Currency' (2016) 4 LMU Law Review 80, 84-86; McLean and Deane-Johns (n 8) 97; Spaas and Van Roey (n 6) 113-116; Kaulartz (n 6), 474-477; Joost Linneman, 'Juridische aspecten van (toepassingen van) blockchain' [2016] Computerrecht 319, 319-323; Schrey and Thalhofer (n 1) 1431-33; Tjong Ting Tai (n 1) 568-573 paras 5-11; Verhelst (n 14) 25-60 paras 5-125; Schlund and Pongratz (n 6) 598-599.

Please cite this article as: S. Geiregat, Cryptocurrencies are (smart) contracts, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.05.030