Journal of Law and Judicial System
Volume 2, Issue 4, 2019, PP 26-31
ISSN 2637-5893 (Online)

Digital Technology and Payment System

Siniša Franjić*

Faculty of Law, International University of Brcko District, Brcko, Bosnia and Herzegovina

**Corresponding Author: Siniša Franjić, Faculty of Law, International University of Brcko District, Brcko, Bosnia and Herzegovina, Email: sinisa.franjic@gmail.com*

ABSTRACT

Cryptocurrencies are digital records of certain values stored in digital databases. Or, more simply, cryptocurrency is digital money, created in digital form as a means of digital exchange. They only exist on the internet and are not published by or controlled by the central bank or the state. Precisely because they are not controlled by the central bank, they are not formally money. Just as people have their money in a bank account, so do their cryptocurrencies in their "digital wallet" on one of the websites that provide this service. Each transaction that is made is a highly edited digital record, that is, a file consisting of the amount of cryptocurrency units transferred and certain public and secret keys of the "digital wallets" of the sender and recipient. Keys are passwords that are more complex than the ones we use everyday to get into online accounts, such as email or other applications. Each transaction is signed by the sender with a private key, and the transaction is then validated and recorded online. No one in the network can see the private key, but they can see that whoever really has the private key sent the transaction. The sender's signature ensures that no one can compromise the content of the transaction. That is why it is important to keep private keys offline.

Keywords: *Blockchain, Bitcoin, Currency*

INTRODUCTION

For the world of technology users, blockchain represents a dramatic improvement to the landscape of information collection, distribution, and governance [1]. That point has been espoused these past few years in the books and presentations that hype and imagine this new world. A blockchain is a database encompassing a physical chain of fixed-length blocks that include 1 to N transactions, where each transaction added to a new block is validated and then inserted into the block. When the block is completed, it is added to the end of the existing chain of blocks. Moreover, the only two operations-as opposed to the classic CRUD-are add transaction and view transaction.

More comprehensively, a blockchain is also a distributed database that maintains a doubly linked list of ordered blocks. Each block averages 1 megabyte and contains control data of approximately 200 bytes, such as a timestamp, a link to a previous block, some other fields, and 1 to N transactions as can fit in the remaining space.

Blockchains are secure by design and an example of a distributed computing system with high byzantine fault tolerance. Decentralized consensus can therefore be achieved with a public blockchain. These features make blockchains ideal for recording events, medical records and other records management activities, identity management, transaction processing, and a host of emerging applications. Moreover, blockchain technologies allow us to achieve large-scale and systematic cooperation in an entirely distributed and decentralized manner. This can be considered and implemented as a global governance tool, capable of managing social interactions on a large scale and dismissing traditional central authorities.

A public blockchain is not stored in one central computer. Nor is it managed by any central entity. Instead, it is distributed and maintained by multiple computers or nodes that compete to validate the newest block entries before the other nodes to gain a reward for doing so.

The block validation system is designed to be immutable. That is to say, all transactions old and new are preserved forever with no ability to delete. Anyone on the network can browse via a designated website and see the ledger. This provides a way for all participants to have an up-to-date ledger that reflects the most recent transactions or changes.

From a technical point of view, the blockchain is a distributed, transparent, immutable, validated, secured, and pseudo-anonymous database existing as multiple nodes such that if 51 percent of the nodes agree then trust of the chain is guaranteed. The blockchain is distributed because a complete copy lives on as many nodes as there are in the system. The blockchain is immutable because none of the transactions can be changed. The blockchain is validated (e.g., in the Bitcoin space) by the miners who are compensated for building the next secure block. The blockchain is pseudo-anonymous because the identity of those involved in the transaction is represented by an address key in the form of a random string.

Currency

Social transactional frameworks and market transactional frameworks have substantial and different setup costs [2]. Markets require the definition of property rights and contracting arrangements, legal enforcement systems, often physical exchange locations and information flow mechanisms, and so on. Social arrangements require norms to be developed, social networks formed, cultural values of cooperation inculcated, and so on. Assuming, however, that asociety has invested in both types of transactional frameworks, individual marginal transactions within each system also have a marginal cost. We have long understood that these marginal transaction costs can lead resources to be allocated through a managerial firm–based transactional framework rather than through a price-based transactional framework.

For goods that meet the focused definition of shareable goods, there are two discrete differences between the information characteristics of market transactions and social transactions, the first more important than the second. A market transaction, in order to be efficient by its own measures, must be clearly demarcated as to what it includes so that it can be priced efficiently. That price must then be paid in equally crisply delineated currency. Even if initially a transaction may be declared to involve sale of “anamount reasonably required to produce the required output,” for a price “ranging from x to y,” at some point what was provided and what is owed must be crystallized and fixed for a formal exchange. The crispness, or completeness of the information regarding all aspects of the transaction, is a functional requirement of the price system and derives from the precision and formality of the medium of exchange – currency – and the ambition to provide refined representations of the comparative value of marginal decisions through denomination in the exchange medium that represents these incremental value differences. Social exchange, on the other hand, does not require the same degree of crispness.

The empirical markers of this new economy are easy to identify [3]. From the 1970s onward there were pronounced increases in the depth of international economic integration, as registered particularly in trade and investment flows. During this period, trade as a proportion of total world economic activity grew steadily. Complementing this trend (and indeed, contributing to it) was an even more rapid increase in foreign direct investment (FDI) by multinational corporations. Moreover, the nature of FDI evolved in important ways. Historically, FDI was concentrated in extraction industries and public and private infrastructure projects; during the late twentieth century, however, FDI increasingly targeted the establishment of international ‘commodity chains’ that integrated production of simple and even complex products across national borders. Finally, during the 1990s there was an extraordinary increase in international portfolio investment – short-term investment in currencies, stocks, bonds and other liquid assets. The principal traders in these markets were large investment funds that by then had begun to consider the whole world as offering viable opportunities for lucrative financial activity.

Although technological advancement biased economic change toward greater international integration, its effects were amplified greatly by government strategies.During the last quarter of the twentieth century,leading states took dramatic steps to promote market-based international integration.On the trade front,operating initially through the General Agreement on Tariffs and Trade (GATT) and later through the WTO and regional and bilateral agreements, states substantially reduced tariff and non-tariff barriers to the international flow of goods and services.Regarding FDI,states enacted strong international protections for corporations – not least through new mechanisms in trade agreements that committed the signatories to protect real and intellectual property rights. Indeed, the investment provisions of ostensible trade agreements by the mid-1990s had come to be a much more important facilitator of deepening international economic integration than were their trade provisions. The North American Free

Trade Agreement (NAFTA) is the pivotal agreement in this respect: its investment provisions provide for the strongest protections for cross-border investors of any agreement in history.Finally,under guidance of (and substantial pressure by) the World Bank, the International Monetary Fund (IMF), the USA and other national governments during the 1980s and 1990s, states across the globe took steps to eliminate capital controls.These controls had been explicitly provided for in the IMF Articles of Agreement,and national governments had imposed controls consistently ever since World War II to protect against rapid inflows and outflows of hot money that could destabilize currencies, trade balances and macroeconomic performance. But over a 20-year period, capital controls fell by the wayside as countries sought to reposition themselves in emerging world financial markets. Why so many states took this rather drastic step (and with what consequences) was contested during the 1990s. But all agreed that the elimination of capital controls, like the reduction in tariffs and the extension of property rights for investors, was vital to the rapid deepening of integration at the close of the twentieth century.

Bit Coin

Digital currency advocates point to the rapid adoption of Bitcoin, now accepted by thousands of businesses including Virgin Galactic, Tesla, WordPress, and Overstock, as clear evidence of a changing tide [4]. Critics paint them as a speculative toy with little or no intrinsic value. To them, digital currencies are a tool used by cyber-criminals to launder money and avoid taxes. Lack of oversight and regulation—and the prevalence of fraud and hacking—make digital currencies volatile, opaque, and untrustworthy.

But digital currencies off er tremendous ease of use—no permanent address, bank account, or identification is needed. Simply owning a cell phone empowers billions of people living in poverty to take control of their limited finances and enter into transactions without a bank account or credit card.

Digital currencies have low to no transaction costs. As an example, Bitcoin has no enforced fees, unlike traditional payment systems such as credit cards, debit cards, and PayPal. This has caught the attention of financial companies, such as banks and credit card companies. They wonder if service fees will evaporate as quickly as long distance revenues did for the telcos when Skype appeared.

Yes, digital currencies involve risks. Lack of trust is at the heart of the risk to users of digital currencies and to the currencies' long-term viability. They can also be volatile.The current Internet is good for social collaboration and access to information. But it lacks many of the key capabilities needed for rich, trusted commerce. Imagine a new global platform where identity and trust are assured, where fraud is virtually impossible, and where appropriate payments are always made.

Bitcoin combines established primitives for managing ownership through public key cryptography with a consensus algorithm for keeping track of who owns coins, known as proof-of-work [1]. The mechanism behind proof-of-work simultaneously solves two problems. First, it provides an effective consensus algorithm, allowing nodes in the network to collectively agree on a set of updates to the state of the Bitcoin ledger. Second, it provides a mechanism for allowing free entry into the consensus process, solving the political problem of deciding who gets to influence the consensus, while simultaneously preventing Sybil attacks—that is, attacks where a reputation system is subverted by forging identities in peer-to-peer networks. It is named after a case study of a woman diagnosed with dissociative identity disorder. It works by substituting a formal barrier to participation, such as the requirement to be registered as a unique entity on a particular list, with an economic barrier—the weight of a single node in the consensus voting process is directly proportional to the computing power that the node brings. More recently, an alternative approach has been proposed called proofof-stake, calculating the weight of a node as being proportional to its currency holdings and not its computational resources.

Smart Contract

The qualities of a smart contract (control, transparency, and traceability) would allow for much more automation [1]. A smart contract would provide the customer and insurer with the ability to manage claims in an open, speedy, and indisputable way. The contract (policy) is uploaded to the blockchain and validated by the network. Similarly, claims are then uploaded to the blockchain and applied to the smart contract. That being said, blockchains cannot access data outside their network. This data can represent external conditions such as temperature, payment, price change, or RFID presence trigger. An oracle (or data provider) is a third-party service designed for use by smart contracts. An oracle provides the necessary external data and pushes it onto the blockchain. Then the contract and the network will be able to validate and enforce the claim and either automatically reject or accept it. When the correct conditions are met, a payment is automatically triggered.

PAYMENT

Trade finance refers to financial transactions, both domestic and international, that relate to trade receivables finance and global trade [1]. Trade finance is a core business function for all global banks, especially tier 1 banks. Given its importance, it still lags in its application of technology and still resorts to using very manual processes for its document-centric flows. This leads to interruption in business cycles, and the lack of transparency leaves the door open to financial crime. Supply chains between many parties are complicated, distributed, and lack trust, therefore they are very slow and need many third parties such as banks and clearinghouses to facilitate the trust aspect and allow the commerce supply chain to flow.

Blockchain will hold all of the necessary information in a smart contract, updated instantly and viewable by all members on the network. The smart contract can be used to automate the transfer of title to goods and money. This automation and network validation remove the need for third-party facilities, such as letters of credit (LCs), and will help to streamline the whole process and measurably reduce costs by eliminating the third parties and their associated fees.

It can take days to transfer money from a party in one country to a party in another country. The global payments business is a large, slow, costly, and error-prone industry. It is also attractive to those who wish to engage in money laundering because it is not completely traceable.

Blockchain payment technologies can add tremendous value in this space by (a) reducing the multi-day payment cycle down to real time, (b) enhancing currency conversions, and (c) providing transparency to improve anti–money laundering capabilities.

TECHNOLOGY

The devices interconnected by the Internet, essentially computers, process information digitally [5]. The network organizes communication between these machines on the basis of the "client–server" model. The "client" sends requests to the "server", which processes them and then sends a response. Any device connected to the Internet can be both a client and a server. This is notably the case for the most common applications on the Internet, e-mail and the Web. Sending an e-mail involves asking the server (recipient) whether he agrees to receive information. If he does, the client (sender) sends the information. In practice, e-mail servers carry out these operations. Unlike user terminals, the servers are permanently connected to facilitate data flows. Similarly, when consulting a website, the visitor sends a request to a computer in which information is stocked. The information server sends back HyperText Markup Language (HTML) codes to the client that enable the computer to re-build pages on the client's screen. Generally speaking, independently of the application being considered, requests and responses are broken down into data packets, which their senders and recipients identify and which circulate within the network where they are relayed by routers. After the packets are transmitted and received, the receiving terminal reconstitutes the original programming lines containing an informational content or instructions to the machine that pilots it from a distance.

LEGAL RULES

The legal industry will also be transformed and disrupted by blockchain technology and the associated scripting language and protocols known as smart contracts [1]. As we have seen, this technology is already affecting the banking, financial services, and payments industries. They implement blockchain to facilitate transactions, save on fees, and approach instantaneous clearing of transactions. The fintech movement, which has embraced blockchain, is always looking to disrupt traditional banking models and the software that supports it to deliver increased convenience, efficiency for service consumers, reduced risk, and of course lower cost of operations for financial services providers. For too long, lawyers have been slow to adopt new technologies. This is all changing; lawyers need to understand how to communicate securely and protect their client data. In particular, they need to understand blockchain and smart contracts. The New York County Law Association as well as many bar associations nationwide provides legal technology education so their members can avoid potentially being at odds with the new American Bar Association (ABA) rules.

Only recently, in response to demand and new standards, have lawyers started to use and rely on computing and communications tools. For example, e-discovery software is now a standard used to search email, documents, and other artifacts in the litigation discovery process. This process as well as other legal procedures would be facilitated with blockchain, which is an immutable and virtually infinite log. Blockchain when it is universally accepted will obviate most evidentiary issues. One question is how to treat blockchain data as evidence. In the U.S. judicial system, the standard for admissibility of evidence turns on whether a human has sworn under penalty of perjury that the information is true.

The creative effect of regulation is seen in the World Trade Organization (WTO) agreements of the mid-1990s [6]. The WTO is the central institution of the multilateral rules based legal order. New rules were created; old rules were recontextualised; and process becomes ordered and critical. By establishing a binding inter governmental dispute settlement mechanism, the WTO has ensured that the new rules will be binding and enforceable.

Despite advances in technology in the field of financing, including blockchain, the letter of credit remains a central payment mechanism in international business. It has always been axiomatic that fraud undoes everything. But the scope of this exception from liability is itself highly controversial. Does it apply only when the fraud was committed by the beneficiary? Can a bank be expected to pay when it knows that one of the documents is fraudulent? Even where there is strict compliance, there are issues of principle and practice. Surprisingly, the Uniform Customs and Practices for Documentary Credits (UCP), the universally accepted rules regulating letter of credit promulgated by the International Chamber of Commerce, has until now refused to address the issue of fraud.

After 50 years of intermittent debate, the United Nations Commission on International Trade Law (UNCITRAL) appears to have reached a transnational consensus on the Secured Transactions Law. It has reached this goal by using the mechanism of a model law containing single uniform provisions. It has not omitted those issues where no consensus was reached but has offered a choice of alternative approaches. Given the far-ranging consequences of these provisions on property rights, including those of third parties and of state instrumentalities and norms, this is a significant victory for consensus as a legal mechanism.

Cyber Space

Cyber space and e-commerce have become a driving force for the globalization of the world economy, and countries that do not engage in e-commerce may put the competitiveness of their economies at risk [7]. As a result, many firms and organizations in developing countries have become integral parts of global networks of production supply chains that increasingly use e-commerce mechanisms. Through these networks, entities in more developed countries induce developing-country enterprises to adopt new information technologies, organizational changes, and business practices.

The diffusion of cyber use in developing/ emerging economies is relatively low. The main stumbling blocks are associated with regulatory, cultural, and social factors, including (1) the lack of regulations dealing with data messages and recognition of electronic signature; (2) the absence of specific legislations protecting consumers, intellectual property, personal data, information systems, and networks; (3) the dearth of appropriate fiscal and customs legislation covering electronic transactions; and (4) the absence and/or inadequacy of laws dealing with cyber crimes.

Today's technological advances are faster (Moore's law) and more fundamental (break throughs in genetics). They are driving down costs (computing and communications) at a pace never before seen. Leading these transformations are the accelerated developments in ICT, biotechnology, and just- emerging nanotechnology. Information and communications technology involves innovations in microelectronics, computing (hardware and software), tele communications, and optoelectronics – micro processors, semiconductors, and fiber optics. These innovations enable the processing and storage of enormous amounts of information, along with rapid distribution of information through communication networks. Moore's law predicts the doubling of computing power every 18–24 months due to the rapid evolution of microprocessor technology. Gilder's law predicts the doubling of communications power every six months – a bandwidth explosion – due to advances in fiber optic network technologies.

Cyber Crime

There is no doubt that the technology utilized by a large number of businesses, including financial institutions, noticeably in developing and emerging countries, is becoming more and more varied, advanced, and innovative [7]. When measuring the gap between financial institutions that are technology centric and those that are not, one finds a notable difference.

The International Telecommunication Union (ITU) has identified five key factors to the success of a cyber security program at the national level; these are: (1) a national strategy; (2) collaboration between government and industry; (3) a sound legal foundation to deter cyber crime; (4) a national incident management capability; and (5) a national awareness of the importance of cyber security.

Attacks and unauthorized uses on businesses and institutions include malicious acts such as theft or destruction of intellectual property, abuse by insiders, and unauthorized access to information that results in a loss of data integrity and confidentiality, as well as malware threats such as viruses, spyware, worms, and Trojans. These cyber attacks affect the trust of cyber users and, as such, lead to apprehension about using the Internet as a means to conduct transactions.

Conclusion

The ledger or public ledger that records all such transactions and the value changes of cryptocurrency units is called blockchain. Each record is based on complex mathematical cryptography and is written in sequence, one block of codes after another, thus forming a chain of blocks. Therefore, it is not possible to change the data in the chain because it is usurping the state of the data blocks on it. Blockchain is not located in one place. Everyone who owns a unit of a cryptocurrency has their own copy of a blockchain book that syncs across all computers on the network. The blockchain system consists of computers connected to the network that confirm / verify certain transactions. To own a unit of some cryptocurrency is about like owning some amount of gold. Gold may have a higher or lower value, depending on the changing value of the market.

References

[1] Bambara, J. J.; Allen, P. R. (2018.): „ Blockchain - A Practical Guide to Developing Business, Law, and Technology Solutions“, McGraw-Hill Education, New York, USA, pp. 1. – 6.; 16.; 39. – 41.; 75.

[2] Benkler, Y. (2006.): „Peer Production of Survivable Critical Infrastructures“ in Grady, M. F.; Parisi, F. (eds): „The Law and Economics of Cybersecurity“, Cambridge University Press, Cambridge, UK, pp. 93. – 94.

[3] DeMartino, G. (2008.): „The ethical dimensions of the 'globalization thesis'debate“ in Davis, J. B.; Dolsma, W. (eds): „The Elgar Companion to Social Economics“, Edward Elgar Publishing Limited, Cheltenham, UK, pp. 59. – 60.

[4] Tapscott, D. (2015.): „The Digital Economy - 20th ANNIVERSARY EDITION - Rethinking Promise and Peril in the Age of Networked Intelligence“, McGraw-Hill Education, New York, USA, pp. 119.

[5] Brousseau, E.; Curien, N. (2007.): „Internet economics, digital economics“ in Brousseau, E.; Curien, N.(eds): „Internet and Digital Economics - Principles, Methods and Applications“, Cambridge University Press, Cambridge, UK, pp. 4.

[6] Kono, T.; Hiscock, M.; Reich, A. (eds) (2018.): „Transnational Commercial and Consumer Law - Current Trends in International Business Law“, Springer Nature Singapore Pte Ltd., Singapore, Singapore, pp. viii. – ix.

[7] Shalhoub, Z. K.; Al Qasimi, S. L. (2010.): „ Cyber Law And Cyber Security In Developing And Emerging Economies“, Edward Elgar Publishing Limited, Cheltenham, UK, pp. 11.; 30.

Citation: *Siniša Franjić, "Digital Technology and Payment System", Journal of Law and Judicial System, 2(4), 2019, pp. 26-31.*