Turkish Journal of Computer and Mathematics Education Vol.11 No 2 (2020), 584-587

Research Article

Regulatory Practices of Block Chain Finance in the Context of Embedded Supervision

Dr. R.M.Indi

Professor, Dr. D. Y. Patil Institute of Management & Entrepreneur Development
E-mail:rmin1962@gmail.com

Article History: Received: 13March2020; Accepted: 5August2020; Published online: 28August 2020

Abstract

Fin Tech (Financial Technology) and Block chain are highly discussed topics among technology leaders in finance today. This article describes the impact and revolution of Fin Tech and Block chain in the financial industry and demonstrates the main characteristics of such technology. However, the development of Block chain is still an ongoing process. Some challenges have arisen, such as scalability, security, privacy, latency, etc. It is important for financial markets to have a better understanding of the Block chain industry and find robust solutions. Therefore, this paper can demonstrate an overview of the Block chain and its development in the financial services and investigate challenges for adaptation of the technology.

Keywords: Block Chain, Fin-tech, Financial Industry, Financial Services, Investigate Challenges, Robust Solution.

1. Introduction

The primary mission of blockchains is to establish a creditworthy ecosystem among independent participants in a non-trustable distributed environment. A blockchain system is secure and autonomous based on its chained blocks, peer–peer nodes, consensus-based ledger mechanism, anonymous accounts, self-regulated data ownership, and programmable smart contracts. Furthermore, the devoted credit mechanisms are required to make blockchain systems to be creditworthy although blockchains provide a creditworthy infrastructure for data-level storage and operations.

The rapid growth in the adoption of blockchain technology and the development of blockchain-based applications has begun to revolutionize the finance and financial services industry. Beyond the highly publicized cryptocurrency bitcoin, common blockchain applications range from proprietary networks used to process financial transactions or insurance claims to platforms that can issue and trade equity shares and corporate bonds.While blockchain use cases and applications expanding inscope and number, regulators around the world, have expressed interest in regulating blockchain to protect consumers andthe market from fraud and other illegal conduct. As a result, organizations launching blockchain-based systems should prepare themselves to demonstrate that, their blockchain networks comply with applicable industry regulations and guidance to avoid a regulatory investigation.

This paper explores the emerging landscape for blockchaintechnology and virtual currencies, focusing on the regulatory issues and risks facing participants in this space. In particular, itdiscusses:

1. The basics of blockchain technology and its current commercial applications.
2. To understand the legal issues in the purview ofBlockchain Technology Regulatory Framework
3. To analyse how embedded supervision can build regulation into blockchain finance.

2. Basics of blockchain technology

In its simplest form, blockchain is a decentralised technology or distributed ledger on which transactions are anonymously recorded. This means the transaction ledger is maintained simultaneously across a network of unrelated computers or servers called “nodes”, like a spreadsheet that is duplicated thousands of times across a network of computers. The ledger contains a continuous and complete record (the chain) of all transactions performed which are grouped into blocks: a block is only added to the chain if the nodes, which are members in the blockchain network with high levels of computing power, reach consensus on the next ‘valid’ block to be added to the chain. A transaction can only be verified and form part of a candidate block if all the nodes on the network confirm that the transaction is valid. And in order to determine the validity of a candidate block, “miner” nodes compete to solve a highly complex algorithm to verify it (on the Bitcoin Blockchain this is known as the ‘Proof of Work’). The first node to solve the algorithm and validate the block should be rewarded – on the Bitcoin Blockchain this reward takes the form of Bitcoins and this is referred to as “mining for Bitcoins.”

A block generally contains four pieces of information: the ‘hash’ of the previous block, a summary of the included transaction, a time stamp, and the Proof of Work that went into creating the secure block. Once information is entered on the blockchain, it is extremely difficult to alter: a blockchain network lacks a

centralised point of vulnerability for hackers to exploit and each block includes the previous block's 'hash' so any attempts to alter any transaction with the blockchain are easily detectable.

In other words, blockchain is a self-maintaining database which typically has a "functionality wrapper", or app development platform, on top. Blockchain can be thought of as operating systems for which useful applications or "smart contracts" can be written. Assets and information about transactions can be stored and tracked without the involvement of a typical intermediary, such as a bank, or a central authority or some other trusted third party (McKinlay,Pithouse, McGonagle, Sanders, 2018).
There are two types of blockchain networks:

a. Permissioned blockchains: These networks are proprietary networks that specific individuals or entities use to conduct transactions (such as a group of banks processing financial transactions).
b. Permissionless or public blockchains: These are open source networks that anyone can access and use (such as bitcoin users who transact with each other using bitcoin for payment).

3. Legal Issues in Block chain Technology

Blockchain's key characteristics present challenges to the existing legal and regulatory framework. It is comprised of digitally recorded data in "blocks" that are linked together in chronological order in a manner that makes the data difficult to alter once recorded, without the alteration of all subsequent blocks and collusion of a majority of the network.(John Salmon and Gordon Myers,2019)

3.1 Jurisdiction

Blockchain has the ability to cross jurisdictional boundaries as the nodes on a blockchain can be located anywhere in the world. This can pose a number of complex jurisdictional issues which require careful consideration in relation to the relevant contractual relationships.

The principles of contract and title differ across jurisdictions and therefore identifying the appropriate governing law is essential. In a conventional banking transaction, for example, if the bank is at fault then irrespective of the transacting mechanism or location, the bank can be sued and the applicable jurisdiction will most likely be contractually governed. However, in a decentralised environment, it may be difficult to identify the appropriate set of rules to apply.

At its simplest level, every transaction could potentially fall under the jurisdiction of the location of each and every node in the network. Clearly, this could result in the blockchain needing to be compliant with an unwieldy number of legal and regulatory regimes. In the event a fraudulent or erroneous transaction is made, pinpointing its location within the blockchain could be challenging.

3.2 Data privacy

As one of the key USPs of the blockchain is that once data is stored it cannot be altered (at least, not easily), this clearly has implications for data privacy, particularly where the relevant data is personal data or metadata sufficient to reveal someone's personal details. Equally the unique transparency of transactions on the blockchain is not easily compatible with the privacy needs of the banking sector: the use of crypto-addresses for identity is problematic as no bank likes providing its competitors with precise information about its transactions and the banking secrecy must be kept by law.

In order to prevent this becoming a barrier to take-up, technology-based solutions will need to be found to design privacy-protecting blockchains. This might include limiting who can join the blockchain network to "trusted" nodes and encrypting the data on the blockchain, although this is not without its challenges, and it remains to be seen how vendors, particularly those targeting the financial services industry, tackle the balance of privacy versus transparency.

3.3 Risk of cyber-attack

Despite the high level of security that blockchain systems provide to the data recorded on them, there are some key cybersecurity risks that remain. The unique challenge to decentralized systems, particularly public

blockchains, is that data input can be from any number of nodes, meaning there is a risk of tampering at each node. The benefit of using a 'tamper proof' technology is negated if the information stored on the ledger is compromised to begin with. This type of attack is not aimed at the blockchain itself, but at external systems such as cryptocurrency wallets. There is a risk that individuals might target the data input point (rather than the ledger itself), leading to the dissemination of inaccurate information. Users operating on the blockchain would then unknowingly rely on misleading or false information. A 15-year-old boy from the United Kingdom proved this attack possible by developing a proof-of-concept code that allowed backdoor access into hardware wallets sold by Ledger.9 Using this approach, it would be possible to change wallet destinations and amounts of payments. An attacker could divert payments to his own account while making it appear to be the intended destination, ensuring the attack is undetectable to verifying nodes.

3.4 Double spending and DDoS attack

Double spending attacks occur when the same currency unit is assigned to multiple users, enabling them to use the same coin simultaneously. A distributed denial-of-service, or DDoS, attack is a type of cyber-attack in which a perpetrator attempts to render a service unavailable to its users by overwhelming its bandwidth, often by flooding it with traffic. Blockchain systems are less susceptible to these kinds of attacks than are traditional centralized systems, given the lower numbers of potential points of failure and ability to include denial of service prevention. However, where ledgers are concentrated on a few high-performing nodes, the likelihood of a successful DDoS attack is increased.

4. SmartContracts

Blockchain makes possible the use of so-called "smart contracts". Smart contracts are blockchain based contracts which are automatically executed upon certain specified criteria coded into the contract being met. Execution over the blockchain network eliminates the need for intermediary parties to confirm the transaction, leading to self-executing contractual provisions. In addition to the cost and efficiency gains it is hoped this will achieve, this also raises significant legal questions in relation to applicable regulation, leaving a sense of uncertainty as to the legal enforceability of smart contracts.

Since smart contracts are prewritten computer codes, their use may present enforceability questions if attempting to analyse them within the traditional 'contract' definition. This is particularly true where smart contracts are built on permissionlessblockchains, which do not allow for a central controlling authority. Since the point of such blockchains is to decentralize authority, they might not provision for an arbitrator to resolve any disputes that arise over a contract that is executed automatically. It remains unclear whether the elements of capacity, including the ability to rely on apparent or ostensible authority would apply and the questions of offer and acceptance, certainty and consideration would also need to be considered. However, there have been advances in many countries regarding the level of acceptability of electronic contracts so it is realistic to hope this is carried over to smart contracts. In the meantime, customers should ensure that smart contracts include a dispute resolution provision to reduce uncertainty and provide for a mechanism in the event of a dispute.

5. Embedded supervision

The spreadof distributed ledger technology (DLT) in finance could help toimprove the efficiency and quality of supervision. Embedded supervision, ie a regulatory framework that provides for compliance in tokenised markets to be automatically monitored by reading the market's ledger, thus reducing the need for firms to actively collect,verify and deliver data.

Embedded supervision is distinct from other forms of "suptech" or "regtech", which aim to use machine learning or artificial intelligence to more efficiently monitor the financial industry (FSB 2017, Broeders and Prenio2018).

The key principle of embedded supervision is to rely on the trust-creating mechanism of decentralised markets for regulatory purposes too. If DLT-based markets were to develop, this would change the way assets are traded and how they are packaged into complex financial products. Since the information contained in the blockchain is verified by decentralised economic consensus, it could replace current processes for data delivery and verification. In today's compliance process, the data's trustworthiness is guaranteed by the legal system, the relevant authorities and the threat of legal penalties. In DLT-based markets, by contrast, data credibility is assured by economic incentives. In this world, the supervisor must examine the conditions under which the market's economic consensus is strong enough to guarantee the quality of the data contained in the distributed

ledger. To implement embedded supervision, regulators would also be required to acquire substantial technological know-how and the willingness to adjust their operational approach to the technology that is being developed by the financial sector.

References:

1. John Mckinlay, Duncan Pithouse, John Mcgonagle, Jessica Sanders (2018)Blockchain: background, challenges and legal issues, DLA PIPER Publications.
2. John Salmon and Gordon Myers (2019), Blockchain and Associated Legal Issues for Emerging Markets, fresh ideas about Business in Emerging Markets, EM Compass,www.ifc.org/thoughtleadership
3. Gabriel Callsen (2019)WP811, Embedded supervision: how to build regulation into blockchain finance, FinTech inInternationalCapital Markets, international capital markets association
4. Broeders, D., &Prenio, J. (2018), Innovative Technology in Financial Supervision (Suptech)-the Experience of Early Users. Basel: Bank for International Settlements-Financial Stability Institute.
5. FSB (2017), Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention, https://www.fsb.org/wp-content/uploads/R270617.pdf