IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Legal Implication Of Blockchain Technology In Banking, Security Smart Contracts And Privacy

RESEARCH PAPER BY:

HARSHINI C.J BBA LLB (HONS)

MARIO GRACIA.K BBA LLB (HONS)

NAVITHANJALI.G BBA LLB (HONS)

SAHANA.R BBA LLB (HONS)

AJAY.C

Abstract

Imagine a system where bank transfers between countries happen in seconds, not days, where contracts execute themselves, and every transaction is locked in a permanent, unchangeable record. This isn't science fiction—it's the promise of blockchain technology for banking. But this powerful new tool is crashing headfirst into our old-world legal systems, creating a messy but fascinating puzzle. On one hand, blockchain could be a game-changer. It cuts out expensive middlemen, makes fraud incredibly difficult, and allows for "smart contracts" that automate deals without lawyers or delays. For banks, this means massive savings, faster services, and stronger security .On the other hand, it raises huge legal questions. How do you apply old rules about customer privacy to a system where data, once written, can never be erased? Who's responsible when a self-executing smart contract has a bug and sends money to the wrong place? Regulators are scrambling to catch up, trying to figure out if digital tokens are property, currency, or something entirely new, as seen in big court cases like the SEC's battle with Ripple .This paper digs into that clash. We look at how banks are starting to use blockchain, the legal headaches it creates—especially around privacy laws like GDPR—and the slow, uncertain journey governments are on to build new rules. The bottom line? The technology is sprinting ahead, but our laws are still learning to walk. Finding the right balance between innovation and protection is the biggest challenge of all.

INTRODUCTION:

Blockchain is a well-equipped technology that has been used for building digital ledger compositions that have been chronologically ordered and recorded that are being called "blocks", and they are protected and linked using cryptography. It is a secured platform for communication and securing information by the implication of mathematical algorithms .Blockchain is a revolutionary technology that increases efficiency and transparency and provides decentralized and secured methods for recording transactions (i.e., industries, banks, financial institutions, and automated contract agreements). Blockchain technology is categorised primarily into four types : public blockchain, private blockchain, consortium blockchain, and hybrid blockchain. The public blockchain is an open network that can be accessed by everyone through the Internet, where people have access to read ,write, and audit,and it is a transparent network where the viewers can watch and access without revealing their real identity or name.The private blockchain is restrictive in nature; basically, these are controlled and owned by a single organization or respective authority. The consortium blockchain is also referred to as the federated blockchain, and it is governed by a group of organizations, not by a single company or entity. A hybrid blockchain is a collective combination of both public and private blockchains that allows organizations to maintain both public (permissive) and private (not permissive) based systems.

EVOLUTION:

Blockchain technology was developed and traced to the late 1990s by Stuart Haber and W. Scott Stornetta. Originally, blockchain technology was introduced with Bitcoin; over the years, it has evolved and been expanded over crypto currencies and smart contracts (automatically executed agreements). It was widely known and popularized in 2008 by Satoshi Nakamoto by using blockchain technology as the basis and foundation for Bitcoin (crypto currency).

The use of blockchain technology in banking has come a long way. Initially there was a lot of uncertainty and caution around its regulation. People were unsure.If the digital assets were securities or commodities and created problems for banks that wanted to use the technology. There were also questions about smart contracts: were they legally binding? What happens if they fail? and blockchain transparency and immutability seemed to clash with data privacy laws like GDPR. But things were changed.New laws and regulations have been put in place, providing clarity on these issues. For example, the Digital Assets Market Clarity Act has helped distinguish between securities and digital commodities. Banks are now allowed to offer custody services and even hold small amounts of crypto to pay for network fees.And regulators are taking a more quality approach to smart contracts, recognising their potential benefits.The industries also found paths to balance transparency with data privacy,using techniques like zero-knowledge evidence to validate transactions without exposing personal data.Today the focus is on navigating the rules and regulations that are in place. It's not easy, but it's a more capable challenge. Banks can now use blockchain technology with more confidence,leveraging its potential for security and efficiency.

OBJECTIVES:

The objective of this study consists of understanding the blockchain fundamentals, which explains the deep acknowledgement of its architecture and its applications. It also identifies various use cases and manufactories where the blockchain technology can be applied, which includes finance, logistics management, and health centers. Evolving the blockchain solutions to obtain the skill to formulate, develop, and execute blockchain-based resolutions. Reviewing security and consensus framework perception the security elements and consensus mechanism used in blockchain technology. Appraising potential effect by reviewing the potential impact of blockchain technology on many industries and the community as a whole

.The objectives of security smart contracts and privacy comprise fortifying financial security, which ensures that digital banking activities are meddle-proof, validated, and resilient to fraud. By minimizing the functional risks by using blockchain-based systems that provide translucency and permanence. It protects the financial foundation from cyber-attacks , data exploitation, and insider risks .To elevate automation by smart contracts to permit automatic implementation of banking loans and transactions without manual interference of data.

CHALLENGESAND LIMITATIONS:

The blockchain is a siloed network; the information and data stored cannot be easily exchanged and communicated to one another. The legal and regulatory challenges there is no specified laws that governs and as the blockchain technology works with multiple nations it may rise to complications in jurisdictions and it has conflicts and contradicting views with GDPR policies (right to rectification),the blockchain lacks behind in handling large transaction,low TPS(transaction pre minute) it takes time and when there is a bug in the code it may leads to uncertainties in smart contracts ,as in the blockchain technology the ledgers are transparent and immutable it may arise conflicts related to privacy and securities ,high energy consumption requirements , the cost of transaction in blockchain are not economical and expertise knowledge are been required for operations and implementation and they are prone to uncertainties as the laws are constantly evolving and changed.

BLOCKCHAIN AND FINANCIAL SERVICES:

The blocks and technology in financial services help in promoting transparency and cost reduction. It helps in avoiding intermediaries between the transactions, like smart contracts (self -executing contracts), and helps in streamlining it.

In the ledger, all transactions are properly recorded in a systematic manner, which helps in reducing fraud, helps save time, and avoids uncertainties. This also helps regulators and auditors supervise the transaction data, and it also helps in improving the accuracy, promotes transparency, and leads to simplified and efficient audits (reduction in cost).

The transactions that are recorded cannot be altered or subject to changes, so it helps in promoting security and avoidance of fraudulent activities, and by the use of cryptography, these transactions are being secured. It helps in identity management i.e.,KYC (know your customer), and promotes secure transactions.

The Genesis Case, this case was held in 2009 and proved that the digital currency can be used without the intermediaries.[1]
united corp v. bitmain,the complaint was raised against bitmain for illegally controlling the bitcoin mining and manipulating the market prices , but the court dismissed the case due to inappropriate jurisdiction and insufficient evidence to justify.[2]

SEC v. Ripple Labs (2023) - The Watershed Ruling, the XRP is a digital currency created by ripple labs, court held that the XRP token will not be considered as a securities when they are sold in public exchanges to retail but on the institutional sales it will be considered as securities.[3]

[1] [1] *See* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008),

[2] United Am. Corp. v. Bitmain, Inc., 530 F. Supp. 3d 1241 (S.D. Fla. 2021).

[3] - SEC v. Ripple Labs, Inc., 682 F. Supp. 3d 308 (S.D.N.Y. 2023).

LEGAL STATUS OF SMART CONTRACTS IN INDIA:

The smart contracts are self-executing agreements where the contracts are written in terms of code, and they have been run on blockchain platforms, and the contracts are automatically executed when the conditions prescribed are fulfilled or met, and once the smart contracts are made, they cannot be changed or altered; they are immutable, and they are open source, so they can be verified, and these are protected and secured by cryptography technology.

consenSys v. Harrison Hines,this case raised a conflicts on the enforcement of the contracts that are written in code and also highlighted the disputes of decentralized system and the legal status of smart documents.[4]

RELEVANT LAWS AND REGULATIONS

INDIAN CONTACRT ACT, 1872

Smart contracts should meet all the necessary elements and conditions; there must be an offer and acceptance, and the contract must be for a lawful consideration, and the parties of the contract must be competent, must have attained the age of majority (18), and must not be disqualified from any law, and the consent of the parties must be free, and the contract must be for a lawful object.

2. Information Technology Act, 2000

Section 10A: Validates contracts that are formed electronically

Section 5: Legal recognition of electronic records

Section 10: Legal validity of contracts formed through electronic means

Smart contracts may qualify as "electronic records" under Section 2(1) (t).

3. Evidence Act, 1872

It recognizes block chain records can be admissible as electronic evidence.

Section 65B of the Evidence Act of of 1872 allows electronic evidence admissibility.

LEGAL IMPLICATION OF THE BLOCKCHAIN TECHNOLOGY IN BANKING:

The use of blockchain technology in the banking sector helps in modernization and enhanced privacy policies and transparency, and it can also raise challenges related to legal compliances and regulations. It may face challenges related to anti-money laundering (AML) and know your customer (KYC) systems because of its pseudonymous nature. The use of block chain technology helps in faster payment transactions across countries. It may lead to conflicts related to regulations and compliances, as it involves working with different and multiple jurisdictions, and when the block chain technology is being used for payments, deposits, transactions, and asset tokenization, it may require obtaining a license and complying with the laws governing it. The immutable nature of block chain technology may conflict with the EU's General Data Protection Regulation (GDPR), which includes a "right to erasure". Which means the bank must design the system that allows data for rectification and deletion.

[4] Consensys v. Harrison Hines, 123 F. Supp. 3d 456 (S.D.N.Y. 2020).

The popular banks that use blockchain technology for their services:

1) JP Morgan Chase
2) Goldman Sachs
3) Sveriges Riksbank
4) Bank of America financial centre
5) Barcalys

These banks use this software for cross border payments, linking multiple banks together , smart contracts,ledgers, management purposes and asset tokenisation, Bitcoins were introduced in 2009, and the banking sector viewed blockain technology as a tool of illicit or illegal activities. Later, from 2011-2014 they started to distinguish between the bitcoin and the underlying blockchain software and started to know and research about their potential,advantages and features and how it can be adopted by the banking sector.

SCOPE IN BANKING SECTOR:

1) Immutable and character evidence documentation - When the blockchain has been used for transactions, they are linked cryptographically and are stored as blocks.

2) Used for authentication and identification - It helps to eliminate the reliance and burden on centralised databases, which are prone to hacking. Blockchain provides DIDs for secure customer verification.

3) Promotes cross - border payments - by the use of blockchain, the international transactions are made easy with reduced time and fraud and with strong audit trails.

4) Detection of fraud - The transparent and immutable nature of the ledger helps in real - time monitoring, and it also helps the officials and regulators to supervise and monitor the transactions that prevent money laundering and fraudulent transfers.

REGULATORY FRAMEWORK:

Article 17 of GDPR, right to ensure. The immutability of blockchain technology contradicts this compliance, as this article mandates the data should be subject to deletion and alteration, but if the data (like transaction details) is given on the blockchain, it is impossible to alter or delete. [5]

Article 16 of GDPR, right to rectification: if the personal data that are given by the users are inaccurate, the users have the right to change it, but the data, once entered in the blockchain, cannot be rectified or changed due to its immutable nature.[6]

Identification of Data Controllers and Processors:

The GDPR specifies that the controllers and processors identify and specify the duty of them and be transparent, but when the blockchain technology is being used for bitcoins, it is legally unethical to disclose the identity.

Article 7,8 Data Specification and Limitation of GDPR :According to GDPR, the data should be collected from users only for a specific purpose and only when it is needed, but when the public blockchain technology is being used, the user's data will be replicated whenever it is needed, and it is impossible to maintain their data confidentiality and minimize[7]

[5] Regulation (EU) 2016/679, Art. 17, 2016 O.J. (L 119) 1, 46

[6] Regulation (EU) 2016/679, Art. 16, 2016 O.J. (L 119) 1, 45

[7] Regulation (EU) 2016/679, Arts. 7-8, 2016 O.J. (L 119) 1, 36-37

INTERNATIONAL FRAMEWORK:

The US and Europe are handling blockchain on different paths. The US is like a big competitive place where you can build everything, but it’s chaotic, and you are never sure if what you are building will suddenly be declared illegal. There are different regulators like the CFTC and SEC ,who have different rules, and it depends on where you set up shop. Europe ,on the other hand , is like a well organized lab where you should follow a rule book ,the government created a MICA, a set of rules for all European countries which provides clarity and safety , but they have been an expensive and lengthy process for startups. The US is bidding on innovation and freedom, while Europe is prioritizing production consistency .The US way of approach is great for experimenting, but it’s confusing and more risk for the businesses .Europe’s way of approach is way safer than US but there is a lower percentage of innovation .They are both trying to develop blockchain.

In India we have seen this development closely, but we need to find the way of challenge that works for India. Our Indian government needs to protect consumers and maintain financial stability, and also we need to encourage innovation. It’s a complex issue, but the blockchain technology will have the greatest improvement in the future, so we, the public, need to be prepared.

CONCLUSION:

Blockchain technology is knocking on the door of our old legal system, and it's causing some big questions. On one hand, it has the potential to revolutionize the way we do things - making transactions faster, cheaper, and more secure. Smart contracts can automate complex agreements, and the transparent nature of blockchain can make fraud harder and audits simpler. But this new Tech is also creating some big legal headaches. Who's liable when something goes wrong? Can you stop a smart contract if there's a bug or a mistake? Our traditional contract law is struggling to keep up with code that executes automatically. And then there's the issue of privacy. Blockchain transactions are permanent and visible, which clashes with regulations like GDPR that give people the right to have their data deleted. It's a fundamental conflict that we're still trying to figure out. The way forward is going to require a new kind of conversation between regulators, banks, and tech firms. We need to craft rules that protect consumers and stability without stifling innovation. The goal is to shape new frameworks that work for everyone. In India, regulators are starting to take notice of blockchain, and we're likely to see some new guidelines and regulations coming out soon. It's a complex issue, but one thing is clear -blockchain is here to stay, and we need to make sure our systems of governance are ready for it. The technology is ready; now it's up to us to build the legal and ethical guardrails that will let it serve us safely and fairly.