INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 4 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 4 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-4-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

BLOCKCHAIN

AUTHOR - KHUSHI BHATT* & DR. MAYURA SABNE**

* STUDENT AT UNITEDWORLD SCHOOL OF LAW, KARNAVATI UNIVERSITY

** ASSISTANT PROFESSOR OF LAW, UNITEDWORLD SCHOOL OF LAW, KARNAVATI UNIVERSITY

BEST CITATION - KHUSHI BHATT & DR. MAYURA SABNE, BLOCKCHAIN, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (4) OF 2025, PG. 1143-1155, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

This research paper investigates the transformative impact of blockchain technology and cryptocurrencies on the financial landscape, particularly in India. It explores the evolution of blockchain, its security features, and the regulatory challenges posed by the rapid growth of cryptocurrencies. By analyzing existing literature, expert insights, and market trends, the study aims to provide a comprehensive understanding of the implications of blockchain and cryptocurrencies for various sectors, including banking and finance.

Keywords: Blockchain Technology, Cryptocurrencies, Digital Currency, Smart Contracts, Tokenization.

INTRODUCTION

Blockchain technology has emerged as a revolutionary force in the digital economy, fundamentally altering transaction processes. This paper examines the implications of blockchain and cryptocurrencies, focusing on their potential benefits, risks, and the evolving regulatory landscape in India.

What are the transformative impacts of blockchain technology and cryptocurrencies on the financial landscape in India, and what regulatory challenges do they pose for various sectors, including banking and finance? This study will employ a mixed-methods approach culminating in a synthesis of findings to inform regulatory recommendations

1.1 BLOCKCHAIN

Considered as a collection of linked blocks joined by an alphabetic code repeated as the first part of one "block" and the last part of another, a blockchain is A blockchain is a time-stamped, any-type information record. The data on the blockchain is safeguarded in several linked methods, including the cryptographic security of every record and the linking and distribution of all records.[1811]

Every record is first cryptologically protected using a one-way hash function. A hash function is a mathematical technique turning any input into a fixed-length output.

From any bit of data, a hash function creates a distinct fixed-length string of characters known as a hash. Although the SHA-algorithm is a widely used hash method, as technology develops new and better algorithms could surface.36 Unlike other hash systems, cryptographic ones are practically difficult to reverse but efficient in one direction. Therefore, even if creating a hash from a piece of data is rather simple, a computer has great difficulty extracting the actual data from the hash. This is a far wider difference than, example, solving a Rubik's Cube from scrambling it.

These hashes are linked together and subsequently hashed once again to create a

[1811] Amy Whitaer, 'Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts ' (Project Muse Artivate, Volume 8, Issue 2, Summer 2019, pp. 21-46) file:///C:/Users/fgh/Downloads/project_muse_811867.pdf accessed on 6 March 2023 summary hash for every block or collection of transactions. Work's contents are also hidden as typically just the hash not the actual work is available on the blockchain. "One especially valuable feature of digital time-stamping is that it allows one to show highest value of intellectual property without revealing its contents," In their paper, write Haber and Stornetta.

The design of the system has the largest safety net. Sean Moss-Pultz, the founder of Bitmark, underlines: "Blockchain security is a dynamic, emergent quality that arises from the competition to find the next block. Without this dynamic component, what is presented is a list (chain of blocks) that must call for a trusted authority to create the next block."[1812]

The development of the bitcoin cryptocurrency changed the compensation and motivation of the operators of the computer nodes verifying the blocks. This incentive not only generated money but also effectively built a crowdsourced block verification process. Computers acting as Bitcoin system nodes are always solving mathematical problems to verify every block.

More precisely, the computers struggle with one another to find the "nonce," a problem solved by brutal trial-and-error processing power mixed with chance.[1813] The first computer to find the nonce validates block and gets paid Bitcoin. The award's value halves on regular intervals throughout time.[1814]

These systems are insecure even though they have connected blocks and cryptographic processes. The emergence of "quantum computing," or more sophisticated types of computing, begs issues on how different levels of computing can affect blockchain governance. Though it is unclear that computer capability would rise that dramatically, if one bad actor has enough processing capability and no one else does, the bad actor may find others' secret keys and approve transactions. Observers of blockchain technology sometimes refer to the scenario whereby most of the nodes of a blockchain are compromised as "percent Attack".

Furthermore, mining is decentralised in line with the blockchain's design because it is theoretically carried out by numerous dispersed players. But, in actuality, mining is geographically and organisationally centralised. In order to benefit from the highest processing power available, mining uses specialised servers and chips. Because of economies of scale, running several mining machines is more cost-effective than installing just one. The use of a larger number of servers also has the benefit.

Supplementary factors in blockchain design include whether a company runs on Bitcoin, Ethereum, or another protocol as well as whether the blockchain is public or private or permissioned. Currently running several blockchain-based art companies use Bitcoin, Ethereum, private, permissioned blockchains, and public blockchains. Many blockchain startups in the creative sectors handle issues with accessibility, technological knowledge, and privacy. Their objectives entwine more general concerns of diversity, inclusion, and equity with those particular to the arts, law, and technological sectors like blockchain and artificial intelligence.

1.2 IS BLOCKCHAIN SECURE?

By linear and chronological storage of fresh blocks, the blockchain technology offers distributed security and trust. Once added, they join the end of the blockchain. Once a block gets on the blockchain, changing its contents is quite difficult unless most of the network agrees. This is so because every block contains a unique timestamp and hash in addition to the hash of the one before it. A mathematical procedure transforms digital data into a string of numbers and letters, hence producing hash codes. Should the data be altered, the hash code changes as well. The blockchain's integrity

[1812] 3 Moss-Pultz, personal communication, October 2019.
[1813] Nonces depend on random-number generation, itself a source of idiosyncratic risk in the blockchain ecosystem. See, for example, Bonneau, Clark, and Goldfelter, 2015.
[1814] Supra at 35

is therefore maintained, hence it is practically tamper-proof.[1815]

Imagine the situation whereby a hacker controlling a blockchain node also wants to modify the blockchain and pilfers everyone else's cryptocurrency. If one edited their own copy, the copies made by others would not line up. Since everyone will see that one copy sticks out when compared to the others, the hacker's rendition of the chain will be seen as fake.

To make their new copy the majority copy and, therefore, the agreed-upon chain, the hacker would have to simultaneously control and alter at least 51% of the blockchain copies.

Given their great scale and explosive expansion, many bitcoin networks make it quite improbable that a 51% attack could be successful given their exorbitant cost. Any such assault would also be rapidly discovered by network participants who would migrate to a stable form of the chain, therefore rendering the attack worthless. Actually, trying such an attack would not be financially possible since it would demand for a lot of computational capability and financial means. Moreover, should the assailant target a particular token version of the blockchain, the value of that asset would finally drop, therefore making the attack useless. This is exactly the reason taking part in the network is significantly more financially rewarded than fighting it. Should an assailant target the most recent fork of Bitcoin, the same result would follow. These networks' distributed character essentially offers a great degree of security, so it is challenging for any one entity to control or damage the integrity of the network.[1816]

1.3 BLOCKCHAIN VS. BITCOIN

Researchers Stuart Haber and W. Scott Stornetta first put forward blockchain ideas in 1991 as a means of implementing a system whereby document timestamps could not be changed. But blockchain had its first useful application only once Bitcoin was launched in 2009.[1817]

Introduced as "a new electronic cash system, fully peer-to-peer, with no trusted third party," Bitcoin's technology is built on a blockchain.[1818] under the alias Satoshi Nakamoto, its pseudoneer Although blockchain technology is used in Bitcoin, blockchain is not unique to that cryptocurrency. Without central authority, blockchain is a distributed ledger system offering a transparent and unchangeable method of storing and verifying data. Beyond only cryptocurrencies, it finds several possible applications in supply chain management, voting systems, and digital identity validation. Fundamentally, though, the blockchain forms the basis of Bitcoin's distributed payment system. In theory, though, blockchain allows any quantity of data points to be absolutely recorded. As was already established, this could show up as transactions, election votes, inventory of commodities, state identifications, acts towards assets, and much more.

1.4 THE USE OF BLOCKCHAIN IN BANKING & FINANCE

1.4.1 International Payments

International payments and money transfers are best suited for blockchain technology since it offers a quick and safe method to produce a tamper-proof record of delicate operations. Bank Santander revealed in April 2018 the first blockchain-based money transfer service available worldwide, "Santander One Pay FX." Customers may utilise Ripple's xCurrent to transmit money abroad on the same day or the next day with this service. By automating the whole process on the blockchain, Santander has cut the number of middlemen needed in these exchanges and raised effectiveness. Foreign transactions especially benefit from this since consumers may get less costly and faster payments. Blockchain technology can reduce international payment costs by removing banks'

[1815] Adam Hayes, 'Learn how these digital public ledgers enable crypto and NFTs' (Investopedia 27 September 2022) https://www.investopedia.com/terms/b/blockchain.asp accessed on 7 March 2023

[1816] Id at 40

[1817] Coinbase. "What Is Bitcoin?" accessed on 6 March 2023

[1818] Bitcoin. "Bitcoin: A Peer-to-Peer Electronic Cash System," Page 1 requirement for human processing. Having many retail customers, Santander can use the blockchain to provide a more quick and affordable money transfer tool while maintaining transaction integrity and security.

1.4.2 Capital Markets

Furthermore, capable of improving finance markets are blockchain-based technology. A McKinsey analysis highlights advantages blockchain technology provide capital markets, some of which relate to[1819]:

- Faster clearing and settlement
- Consolidated audit trail

1.4.3 Trade Finance

Because of the drawn-out procedures that often create company interruptions and complicate managing liquidity, traditional trade financing solutions have been a key cause of misery for companies. Transporting information about the country of origin and product specifications calls for a lot of documentation and many variables in cross-border trade.

Blockchain could help to simplify cross-border trade finance operations. Thanks to this, companies can engage more freely across national and regional barriers.[1820]

1.4.4 Regulatory Compliance and Audit

Blockchain's very strong security features will be much appreciated in accounting and auditing since they significantly reduce the likelihood of human mistake and guarantee record accuracy. Furthermore, once the account records have been encrypted using blockchain technology, none—not even the record owners are authorised to change them. The drawback is that blockchain technology may someday replace the demand for auditors and result in job losses.

1.4.5 Money Laundering Protection

Likewise, the blockchain's natural use of encryption helps much in the fight against money laundering. The technology supporting record-keeping makes the "Know Your Customer" (KYC) process which helps a company to acknowledge and authenticate the identification of its customers possible.

1.4.6 Insurance

For the insurance sector, smart contracts are a vital blockchain tool since they provide a safe and open approach for handling claims between consumers and providers. By use of the blockchain, all contracts and claims can be tracked and verified by the network, thereby avoiding several claims for the same accident and so lowering false claims.

For example, on the IBM Blockchain Platform the American Association of Insurance Services and IBM created the openIDL network, which speeds compliance procedures and automates regulatory reporting for the insurance sector.

1.4.7 Peer-to-Peer Transactions

Though they are useful, P2P payment systems including Venmo have certain limitations. The location of the user determines some services' transaction restrictions. For their usage, some seek money in return. Many of them, meanwhile, are easily hacked, which discourages consumers from providing their crucial financial data. Thanks to all the above mentioned advantages, blockchain technology has the power to remove these obstacles.

1.5 BLOCKCHAIN APPLICATIONS IN BUSINESS

1.5.1 Supply Chain Management

Because of its unchangeable ledger, blockchain is ideally suitable for jobs like real-time tracking of commodities as they pass hands across the supply chain. Using a blockchain increases the choices available to companies who provide these goods. Blockchain entries allow supply chain events such as distributing freshly produced goods to several shipping containers to be queued up. Blockchain offers a fresh and

[1819] 'The growing list of applications and use cases of blockchain technology in business and life'(Insider Intelligence) https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/ accessed on 5 March 2023

[1820] Insider Intelligence 24 January 2022) https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/ accessed on 6 March 2023 creative approach to data organisation and use.

1.5.2 Healthcare

Prescription drugs are being tracked and traced in supply networks using blockchain technology, therefore preventing the sale of counterfeit drugs, regulating their distribution, and enabling recall of potentially harmful drugs. Customer data security, data interchange, and distribution are top priorities in the healthcare sector for enhancing across governments, hospitals, and research labs services.[1821]

1.5.3 Real Estate

By means of transparent and secure recording of transactions, blockchain technology can streamline real estate transfers. This lessens documentation, saves time, and streamlines the deed and title transfer process to new owners.[1822]

1.5.4 Media

Blockchain technology is being sought by media companies in order to guard intellectual property rights, lower expenses, and fight fraud. MarketWatch projects that by 2024 the worldwide blockchain media and entertainment business will have grown to $1.54 billion. One platform that has attracted notice for its media blockchain application is Eluvio, Inc. Launched in 2019, Eluvio Content Fabric leverages blockchain to let content creators handle and distribute premium video to partners and customers without depending on content delivery systems. For dissemination of content, this provides a more affordable and safe answer. Blockchain technology is predicted to become more common in the future as the media sector continues to expand.

1.5.5 Energy

Blockchain technology finds various possible uses in the energy sector according to PWC. Apart from doing energy supply transactions, it can also offer a platform for metering, billing, and clearing procedures. Blockchain technology can ensure provenance, track assets, record ownership, distribute emission permits, and generate renewable energy certificates.[1823]

1.6 BLOCKCHAIN APPLICATIONS IN GOVERNMENT

1.6.1 Record Management

Governments at the federal, state, and local levels have personal records on file including dates of birth and death, marital status, and property transfers regarding residents. Managing this data can be challenging, hence some of these entries remain on file. Blockchain technology solves the difficulty and annoyance of physically visiting local government offices for updates by streamlining recordkeeping processes and raising data security.

1.6.2 Voting

Personal identifiable data on a blockchain allows one to use this technology for voting, therefore preventing fraud and guaranteeing that nobody can vote more than once. Making voting more easily available and convenient that is, via a smartphone app may help boost voter turnout and lower the overall election expenses.[1824]

1.6.3 Taxes

With enough information stored on the blockchain, blockchain software may make the tiresome tax filing process which is prone to human error far more efficient.[1825]

1.6.4 Nonprofit Organizations

Blockchain technology can help organizations fight the anti-trust issues they are progressively confronting by proving funders that NPOs are indeed using their money as intended. By

[1821] PavanVadapalli, 'Top 10 Blockchain Applications in 2023' https://www.upgrad.com/blog/top-blockchain-applications/ accessed on 5 March 2023

[1822] Adam Levy, '15 Applications for Blockchain Technology' (The Motley Fool 13 July 2022) <https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain- applications/>

[1823] Supra at 45

[1824] Supra at 47

[1825] Supra at 45

means of blockchain technology, these NPOs may also be able to improve their tracking skills, manage their resources, and migrate their assets.

1.7 VARIOUS APPLICATIONS OF BLOCKKCHAIN

1.7.1 Cybersecurity

Eliminating the risk of a single point of failure gives blockchain technology a great benefit in cybersecurity. Blockchain also provides anonymity and end-to-end encryption, therefore improving security in several uses.

1.7.2 Artist royalties

Blockchain technology can be used to track music and movie files shared online, which can help to ensure that artists are fairly compensated for their work and reduce content piracy. Its capability to prevent the same content from being duplicated in more than one location makes it ideal for this purpose. Furthermore, blockchain can track playbacks on streaming platforms, and a smart contract can be used to distribute royalties transparently, ensuring that artists receive their rightful compensation.

1.7.3 Secure Internet of Things networks

Blockchain technologies can improve Internet of Things (IoT) security, therefore simplifying our lives but potentially exposing us to cyber dangers. Blockchain can offer better security by keeping sensitive data on a distributed network instead than one server. Furthermore, the blockchain's tamper-proof character provides defence against data tampering. This guarantees a safer and more secure IoT environment by stopping malevolent actors from gaining access to our data and controlling important infrastructure.[1826]

1.8 BITCOIN, CRIME, AND TERRORISM

Since it would be more difficult for law enforcement authorities and counterterrorist experts to monitor bitcoin holdings, criminal and terrorist organisations may be intrigued in cryptocurrencies.[1827] Early on, criminals have started using Bitcoin as a kind of anonymous payment method. For instance, on the notorious dark web site Silk Road, which Ross Ulbricht created in July 2010, Bitcoin was the accepted form of payment for purchasing illegal narcotics.[1828] Between 2010 and 2012, Silk Road handled sales valued 9.5 million Bitcoin from 12 million in circulation.[1829] Bitcoin has been used by hackers in ransomware campaigns like WannaCry, in which case a software like CryptoLocker encrypts all data on hacked systems. Then the hackers provide the encryption key in return for a designated Bitcoin value.[1830] Not surprisingly, academic studies and government investigations on the risks of BT have mostly addressed criminal and terrorist applications of money laundering and cryptocurrencies. But Bitcoin by itself is not officially anonymous but pseudonymous: Everybody on the public ledger may see the sending and receiving wallet addresses used in bitcoin transactions.[1831] Any transaction connected to a specific cryptocurrency wallet a hardware or software program storing private keys can be followed and the owner may be exposed with specialised techniques of analysis and computer forensics.[1832]

Still, Bitcoin gives terrorists, criminals, and dissidents a few benefits. Unless a user keeps the cryptocurrency in a cryptocurrency exchange account under government jurisdiction, a government cannot prohibit transactions or freeze cryptoassets as would be the case with traditional bank transfers and bank accounts. Second, just memorising a private key that provides access to funds on the blockchain allows a person to store theoretically unlimited value in his memory. This makes it difficult for governments to implement capital

[1826] Supra at 35

[1827] Christopher Whyte, "Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise," Studies in Conflict and Terrorism (2019): 2, https://doi.org/10.1080/1057610X.2018.1531565.

[1828] Nathaniel Popper, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money (New York: Harper, 2015), 69-73.

[1829] Werbach, The Blockchain, 49.

[1830] Popper, Digital Gold, 347.

[1831] Whyte, "Cryptoterrorism," 4.

[1832] Werbach, The Blockchain, 179

restrictions on or seize cryptocurrencies even if they can arrest a person or take other tangible assets.[1833] Third, by accepting bitcoin donations from anywhere in the globe and from anyone, a resistance group can quickly raise money without depending on third parties, such front organisations and credit card companies or PayPal. Their public bitcoin addresses should be published on a website. For instance, the Islamic State apparently sought donations by displaying a Bitcoin address.[1834]

Notwithstanding these benefits, many drawbacks have caused terrorist organisations to delay down their acceptance of cryptocurrencies. The main issues are the significant volatility of crypto-assets, which generates organisational uncertainty; the diminished capacity of terror leaders to exercise control over money handed to agents; and the difficulty of turning crypto-assets back into fiat currency.[1835] Thus, a recent RAND research revealed that "there is little evidence that terrorist organisations are using cryptocurrencies in any form."extensive or systematic way."[1836] Privacy coins including DASH, ZCASH, and Monero which have achieved significant innovations including anonymisation through coin-mixing, the encryption of transaction values, and a "zero knowledge-proofs" protocol whereby transactions may be confirmed without disclosing the address of the sender or recipient on the blockchain—may be turned to by future criminals and terrorists.[1837]

1.9 WHAT EXACTLY IS FINANCIAL TECHNOLOGY?

"Financial technology" is a broad term for the several technologies applied in the financial industry. From credit cards to early mobile phone payment systems to more recent peer-to--peer or bank-to--bank payment systems, exchanges, and settlement techniques, it can cover several decades of development in digital payment technology. For example, developers of financial technologies include seasoned stalwarts like SWIFT as well as startups looking at blockchain-based settlement methods and novel transmitters.[1838]

Financial technology also refers to decades of developments made to boost flexibility and efficiency while cutting costs in a variety of operations, including trading, investing, insurance, and compliance. More lately, distributed ledger technology-based digital currencies have seen speculative expansion. Despite the initial bubble burst in 2018, digital currencies still had a market value of more than $175 billion as of early May 2019, indicating that they are probably here to remain a feature of the financial scene.[1839]

Though distributed ledger technology forms the basis for digital currencies, it is also a major new technology in and of itself. Apart from supply chain management and contracts pertaining to monitoring illegal actors, including sanctions evaders, it serves the foundation for numerous creative financial technologies purposes. It can give a community of users an auditable, distributed, unchangeable record of interactions. Some innovative technologies, not especially designed for use in the financial sector, could be applied to provide financial services or otherwise be pertinent to financial operations, including the use of fines and their efficiency. They include artificial intelligence (AI) and machine learning to identify trends in enormous volumes of data. These technologies enable governments and institutions to monitor evolving methods for illicit financial operations.[1840]

[1833] Whyte, "Cryptoterrorism," 14

[1834] Joshua Baron, Angela O'Mahoney, David Manheim, and Cynthia Dion-Schwarz, National Security Implications of Virtual Currencies: Examining the Potential for NonState Actor Deployment (Santa Monica, CA: RAND, 2015), 19-20.

[1835] Whyte, "Cryptoterrorism," 14

[1836] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats (Santa Monica, CA: RAND, 2019), 21.

[1837] Michael C. Casey, and Paul Vigna, The Truth Machine: The Blockchain and the Future of Everything
(New York: St. Martin's Press, 2018), 33.

[1838] Supra at 35

[1839] "Top 100 Cryptocurrencies by Market Capitalization," Coinmarketcap.com, Updated May 5, 2019, https://coinmarketcap.com/.

[1840] Supra at 35

1.10 PRIVATE KEY

A private key in the field of cryptography is an alphabetic code acting as a password. In the field of cryptocurrencies, it is absolutely important since it certifies ownership of a blockchain asset and permits transactions. A private key is crucial for protecting consumers against theft and illegal access to their money since of its encryption features.[1841]

A collection of digital keys and addresses used to manage cryptocurrencies symbolises the ownership and control of virtual tokens. Any public speech is welcome for bitcoin or another token donations. But the recipient must have the specific private key to access any stored cryptocurrency.

Private keys come in a lot of variants. A private key in base- Ten notation would be hundreds of digits long; brute forcely breaking such a key would take a quite lengthy time. Usually presented as an alphabetic string for simplicity of use, private keys.[1842]

1.10.1 Private Keys and Digital Wallets

Users do not need to manually establish or remember their key pairs, even though private keys are a necessary component of cryptocurrencies. Instead, digital wallets generate and store key pairs automatically. After a transaction is started, the wallet software processes the transaction using the private key to produce a digital signature.

Using a private key guarantees that once a transaction is broadcast it cannot be changed. Should the transaction data be even slightly altered, the signature will be erroneous since the algorithm generates the same key from the same data.

Losing their private key renders a user unable to access the wallet for expenditure, withdrawal, or transfer of money. As so, the private key has to be maintained in a safe place. One can save private keys in several methods. Called paper wallets, they can be written on or typed on. Some people print QR codes on paper using software that generates them so they may be rapidly scanned upon a transaction needing signatures.

Two main storage systems exist, each with two separate wallet systems. Custodial wallets are ones in which your keys are kept on your behalf by another person, say an exchange. Noncustodial wallets are those wallets used for key storage. Both groups have hot (internet connection) wallets and cold (no internet connection) wallets.

An example of a custodial cold wallet is the location Coinbase keeps its key files at. Want to use your keys? Move them from cold storage to your Coinbase hot wallet. One non-custodial cold wallet example is the Ledger Nano X. You link it to a non-custodial hot wallet device using the software wallet of your choosing.

1.11 PUBLIC KEY

You can get bitcoin transactions if you have a public key. This key consists of a private key and a cryptographic code, which lets just the bitcoin owner validate and prove they are the ones who made the transaction. Though anyone can transmit transactions using the public key, the owner is the one able to "unlock" and access them. Usually utilised as the receiving address for transactions, the public key's address is a shorter form of itself.

You can so freely distribute your public key. You might know online contribution pages for content providers or charitable organisations including public keys to their crypto addresses. Though anyone can donate, only the owner of the private key can unlock and access the money.[1843]

[1841] Jake Frankfield, 'Private Key: What It Is, How It Works, Best Ways to Store' (Investopedia 17 Febuary 2023) https://www.investopedia.com/terms/p/private-key.asp accessed on 6 March 2023**F**

[1842] O'Reilly. "Mastering Bitcoin | Chapter 4."

[1843] What Are Public and Private Keys?' (Cryptopedia 28 June 2022) https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-public-and-private-keys- control-your-crypto accessed on 9 March 2022

1.11.1 Public and Private Keys Control Your Crypto

Understanding how public and private keys interact helps one to understand how bitcoin transactions are conducted. When you say you have bitcoins, you are really claiming to be in possession of a private key acting as ownership documentation. As your public key is kept on the blockchain, anyone may verify you are the owner. Your philosophy and degree of risk tolerance will all help determine whether you choose to "hold your own keys" or trust a custodian. If you handle your own private keys, think about utilising one of the several great contemporary HD wallets; always keep them to yourself though. If you decide for a custodial solution like an exchange, be sure you select a reputable, well-known company that gives security and regulation top importance.

1.12 COLORED COINS

1.12.1 Origin of the Colored Coin

Tokens called coloured coins let any asset show up on the Bitcoin network. This invention arose as a means of addressing the requirement to relocate assets and generate fresh Bitcoin network tokens. These tokens might stand for anything from equities, goods, real estate, fiat money, and even other cryptocurrencies.

Inspired by MasterCoin, the CEO of eToro, the idea of coloured currencies started to take hold in venues like Bitcointalk and Yoni Hesse announced the concept on his own blog in March 2012. This inspired Meni Rosenfeld to produce a whitepaper on December 4, 2012, on coloured coins. Though imperfect, this was the first official work on coloured coins that attracted the community.[1844]

Flavien Charlon created the Coloured Coin Protocol in 2013, enabling the creation of coloured currencies by transaction input and output modification. This was the first truly practical Bitcoin protocol for coloured coins. But ChromaWay, the firm creating the EPOBC system, started not until July 3, 2014. One of the first to apply Bitcoin Script's new OP RETURN capability, this protocol greatly streamlined the process of creating coloured coins for developers drawn in by such technology.

Coloured coins' inventiveness kept developing, and in 2015 they were unearthed and growingly important in the context of Bitcoin. This all existed before Ethereum made its first formal public release. The introduction of coloured currencies paved the path for the tokenisation of assets, so creating fresh chances for companies and people to represent and trade their assets in a distributed and safe way.

Ultimately, coloured coins became a solution for the requirement to relocate assets and generate fresh Bitcoin network tokens. The introduction of coloured coins has let any asset to be shown on the Bitcoin network, thereby tokenising assets and generating fresh chances for companies and people to show and trade their assets in a distributed and safe way. The invention of coloured coins helped the token economywhich is still developing and growing today to take shape.

1.12.2 The reason behind the creation of colored coins?

Coloured coins basically help to open the path for the development of extra Bitcoin features. Being able to create coins connected to real-world items and backed by a blockchain network is a rare chance. Building a currency, a tokenised bond, or even integrate third-party software with Bitcoin to send microtransactions or operations tracked and secured by the blockchain is not usual.

Furthermore, coloured coins and the opportunities they presented were only the start of other, more advanced technologies, such the second layer protocols we now employ, RSK or BISQ. Simply expressed, the inventiveness of the community created new paths for research and stretched the possibilities of Bitcoin.

Using Bitcoin, for example, one may create a coloured money with a unit value equivalent to

[1844] What is a Colored Coin? (Bit2me) https://academy.bit2me.com/en/que-es-una-colored-coin/ accessed on 4 March 2023 one dollar or euro. Indeed, this is what we nowadays refer to as stable coin. 2014 saw a brand-new idea with a lot of possible uses, and Bitcoin let us look at them all. Of course, it was not the only object that could be depicted; at the time, your creativity was the only limit.

1.12.3 How coloured coins function?

A coloured coin is a cryptocurrency whereby the asset issuer commits to provide the coin owner a good or service. The asset issuer encrypts part of their own bitcoin with metadata using a specialist cryptocurrency wallet with coin colouring capability.

The metadata specify the obligations of the asset issuer to coin holders. For instance, a musician might give the opportunity to see a concert at a specific time and venue using coloured coins. Then anyone can come with one of the coloured coins.

Once coloured coins are produced, the issuer can move them via blockchain-based transactions on the bitcoin. Like any other transaction on the blockchain, these ones provide the same degree of security and irreversibility.[1845]

1.12.4 Expansion of Colored Coins through Blockchain

Blockchain coloured coins allow distributed of objects other than money from anyone. While first concentrated on Bitcoin, other blockchain have now embraced the concept with NFT coins. The most often used example is Ethereum. Coloured Ethereum tokens might be gaming tokens or actual assets like real estate ownership documentation.

Holding those coins gives the owner of the object clear proof of possession. NFT aficioners can see how non- fungible tokens were derived from coloured currencies.[1846]

1.12.5 What is the future of colored coins?

The concept of coloured coins made trading Bitcoins for other currencies possible. But proof of stake used by blockchains like Ethereum—has replaced Bitcoin's original proof of work method for transaction handling.

This trend causes coloured currencies to fall; generally, this is due to slower movement of Bitcoin transactions. NFTs have hence taken front stage on blockchains like Ethereum. Still, the NFT explosion might not have happened if coloured currencies hadn't existed. Still, colourful coins have a lot of benefits.

Advantages

- You may tokenize a variety of assets;
- They are supported by the Bitcoin network, which is the most popular and secure blockchain;
- The use of decentralised exchanges can be expanded by the creation of an infinite number of coins that don't need their own network or specialised gear.

Disadvantages

- very difficult to design and implement;
- high risk.

1.12.6 Colored coins and NFTs

The concept of coloured coins helped non-fungible tokens (NFTs) to evolve. Though it can be complex and delicate, there are some basic concepts that can help provide some foundation on the conversation between coloured coins and NFT. The 2013 paper by Yoni and Buterin addresses the first emergence of the concept of including non-fungible assets to a blockchain. Coloured coins are based on the theory that overlaying an overlay (open asset) on a blockchain can generate a subset of unchangeable tokens.

An update of this concept are NFTs. Reacting to the 2013 whitepaper, Robert Dermody, Adam

[1845] Lyle Daly, 'What are Colored Coins? '(The Motley Fool @4 January 2022) < https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/colored-coins/> accessed on 5 March 2023

[1846] What are colored coins and how do they work? (Etoro) https://www.'etoro.com/crypto/what-are-colored-coins/ accessed on 6 March 2023

Krellenstein, and Evan Wagner founded Counterparty in 2014. This distributed exchange let users design, send, and receive custom coloured tokens. By 2016, Counterparty was exchanging coloured coin-based digital trading cards. Later, this behaviour produced memes like Rare Pepes.

With the release of the CryptoPunks in 2017, NFTs' popularity peaked and it was maybe at this point that the Ethereum tokens started to outshine those on the Bitcoin blockchain. Designed by Larva Laboratories, these 10,000 digital characters were totally unique and regarded by many as the first modern NFTs. Since their theoretical foundation matched those of coloured coins, they were non-fungible assets on the Ethereum network. They fell into a particular kind of ERC-20 token.

1.13 SMART PROPERTY

Different coloured coins can let one employ smart property. Assia's theory holds that a rental company might offer cars varying coloured coins. Each coin could only be activated with a distinct private key; this key might be sent to the renter's smartphone in a message. The key would unlock the car by transmitting a signal from the phone, so the only person renting the car may be able to use it.

- Shares, contracts, and bonds of the company

A business may issue shares in the form of coloured coins. Not only would this enable trading, but it would also provide unquestionable ownership confirmation.

- Demand deposits

One may imagine deposits as NFT cryptocurrency coins. While monitoring their deposits, people could trade Litecoins tokens or coloured Bitcoin coins.[1847]

- Emergent currencies

Different coloured coins could start to be a fresh kind of currency. Though it exists on the Bitcoin blockchain, the coin differs from BTC in value and features.

1.14 SMART CONTRACTS

Smart contracts are self-executing systems designed to automatically carry out contract or agreement conditions' fulfilment. They enable distributed and anonymous parties to participate in trusted transactions and agreements since they run without centralised authority or outside enforcement mechanism. Executed by a network of computers when predefined conditions are met and verified, smart contracts use code created on a blockchain to follow basic "if/then…" statements. Once the requirements have been satisfied, activities are automatically carried out such as registering a car or distributing money and the blockchain is changed to show the fulfilment of the contract. Though most people know blockchain technology from Bitcoin, it has developed to enable many different uses outside of digital currencies.[1848]

1.14.1 Working of Smart Contracts

Designed to be tamper-proof, smart contracts let just authorised users observe the outcomes. They comprise a collection of guidelines or requirements that have to be satisfied if the contract is to run as intended. Participants must first agree on the "if/when…then" statements controlling the transactions, take into account any possible exceptions, and create a structure for handling conflicts. Furthermore agreed upon by all members is the way the blockchain presents data and transactions.[1849]

Although a developer can create a smart contract, many companies today use templates, web interfaces, and other online tools to streamline the process. Among businesses using blockchain technology for their operations, this method is growingly popular. Smart contracts guarantee that the

[1847] Id at 71

[1848] Supra at 66

[1849] 'What are smart contracts on blockchain? ' (IBM) <https://www.ibm.com/in-en/topics/smart-contracts> accessed on 6 March 2023 transaction will be finished properly and cannot be changed once they are signed on by parties.

1.14.2 Smart Contract Uses

From simple transactions between two people, such the purchase and delivery of commodities, to more complicated situations, smart contracts find many uses. Smart contracts, for instance, might let a company control supplier raw material supplies and payments. Depending on the agreement's terms, the supplier could get automatic payment either upon delivery or shipment.

Apart from these, smart contracts find use in real estate transactions, stock and commodity trading, loans, corporate governance, supply chains, conflict resolution, and healthcare. Without middlemen or third-party confirmation, they provide a flexible and effective means of guaranteeing the safe and automatic execution of contracts and methods of party enforcement. Smart contracts are growing in popularity among many different sectors since they could simplify company processes and cut expenses.

1.14.3 Applications Of Smart Contracts

Safeguarding the efficacy of medications

By increasing supply chain openness, Sonoco and IBM expect to reduce issues with the delivery of life-saving drugs. Designed with a blockchain, Pharma Portal tracks drugs across the supply chain that need to be kept at a specific temperature to provide reliable, accurate data to many different partners. Its driving force is IBM Blockchain Open Supply.[1850]

Increasing trust in retailer-supplier relationships

The Home Depot quickly settles supplier conflicts using blockchain smart contracts. Increased supply chain visibility and real-time communication are enabling them to strengthen their ties to vendors, therefore freeing more time for vital work and innovation.

Making international trade faster and more efficient

Joining we.trade, the trade finance network set up by IBM Blockchain, companies are creating a trust-based ecosystem for global trade. We trade, a blockchain-based trading platform combines standard regulations with condensed trading alternatives to lower friction and risk, simplify the trading process, and increase trade prospects for participating businesses and banks.

1.15 IMPLEMENTATION OF SMART CONTRACTS IN RELATION TO VOTING AND BLOCKCHAIN

Blockchain technology applied in the voting process can efficiently solve the shared issues with a centralised voting system, including voter bias, identity fraud, and miscounts. Smart contracts, with their specified terms and conditions, guarantee that no voter may use a digital identity other than their own to cast a ballot, therefore assuring that the contract reflects their own. Every vote is registered on a blockchain network and the computation procedure is perfect; results are automatically computed without third party or manual intervention. With network users themselves verifying legitimacy, the voting process can take place on a public blockchain or a distributed autonomous organization-based blockchain configuration. With the ledger accessible for public audit and validation, this guarantees that every vote is noted on it and cannot be changed.[1851]

Smart contract voting systems can also be made to let members be added or removed, voting methods be changed, debating intervals be adjusted, or the majority rule be changed. inside a distributed autonomous company, for instance, a vote for a decision can be generated and the voting system inside the company can decide if the plan is authorised or

[1850] Supra at 74

[1851] What is a Smart Contract in Blockchain and How Does it Work? (Simpli Learn 10 Febuary 2023) <https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-smart-contract> accessed on 6 March 2023 rejected instead of depending just on one central authority.

1.16 SMART CONTRACT IMPLEMENTATION ON THE BLOCKCHAIN AND CROWDFUNDING

Smart contracts based on Ethereum technology can facilitate the creation of digital currency for use in transactions. With the ability to build and issue your own digital currency, transferable computerized tokens can be generated using a standard coin API. Ethereum provides standardizations such as ERC 2.0, enabling the contract to automatically access any wallet for exchange. This allows for the production of a transferable token with a pre-defined supply. Essentially, the platform functions as a central bank and issues digital money.

CONCLUSION

In conclusion, blockchain technology and cryptocurrencies represent a significant shift in the financial landscape, offering both opportunities and challenges. The decentralized nature of blockchain provides enhanced security, transparency, and efficiency in transactions, which can revolutionize various sectors, including banking, finance, supply chain management, and government operations. However, the rapid growth of cryptocurrencies also raises regulatory concerns, particularly regarding security, fraud, and the potential for misuse in illegal activities.

As blockchain technology continues to mature, its applications will likely expand beyond cryptocurrencies, influencing various industries and reshaping the way we conduct transactions and manage data. The journey towards widespread adoption will require collaboration among stakeholders, including governments, financial institutions, and technology providers, to harness the full potential of this transformative technology.