#ESERPTrabajandoDesdeCasa
#ESERPLiveStreaming

Blockchain
N. 4

Avv. Maria Bruccoleri
www. avvocatobruccoleri.it
Linkedin: https://www.linkedin.com/in/maria-bruccoleri-648440135/

ESERP Business & Law School
C/ Costa Rica 9. 28016 Madrid
www.eserp.com

Piazza A. Diaz, 6
Milano, 20123
Cell 328 8871062
E-mail: studiolegalebruccoleri@gmail.com

Studio Legale
Avv. Maria Bruccoleri

Via Gioacchino di Marzo 5
Palermo, 90144
Tel. 091 309131
Tel/Fax 091 308038
PEC: avvmariabruccoleri@legamail.it

BLOCKCHAIN: LEGAL IMPLICATIONS, QUESTIONS, OPPORTUNITIES AND RISKS

www.avvocatobruccoleri.it

Blockchain is increasingly in the news, but still primarily as the underlying software used for cryptocurrencies such as Bitcoin. Many businesses have yet to realize its potential and the extensive ways in which blockchain can be used to make processes more efficient or to develop new service offerings, but momentum is gathering as its applications are more widely understood.

Decentralized technologies such as blockchain are expected to be the next big wave, comparable in many people's eyes to the transformation that followed the development of the Internet, so a basic understanding blockchain is essential.

However, users need to be very clear about the legal implications, risks and opportunities that blockchain presents, as well as its relative immaturity and current technological limitations, including capacity.

PRIVACY AND BLOCKCHAIN

A blockchain is a shared database that records transactions between two parties in an immutable ledger. Blockchains document and confirm pseudonymous ownership of all existing coins within a cryptocurrency ecosystem at any given time through cryptography.

PRIVACY AND BLOCKCHAIN

After a transaction is validated and cryptographically verified by other participants or nodes in the network, it is made into a "block" on the blockchain. A block contains information about the time the transaction occurred, previous transactions, and details about the transaction.

PRIVACY AND BLOCKCHAIN

Once recorded as a block, transactions are ordered chronologically and cannot be altered. This technology rose to popularity after the creation of Bitcoin, the first application of blockchain technology, which has since catalyzed other cryptocurrencies and applications.

PRIVACY AND BLOCKCHAIN

Due to its nature of decentralization, transactions and data are not verified and owned by one single entity as they are in typical systems. Rather, the validity of transactions are confirmed by any node or computer that has access to the network.

PRIVACY AND BLOCKCHAIN

Blockchain technology secures and authenticates transactions and data through cryptography.

With the rise and widespread adoption of technology, data breaches have become frequent.

PRIVACY AND BLOCKCHAIN

User information and data are often stored, mishandled, and misused, causing a threat to personal privacy.

Currently, many are pushing for the widespread adoption of blockchain technology for its ability to increase user privacy, data protection, and data ownership.

BLOCKCHAIN AND PRIVACY PROTECTION
PRIVATE AND PUBLIC KEYS

A key aspect of privacy in blockchains is the use of private and public keys. Blockchain systems use asymmetric cryptography to secure transactions between users. In these systems, each user has a public and private key. These keys are random strings of numbers and are cryptographically related.

BLOCKCHAIN AND PRIVACY PROTECTION
PRIVATE AND PUBLIC KEYS

It is mathematically impossible for a user to guess another user's private key from their public key.

This provides an increase in security and protects from hackers.

Public keys can be shared with other users in the network because they give away no personal data.

Each user has an address that is derived from the public key using a hash function.

BLOCKCHAIN AND PRIVACY PROTECTION
PRIVATE AND PUBLIC KEYS

These addresses are used to send and receive assets on the blockchain, such as cryptocurrency.

Because blockchain networks are shared to all participants, users can view past transactions and activity that has occurred on the blockchain

BLOCKCHAIN AND PRIVACY PROTECTION PRIVATE AND PUBLIC KEYS

Senders and receivers of past transactions are represented and signified by their addresses; users' identities are not revealed.

Public addresses do not reveal personal information or identification; rather, they act as pseudonymous identities.

It is suggested that users do not use a public address more than once; this tactic avoids the possibility of a malicious user tracing a particular address' past transactions in an attempt to reveal information. Private keys are used to protect user identity and security through digital signatures

BLOCKCHAIN AND PRIVACY PROTECTION
PRIVATE AND PUBLIC KEYS

Private keys are used to access funds and personal wallets on the blockchain; they add a layer of identity authentication.

When individuals wish to send money to other users, they must provide a digital signature that is produced when provided with the private key.

This process protects against theft of funds.

PEER-TO-PEER NETWORK

Blockchain technology arose from the creation of Bitcoin.

In 2008, Satoshi Nakamoto released a paper describing the technology behind blockchains.

In his paper, he explained a decentralized network that was characterized by peer-to-peer transactions involving cryptocurrencies or electronic money.

In typical transactions carried out today, users put trust into central authorities to hold their data securely and execute transactions

PEER-TO-PEER NETWORK

In large corporations, a large amount of users' personal data is stored on single devices, posing a security risk if an authority's system is hacked, lost, or mishandled.

Blockchain technology aims to remove this reliance on a central authority.

PEER-TO-PEER NETWORK

To achieve this, blockchain functions in a way where nodes or devices in a blockchain network can confirm the validity of a transaction rather than a third party.

In this system, transactions between users such as sending and receiving cryptocurrency) are broadcast to every node in the network.

PEER-TO-PEER NETWORK

Before the transaction is recorded as a block on the blockchain, nodes must ensure a transaction is valid.

Nodes must check past transactions of the spender to ensure he/she did not double spend or spend more funds than they own.

PEER-TO-PEER NETWORK

After nodes confirm a block is valid, consensus protocols such as proof of work and proof of stake are deployed by miners.

These protocols allow nodes to reach a state of agreement on the order and number of transactions.

Once a transaction is verified, it is published on the blockchain as a block.

PEER-TO-PEER NETWORK

Once a block is created it cannot be altered.

Through blockchain's decentralized nature and elimination of the need for a central authority, user privacy is increased.

Peer-to-peer networks allow users to control their data, decreasing the threat of third parties to sell, store, or manipulate personal information

ZERO-KNOWLEDGE PROOFS

A Zero-knowledge proof is a Consensus decision-making protocol that one party proves to another party that information is true.

The "prover" does not reveal any information about the transaction.

This can be done through complex cryptographic methods.

This method, which has been recently

introduced into blockchain systems using zk-snarks, has been enacted to increase privacy in blockchains.

ZERO-KNOWLEDGE PROOFS

In typical public blockchain systems, a block contains information about a transaction such as the sender and receivers addresses and the amount sent.

Many users are not comfortable with this sense of transparency.

To maintain the blockchain's nature of decentralization while decreasing transparency, zero-knowledge proofs reveal nothing about a transaction, except that it is valid.

COMPARISON OF BLOCKCHAIN PRIVACY SYSTEMS

Private blockchains (or permissioned blockchains) are different from public blockchains, which are available to any node that wishes to download the network. Critics of public blockchains say because everyone can download a blockchain and access the history of transactions, there is not much privacy. In private blockchains, nodes must be granted access to participate, view transactions, and deploy consensus protocols. Because transactions listed on a private blockchain are private, they ensure an extra layer of privacy.

COMPARISON OF BLOCKCHAIN PRIVACY SYSTEMS

Because private blockchains have restricted access and nodes must be specifically selected to view and participate in a network, some argue that private blockchains grant more privacy to users. While private blockchains are considered the most realistic way to adopt blockchain technology into business to maintain a high level of privacy, there are disadvantages.

For example, private blockchains delegate specific actors to verify blocks and transactions. Although some argue that this provides efficiency and security, concerns that in nature, private blockchains are not truly decentralized because the verification of transactions and control are put back into the hands of a central entity, have arisen

HYBRID BLOCKCHAINS

Hybrid blockchains allow more flexibility to determine which data remain private and which data can be shared publicly.

A hybrid approach is compliant with GDPR and allows entities to store data on clouds of their choices to be in compliance with local laws to protect peoples privacy. A hybrid blockchain contains characteristics of private and public blockchains. Not every hybrid blockchain contains the same characteristics. Bitcoin and Ethereum do not share the same characteristics, although they are both public blockchains.

USE CASES FOR PRIVACY PROTECTION

After Satoshi Nakamoto spurred the creation of blockchain technology through Bitcoin, cryptocurrencies rose in popularity. Cryptocurrencies are digital assets that can be used as an alternative form of payment to fiat. In current financial systems, there exists many privacy concerns and threats.

USE CASES FOR PRIVACY PROTECTION

Centralization is an obstacle in typical data-storage systems. Currently, when individuals deposit money, a third party intermediary is necessary. When sending money to another user, individuals must trust that a third party will complete this task. Blockchain decreases the need for this trust in a central authority.

USE CASES FOR PRIVACY PROTECTION

Cryptographic functions allow individuals to send money to other users. Because of Bitcoin's widespread recognition and sense of anonymity, criminals have taken advantage of this by purchasing illegal items using Bitcoin. Through the use of cryptocurrencies and its pseudonymous keys that signify transactions, illegal purchases are difficult to trace to an individual. Due to the potential and security of blockchains, many banks are adopting business models that use this technology

HEALTH CARE RECORDS

In recent years, more than 100 million health care records have been breached. In attempts to combat this issue, solutions often result in the inaccessibility of health records. Health providers regularly send data to other providers. This often results in mishandling of data, losing records, or passing on inaccurate and old data.

HEALTH CARE RECORDS

In some cases, only one copy of an updated health record exists; this can result in the loss of information. Health records often contain personal information such as names, social security numbers and home addresses. Overall, it is argued by some that the current system of transferring health information compromises patient privacy to make records easy to transfer

HEALTH CARE RECORDS

As blockchain technology expanded and developed in recent years, many have pressed to shift health record storage onto the blockchain. Rather than having both physical and electronic copies of records, blockchains could allow the shift to electronic health records (EHR).

HEALTH CARE RECORDS

Medical records on the blockchain would be in the control of the patient rather than a third party, through the patients' private and public keys. Patients could then control access to their health records, making transferring information less cumbersome. Because blockchain ledgers are immutable, health information could not be deleted or tampered with. Blockchain transactions would be accompanied by a timestamp, allowing those with access to have updated information

LEGAL

The notarization of legal documents protects the privacy of individuals. Currently, documents must be verified through a third party or a notary. Notarization fees can be high. Transferring documents takes time and can lead to lost or mishandled information. Many are pressing for the adoption of blockchain technology for the storage legal documents.

LEGAL

Documents cannot be tampered with and can be easily accessed by those who are granted permission to access them. Information is protected from theft and mishandling. Another possible use of blockchain technology is the execution of legal contracts using smart contracts, in which nodes automatically execute terms of a contract. By using smart contracts, people will no longer rely on a third party to manage contracts, allowing an increase in privacy of personal information.

LEGALITY OF BLOCKCHAIN AND PRIVACY

With the recent adoption of the General Data Protection Regulation in the European Union, questions regarding blockchain's compliance with the act have arisen. GDPR applies to those who process data in the EU and those who process data outside the EU for people inside the EU.

LEGALITY OF BLOCKCHAIN AND PRIVACY

Personal data is "any information relating to an identified or identifiable natural person". Because identities on a blockchain are associated with an individual's public and private keys, this may fall under the category of personal data because public and private keys enable pseudonymity and are not necessarily connected to an identity. A key part of the GDPR lies in a citizen's right to be forgotten, or data erasure.

LEGALITY OF BLOCKCHAIN AND PRIVACY

The GDPR allows individuals to request that data associated with them to be erased if it is no longer relevant. Due to the blockchain's nature of immutability, potential complications if an individual who made transactions on the blockchain requests their data to be deleted exist. Once a block is verified on the blockchain, it is impossible to delete it.

IRS

Because cryptocurrency prices fluctuate, many treat the purchase of cryptocurrencies as an investment. By purchasing these coins, buyers hope to later sell them at a higher price. Internal Revenue Service (IRS) are currently facing struggles because many people do not include revenue from cryptocurrencies in their income reports. In response to these concerns, IRS issued a notice that people must apply general tax principles to cryptocurrency and treat the purchase of it as an investment or stock.

IRS

IRS has enacted that if people fail to report their income from cryptocurrency, they could be subject to civil penalties and fines.

In attempts to enforce these rules and avoid potential tax fraud, IRS has called on Coinbase to report users who have sent or received more than $US20,000 worth of cryptocurrency in a year.

IRS

The nature of blockchain technology makes enforcement difficult. Because blockchains are decentralized, entities cannot keep track of purchases and activity of a user.

Pseudonymous addresses make it difficult to link identities with users, being a perfect outlet for people to launder money.

BLOCKCHAIN ALLIANCE

Because virtual currencies and the blockchain's protection of identity has proved to be a hub for criminal purchases and activity, FBI and Justice Department created Blockchain Alliance.

This team aims to identify and enforce legal restrictions on the blockchain to combat criminal activities through open dialogue on a private-public forum. This allows law enforcers to fight the illegal exploitation of the technology.

Examples of criminal activity on the blockchain include hacking cryptocurrency wallets and stealing funds. Because user identities are not tied to public addresses, it is difficult to locate and identify criminals

FAIR INFORMATION PRACTICES

Blockchain has been acknowledged as a way to solve fair information practices, a set of principles relating to privacy practices and concerns for users.

Blockchain transactions allow users to control their data through private and public keys, allowing them to own it. Third-party intermediaries are not allowed to misuse and obtain data.

If personal data are stored on the blockchain, owners of such data can control when and how a third party can access it. In blockchains, ledgers automatically include an audit trail that ensures transactions are accurate.

TRANSPARENCY

Although many advocate for the adoption of blockchain technology because it allows users to control their own data and exclude third parties, some believe certain characteristics of this technology infringe on user privacy. Because blockchains are decentralized and allow any node to access transactions, events and actions of users are transparent. Sceptics worry malicious users can trace public keys and addresses to specific users. If this was the case, a user's transaction history would be accessible to anyone, resulting in what some consider to be a lack of privacy.

DECENTRALIZATION

Due to blockchain's decentralized nature, a central authority is not checking for malicious users and attacks.

Users might be able to hack the system anonymously and escape.

Because public blockchains are not controlled by a third party, a false transaction enacted by a hacker who has a user's private key cannot be stopped.

Because blockchain ledgers are shared and immutable, it is impossible to reverse a malicious transaction

PRIVATE KEYS

Private keys provide a way to prove ownership and control of cryptocurrency.

If one has access to another's private key, one can access and spend these funds.

Because private keys are crucial to accessing and protecting assets on the blockchain, users must store them safely.

PRIVATE KEYS

Storing the private key on a computer, flashdrive or telephone can pose potential security risks if the device is stolen or hacked.

If such a device is lost, the user no longer have access to the cryptocurrency.[1] Storing it on physical media, such as a piece of paper, also leaves the private key vulnerable to loss, theft or damage.

Piazza A. Diaz, 6
Milano, 20123
Cell 328 8871062
E-mail: studiolegalebruccoleri@gmail.com

Studio Legale
Avv. Maria Bruccoleri

Via Gioacchino di Marzo 5
Palermo, 90144
Tel. 091 309131
Tel/Fax 091 308038
PEC: avvmariabruccoleri@legamail.it

Thanks for your attention

www.avvocatobruccoleri.it