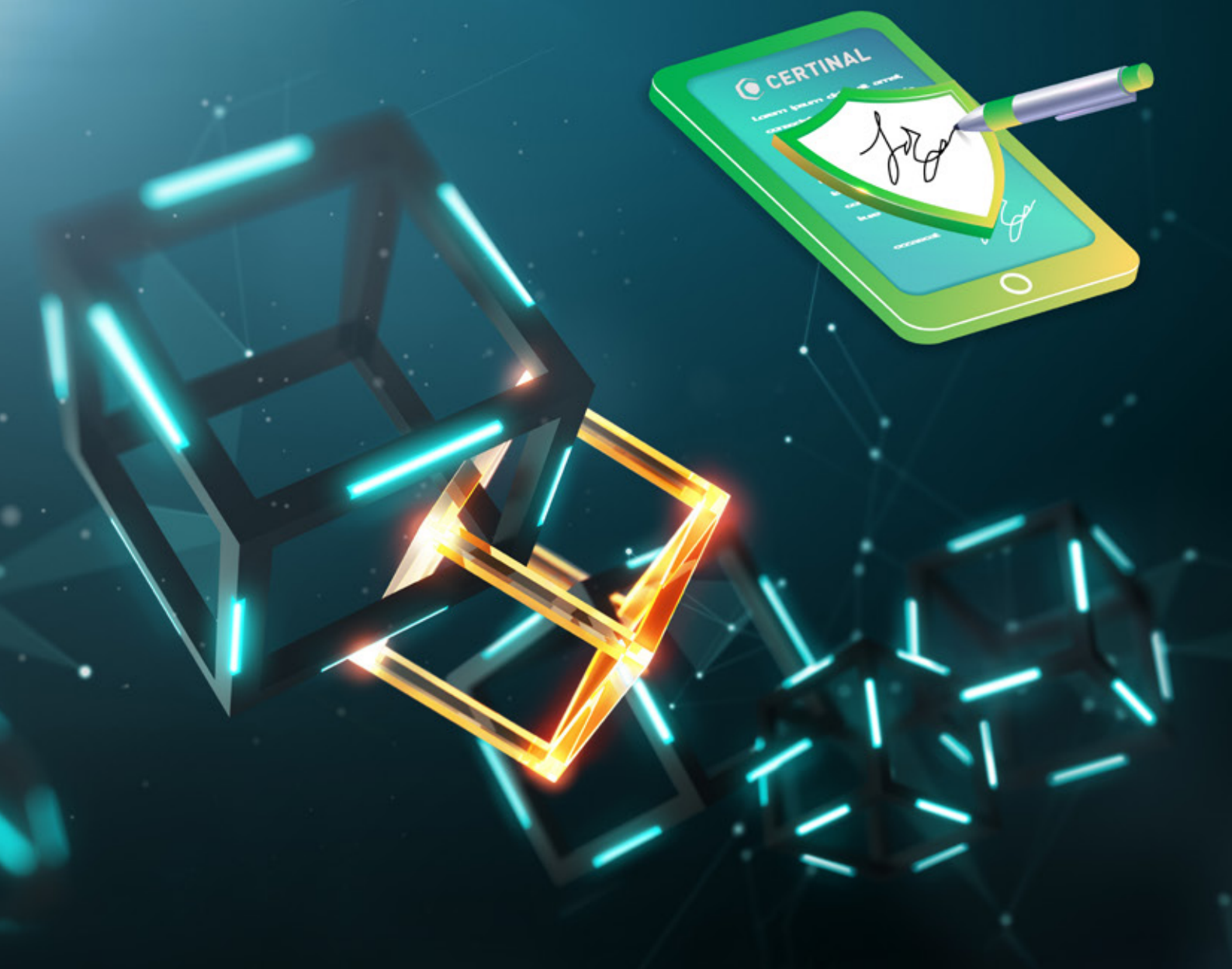
CERTINAL



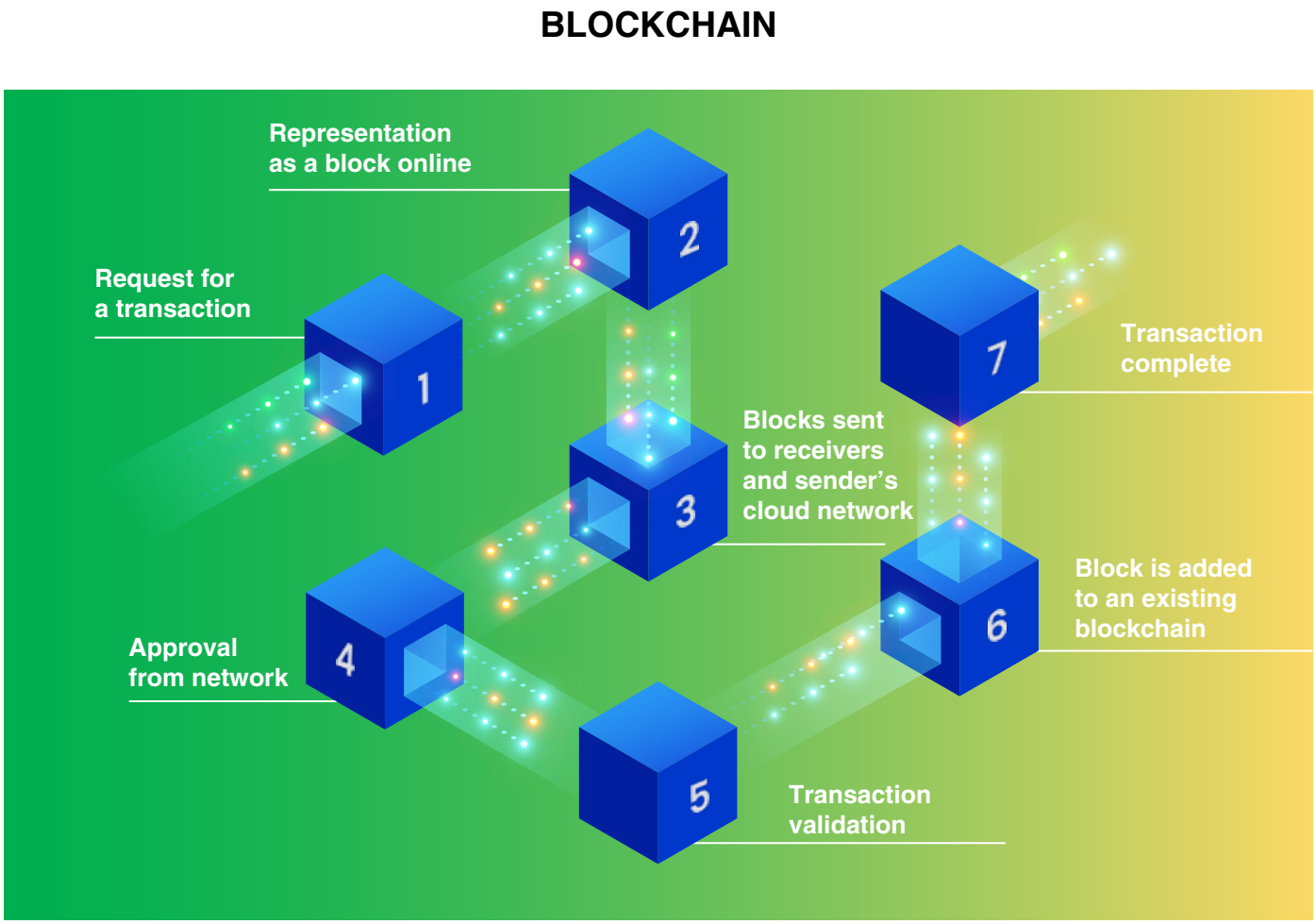
Blockchain Technology Revolutionizing Digital Signatures

Whitepaper

Introduction:

A fascinating word keeps coming up everywhere in the security world: "blockchain." This concept has taken hold of the security industry, much like the word "cloud," and has become one of the hottest growing technologies. Digital signature software is made use of a lot these days to ensure security, non-repudiation, and authentication to access the contents of a data set electronically across networks for decades. Blockchain technology adds a commercial ledger component to a cyber environment, allowing firms or consumers to generate multiple signatures, encrypted fingerprints, and transmit coded information across numerous platforms in a network of centralized servers. Users and companies benefit from the addition of digital signatures. They ensure data's legitimacy and total security against forgery by using complicated mathematical algorithms or codes, making online certificates safe.

Blockchain with a digital signature helps safeguard your online identity and ensures that it is legitimate and authenticated. Documents on the blockchain are encrypted in digital code and stored in transparent, distributed databases that are resistant to manipulation, change, and erasure. As a result, individuals and businesses may now freely transact and engage, and manage in using the enormous potential of Blockchain technology for digital signatures. There will no longer be any fake certificates, degrees, or photoshopped signatures with blockchain document signing. However, there's still uncertainty about how digital signatures and blockchain work together. Here's all you need to know.



What is Blockchain?

Blockchain is a technology used to store data that makes it difficult or impossible to alter, hack, or defraud. It can also be defined as a digital log of transactions copied and distributed throughout the blockchain's complete network of computer systems. Each block on the chain has several transactions. When a new transaction is recorded on the blockchain, a transaction record is added to each participant's ledger.

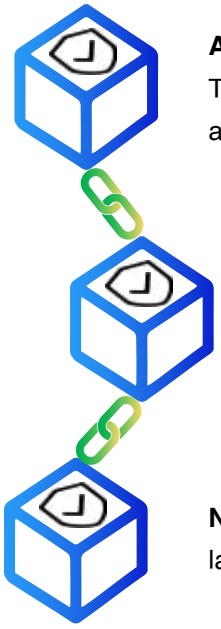
Blockchain can also be defined as a distributed ledger technology that records transactions using a hash. It is an immutable cryptographic signature which means that if a single block in a chain is modified, it will be immediately recognized that the chain has tampered. Every block in the chain across every distributed version would have to be changed if the hackers intend to destroy a blockchain system. The main aim of blockchain is to eliminate the requirement for an external, trusted third party (including certificate authorities) and prohibit anyone from going backward and covering their traces if they corrupt an entry.

Blockchains like Bitcoin and Ethereum are rapidly evolving as new blocks are added to the chain, increasing security.

Role of Blockchain in Digital Signatures

Digital signatures are a vital component to blockchains and are specifically used to validate transactions. When users submit transactions, they must show that they have the power to spend their funds on every node in the system while preventing other users from doing so. Therefore, every node in the network will validate the submitted transaction and review the work of all other nodes to agree on a correct state.

Blockchains provide the following features:



Authentication: Electronic signatures are associated with a specific user using a private key. They use this to determine who owns the private key, which was used to sign the source data in an email or document.

Integrity: Digital signatures use an innovative hashing technique every time to ensure that the message received is not falsified.

Non-Repudiation: This feature is unique, providing that a sender who signs the source material cannot later dispute it.

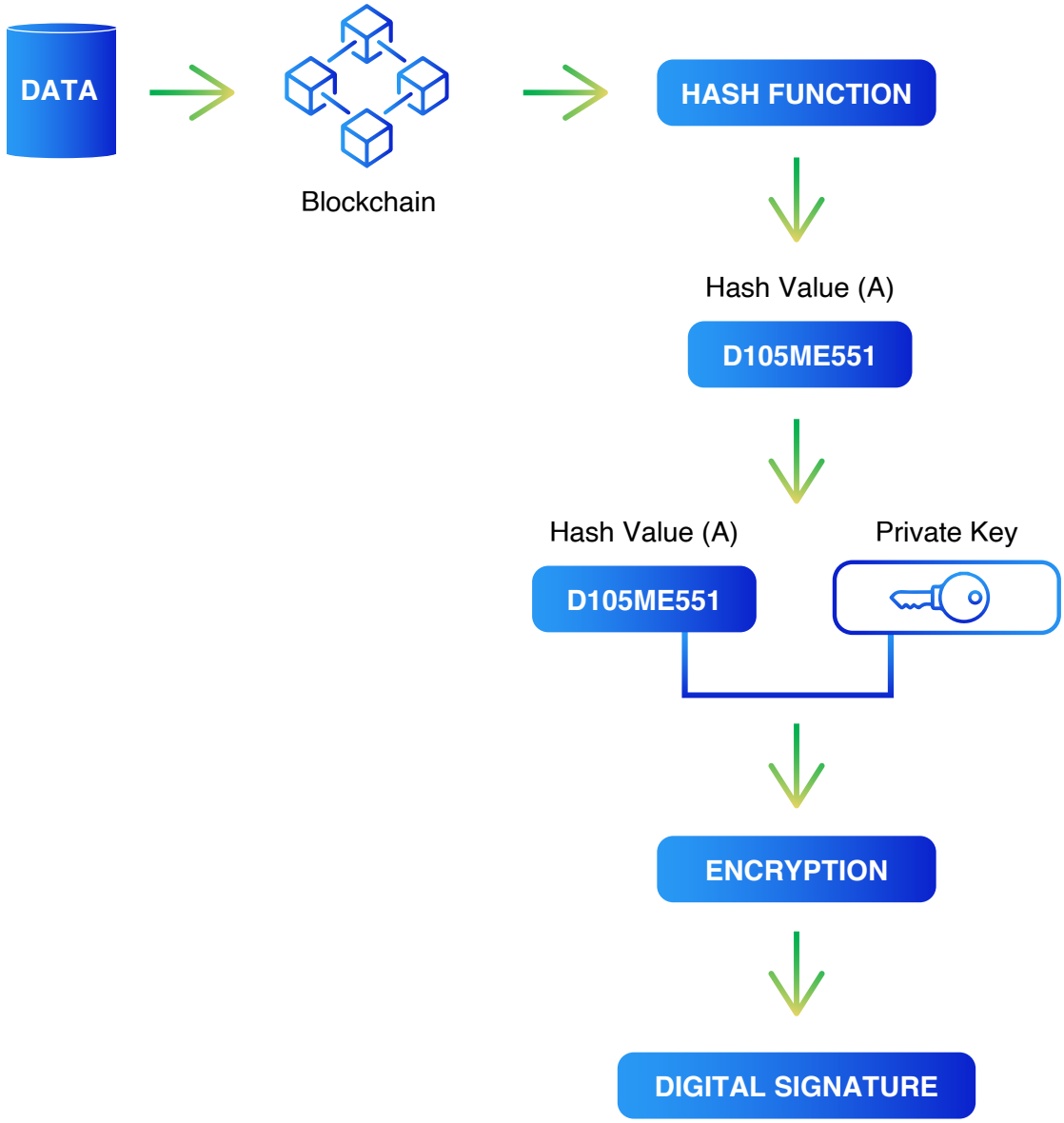
How does Digital Signature Work in a Blockchain?

Blockchain produces a hash of the data. The numerical codes that are used to identify pieces of information are known as hashes. These hash codes are compared to another document's current hash number. If the codes match, the paper is identical, and you can proceed with the transaction safely. Every item of data is allocated a unique hash code.

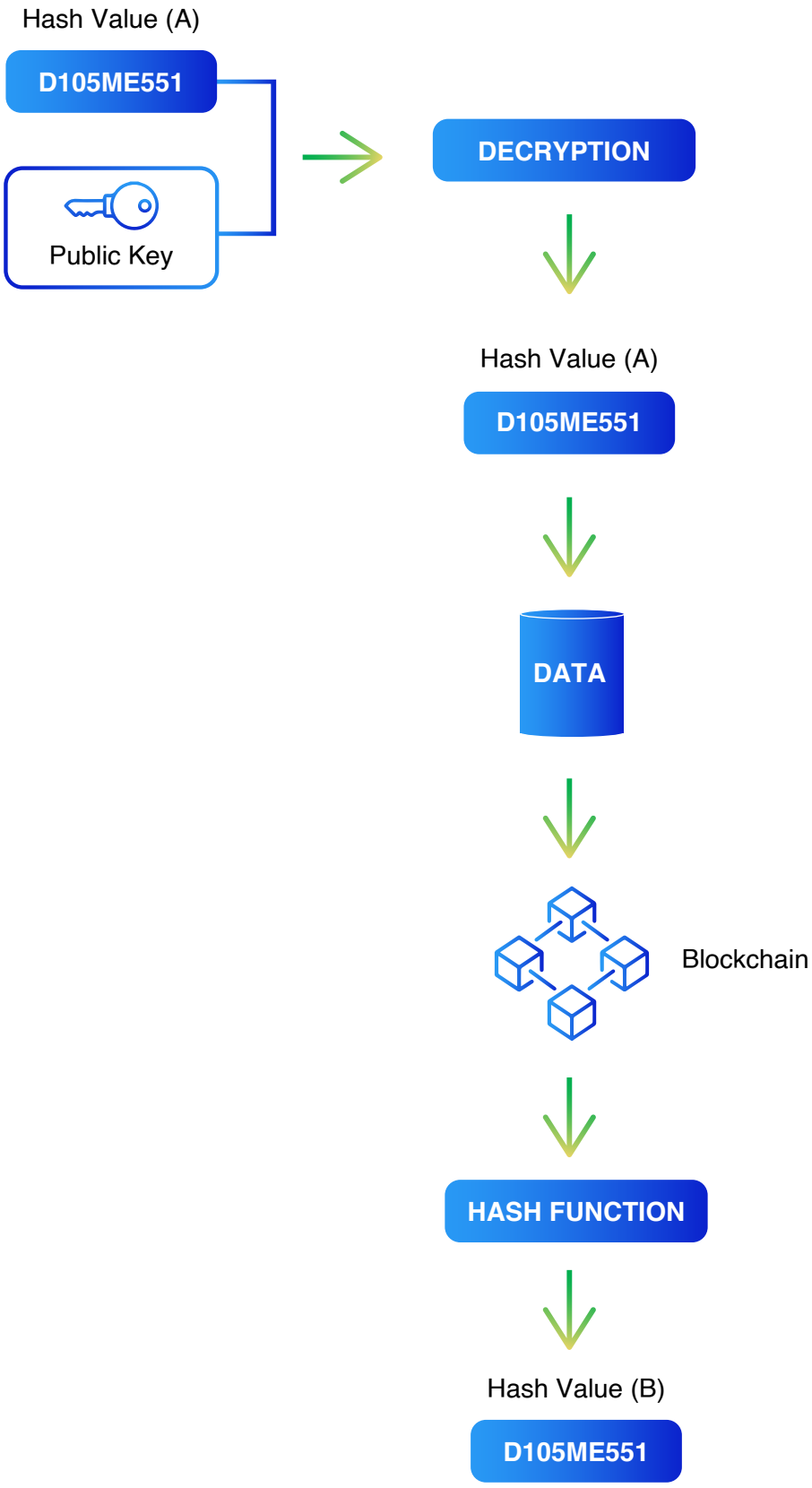
It sends the data with the digital signature to the designated recipient after generating the hash code. When the information and signatures are received, the receiver enters the sender's public key, and the digital signature is submitted to the algorithm. The hash number code is created during this operation.

As previously stated, the receiver verifies the document's legitimacy by comparing the hash code of the original document to their hash code. It is a legitimate signature if both hash number codes are the same; otherwise, it is a forged or invalid signature.

STEP 1: CREATION OF DIGITAL SIGNATURE



STEP 2: VERIFICATION

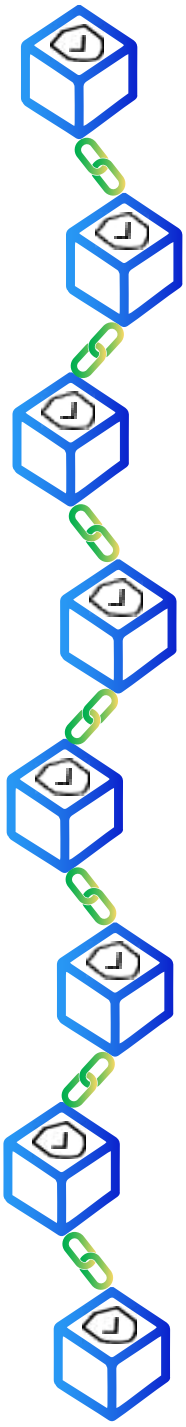


Benefits of Digital Signature in Blockchain

It could significantly benefit the blockchain if a secure private key is used instead of a public key.

With transactions being extremely safe and virtually tamper-proof, they are also easily noticeable. Transparency can be a dream come true for auditors in many cases (such as in financial institutions); the lack of privacy can prevent organizations from fully adopting blockchain in situations where strict privacy requirements are required.

Cryptography is built into blockchain technology, allowing users to e-sign online while maintaining the highest level of data security.



Digital signatures could represent you as a digital identity with the help of blockchain technology.

Signers can sign online legal contracts using their private key (encryption). As a result, the parties can use digital signatures as evidence.

On a blockchain, business users can perform multiple actions in a row.

Blockchain technology adds another layer of security by preventing data tampering and alteration.

It's simple to trace and track documents that have been sent for signatures – keeping track of who has signed and who has yet to sign to complete the documentation process.

This ever-evolving technology aids in the verification of tamper-resistant documents.

The signature and verification processes are independent and do not rely on a central authority.

Since every item on the blockchain is immutable; every user has proof that certain information existed sometime in the past.

Benefits of Digital Signature in Blockchain

Representation as a digital identity

Private key encryption to sign online legal contracts

Perform multiple actions in a row

Prevent data tampering and alteration

Trace and Track documents

Verification of tamper resistant documents

Signature and verification process do not rely on central authority

Proof of information

Conclusion:

Digital signatures are currently gaining popularity as more people accept them. Blockchain here serves as a support for the future of digital signatures by allowing them to become secure and trustworthy. If you take a look at the bigger picture, blockchain in digital signatures exists because of hashing and digital signatures. On the one hand, hashing creates a unique code or key on the blockchain, which makes it safe; on the other hand, a digital signature ensures that the owner completes each transaction without tampering. It is extensively adopted and assimilated into the digital world, representing the future of digital signatures. Using this technology to e-sign sensitive material with an extra level of cryptographic 'hash' can give your company some peace of mind.

Digitally seal your documents using blockchain technology with Certinal and create smooth, hassle-free experiences for your clients and employees.

Book a demo now or contact us at **switchto@certinal.com** to know more.

CERTINAL

Certinal is a wholly owned subsidiary of Zycus, the pioneer in Cognitive Procurement. A familiar name and market leader with years of experience in managing critical contracts & agreements, Zycus boasts of over Fortune 1000 enterprise clients and deployments of procurement and sourcing suite of products. Digital Signing has always been a focus area for Zycus. Thus, Certinal was born with the stated goal of offering a best-in-class Digital Transaction Management solution that will be easy-touse, 100% secure to deploy, and legally compliant around the world. We stand committed to providing a one-stop solution to large enterprise customers, compliant with various security standards and conforming to different regional regulations.

---

919 North Market Street Suite 950, Wilmington, New Castle County, DELAWARE - 19801

www.certinal.com