Demystifying the Digital Wallet

Part 1 – Overview

Demystifying the Digital Wallet

Contents

- Digital Assets
- Digital Currency
- Digital Wallet
- Digital Signature
- Private Key
- Token
- Address
- Blockchain
- Conclusions - Key Takeaways

Digital Assets

A digital asset is anything that exists in a digital format and requires a right to use it. Digital assets include:

- Digital currency

- Digital documents

- Audible content, motion picture, and other relevant digital data

Digital Currency

Digital currency (or digital money) is a form of currency that is available only in digital or electronic form, and not in physical form.

Digital currency refers to any means of payment that exists in a purely electronic form. Digital money is not physically tangible like a dollar bill or a coin. It is accounted for and transferred using online systems. One well-known form of digital money is the cryptocurrency Bitcoin.

Digital currency can also represent fiat currencies, such as dollars or euros. Digital money is exchanged using technologies such as smartphones, credit cards, and online cryptocurrency exchanges. In some cases, it can be converted into physical cash via an ATM.

Note: Fiat money is a government-issued currency that is not backed by a commodity such as gold.

Digital Wallet
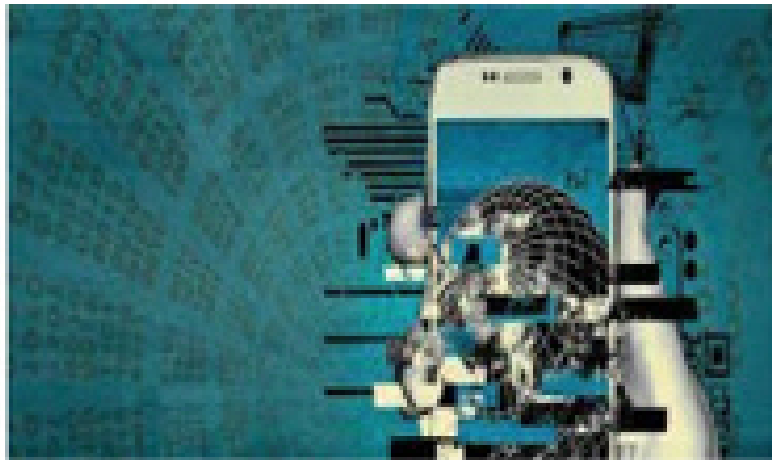
The Digital Wallet **secures** the Digital Currency asset. The digital wallet does not hold Digital Currency.

The digital wallet is a software-based system that provides the following functionality:

- Securely stores account holders' payment information and passwords for numerous payment methods and websites.

- Enables account holders to complete purchases easily and quickly with near-field communications technology

- Facilitates the exchange of digital currency for the account holder.

- Maintains at least one private key for each digital currency for each account

- Generates and maintains multiple private keys necessary to transfer "tokens" for each account

Digital Signature
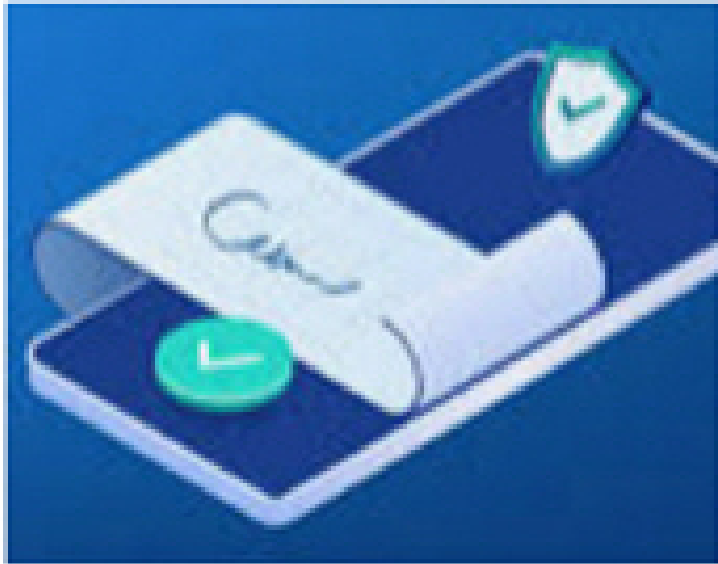
Digital signatures are used to prove identity, to access information or services on the Internet, or to sign certain documents digitally.

A digital signature transaction includes a pair of keys: a **private key** and a public key.

Digital signatures are used for identification. Authentication considers who created the asset, and that no one interfered during a transmission.

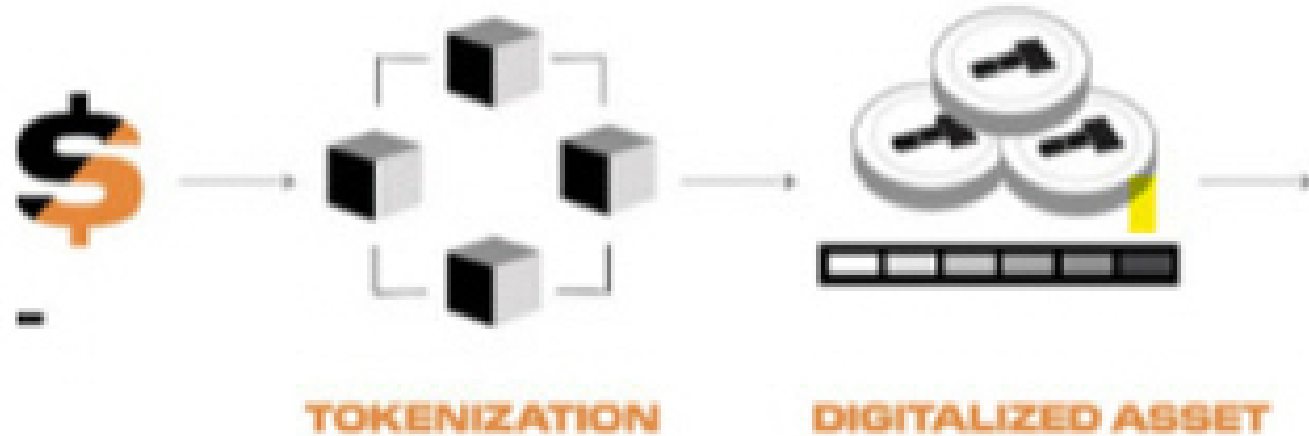Digital signatures are created using algorithms.

Private Key

A digital wallet stores the private keys of a user.

When a transaction is initiated, the wallet software creates a digital signature by processing the transaction with the private key.

Keys never leave the wallet.

Token

TOKENIZATION   **DIGITALIZED ASSET**

Digital wallets employ a process to protect sensitive data by replacing it with secure, surrogate data, called a token, when processing transactions.

Address

A wallet address is an identifier that represents a destination for a digital currency payment. For each address, digital currency is exchanged, using a private key, by:

- Signing transfers
- Reporting balances

Note: The BNYM wallet implements the NexEn client interface, provides unified reporting, and establishes additional compliance process to satisfy regulatory, and BNYM's policy requirements.

Blockchain

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

BLOCK 1	BLOCK 2	BLOCK 3
Transaction A	Transaction B	Transaction C
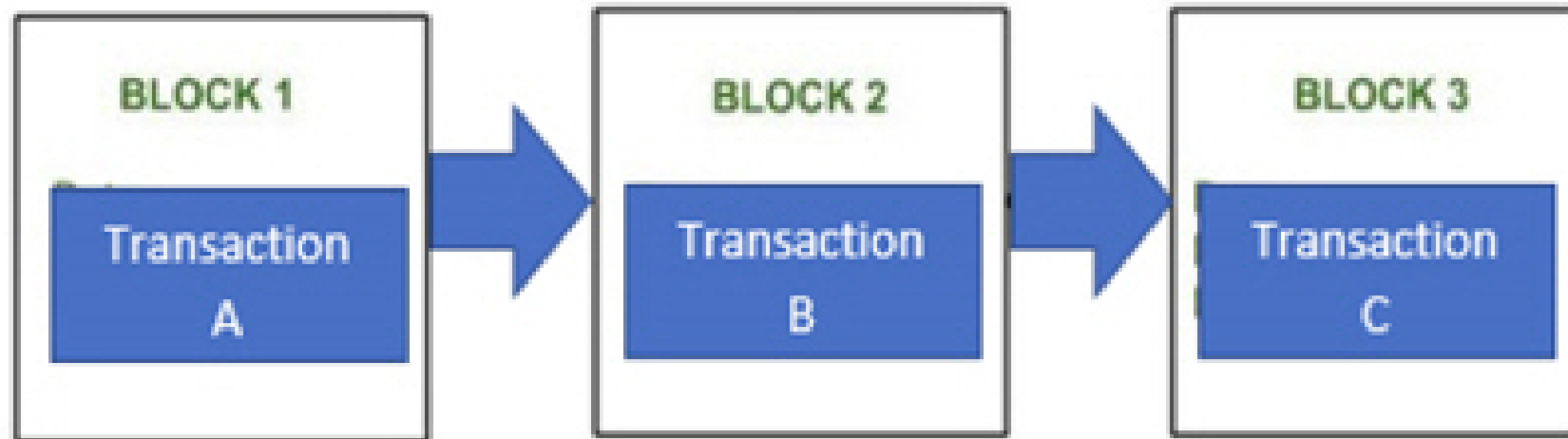
Conclusions - Key Takeaways

A digital wallet is a secure facilitator between BNYM and our clients to withdrawal, transfer and monitoring of addresses managed by BNYM on behalf of our clients.

The digital wallet is a software-based system that provides the following functionality:

- Securely stores account holders' payment information and passwords

- Enables account holders to complete purchases easily and quickly

- Facilitates the exchange of digital currency for the account holder