Demystifying the Digital Wallet

Part 3 – Digital Wallet Functionality

Demystifying the Digital Wallet

Contents

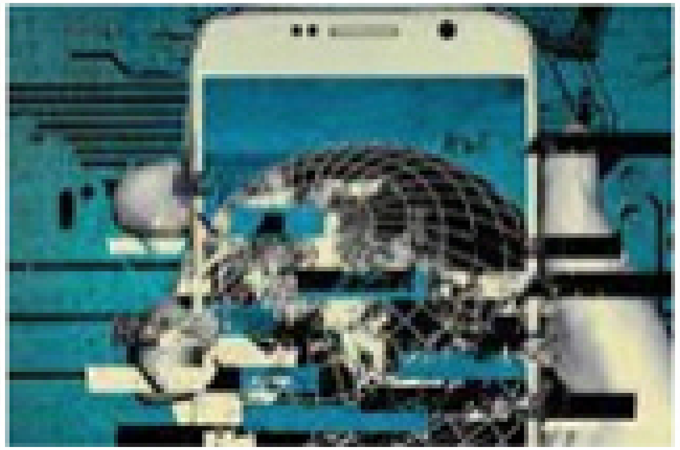
- Handling Traditional Assets vs Digital Assets
- Digital Wallet Functionality
- Digital Wallet - The Nightbox Analogy
- Digital Wallet - Withdrawal/Transfer
- Digital Wallet – Deposit
- Conclusions - Key Takeaways

Handling Traditional Assets vs Digital Assets

The table below highlights the differences between the handling of traditional and digital assets.

Properties	Safe Deposit Box	Financial Transaction	Digital Wallet
Location of Assets	A physical vault (institutional)	Accounting Systems (institutional)	Virtually (digital) on a blockchain
Identity	Safe Deposit Number	Account numbers	Address
Privacy: **Activity / Identity**	Private/ Private	Private / Private	Public / Private, though activity may link to an ID
Balance	Private	Private	Publicly visible
Credentials	Physical key (unique to client)	Financial institutions credentials (not unique to a client)	Address's private key (unique to client)
Deposit	Must have key to deposit	Transact with receiving institution	No action by recipient of funds
Withdrawal	Must have key to withdraw (once open all assets are available)	Require transfer instruction with credentials: • From Address • To Address • Amount • From/To/Amount authenticated by sending bank	Requires transfer instruction with address credentials (digital signature): • From Address • To Address • Amount • From/To/Amount signed by private key of address Note: the withdrawal leg requires the debtor (sender) to sign the withdrawal with the address's unique private key, and no action is required by the beneficiary (recipient).

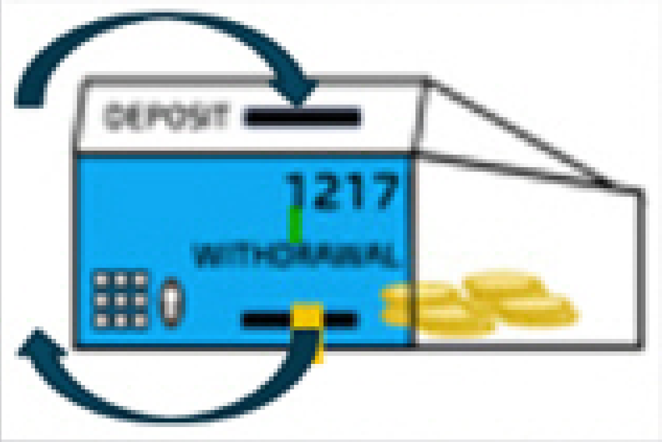
Digital Wallet Functionality



The digital wallet does not hold assets. The digital wallet provides the following functionality:

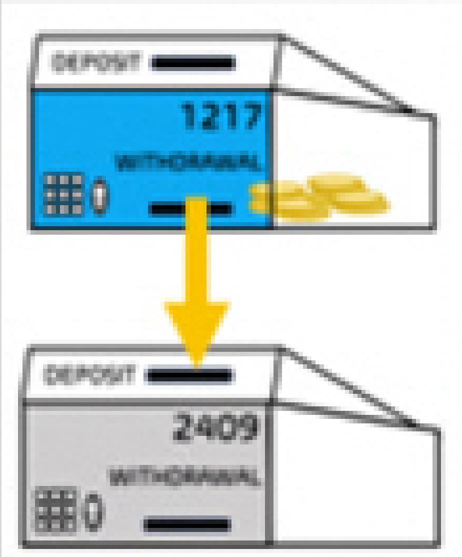
- Holds cryptographic keys resident in the wallet
- Submits signed transactions to the blockchain
- Generates and stores private "signing" keys for each of the account's addresses on one or more blockchain
- Monitors the blockchain for:
    - Transaction confirmations
    - Deposited funds
    - Balances

Digital Wallet - The Nightbox Analogy



Since a digital wallet facilitates transacting cryptocurrencies on a blockchain, the simplified Nightbox Analogy that follows traces the movement of assets on the blockchain, as deposited, and withdrawn from a Nightbox.

Digital Wallet - The Nightbox Analogy



In this analogy consider the storage of tokens in the form of a box with an address.

Deposits and Withdrawals

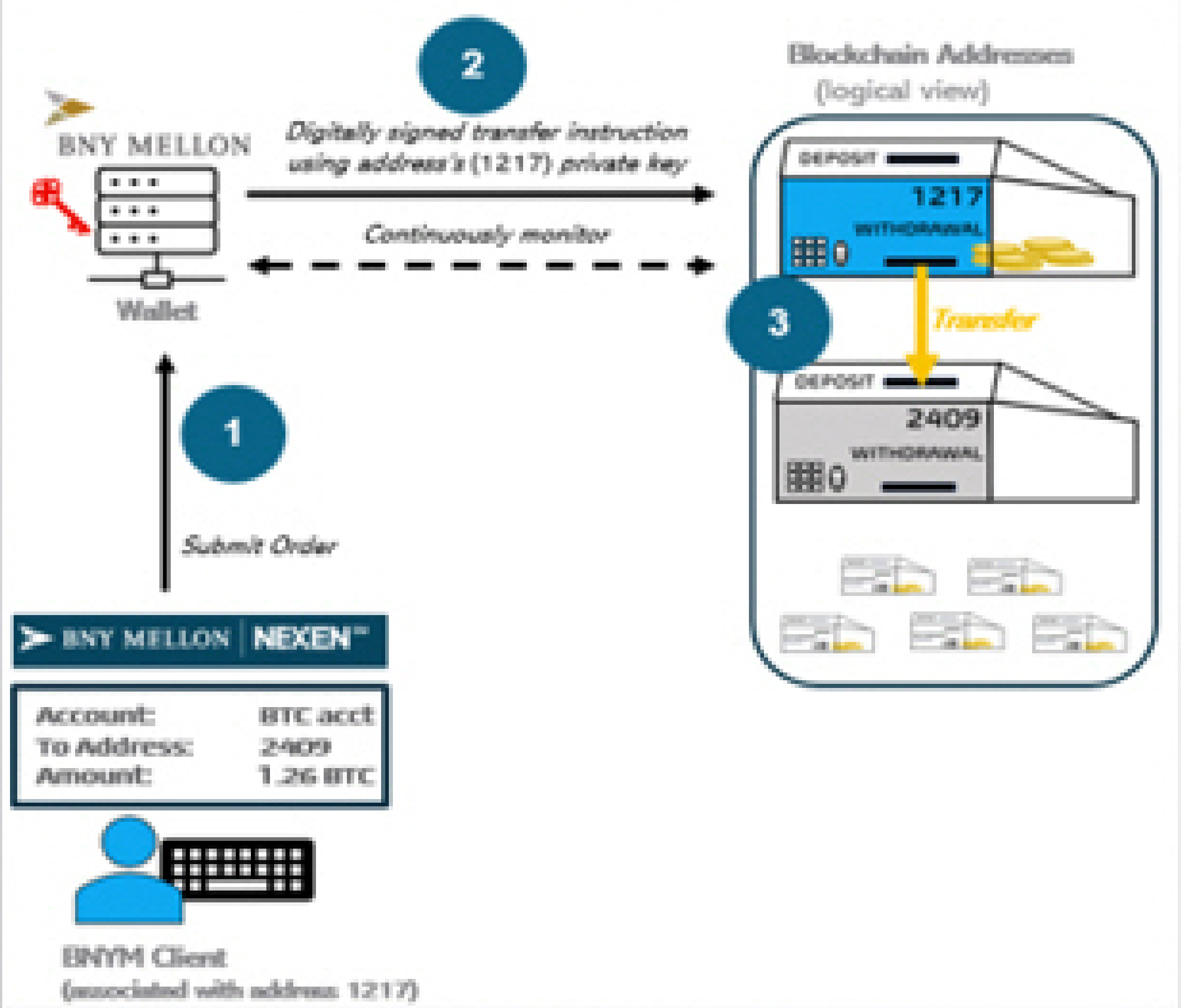
Consider a Nightbox has an address (1217) to identify it. the box is like a Nightbox in that depositing tokens into the box requires no activity by the owner of the box. Withdrawing is much like an ATM. The owner of an account on an ATM, must provide credentials and exact amount, for which they have sufficient balance, to withdraw funds.

Transfers

Tokens are not transferred without proper credentials. To withdraw tokens from an address, signed instruction are submitted to the blockchain. The instruction will include the amount to be transferred FROM address 1217 TO address 2409. This instruction is signed with a digital signature using a secret key, also known as a private key. The blockchain only accepts transactions signed with the private key associated with the address. Note, the recipient has no activity in receiving money transferred.

Lastly, note since any observer can watch funds going in and out of the box, the balance for this address is known publicly.

Digital Wallet - Withdrawal/Transfer



This diagram outlines the path of a digital wallet withdrawal.

Step 1 - the BNNY Client account associated with address 1217 submits a withdrawal order from address 1217 to address 2409

Step2 - the digitally signed transfer instruction using address 1217's private key is sent

Step 3 - a withdrawal (transfer) is made from 1217 and deposited in 2409

BNYM Focus

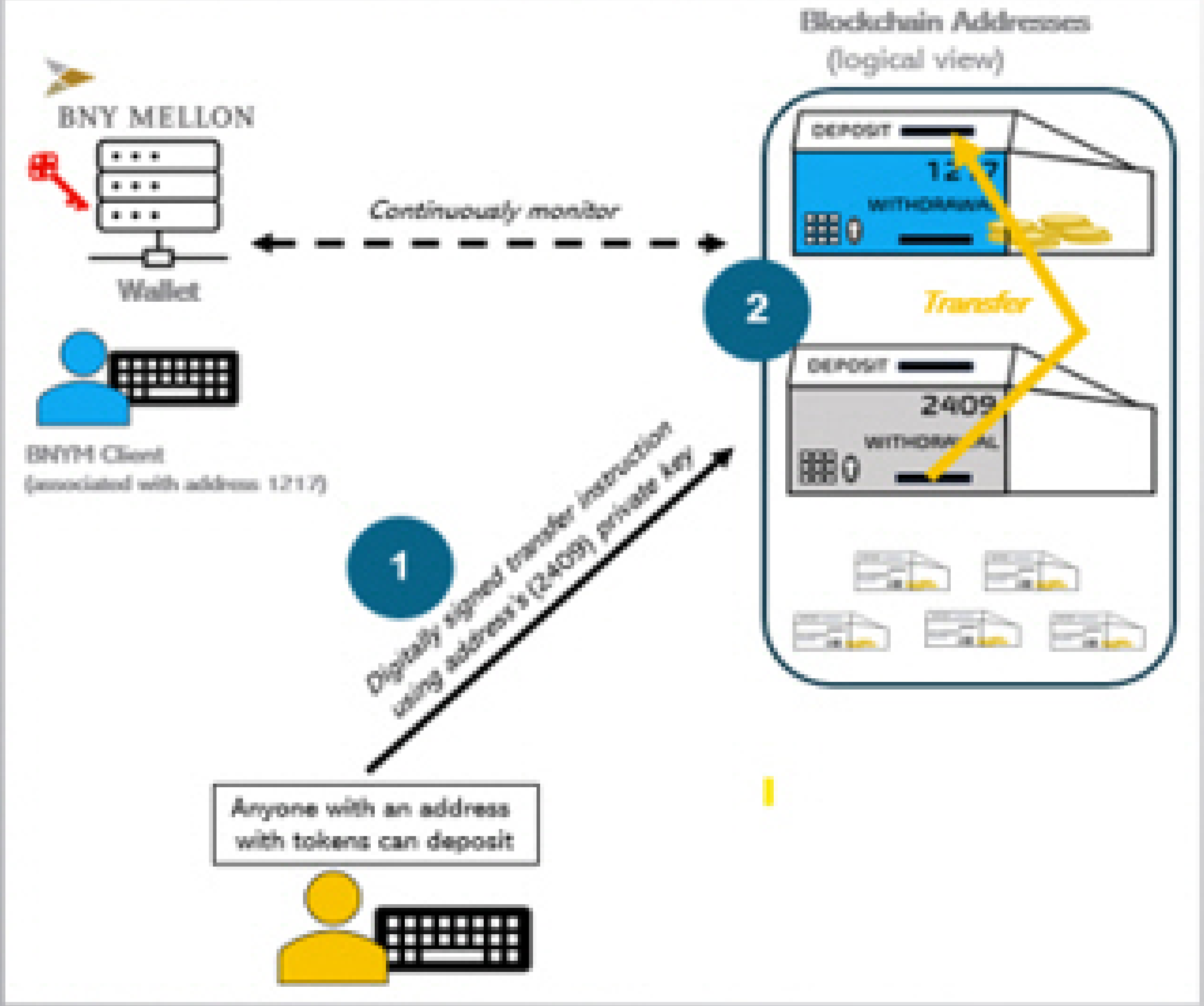
Referring to flow on the previous page, the box 1217, shown as blue, is managed by BNYM. The BNYM wallet holds the private key to sign transfers. Tokens are not held in the BNYM wallet, but rather on the blockchain. To withdraw tokens and deposit into another address, BNYM uses the secret key which it will use to sign “transfer” instructions.

The wallet is a facilitator to transfer and monitor assets associated with addresses on a block chain. At BNYM the wallet resides in our Data Centers and securely holds the private cryptographic keys of the addresses BNYM manages on behalf of our clients. For a client to exchange cryptocurrency, the client provides instructions through a portal, such as NexEn, to BNYM. The instruction will include the customers FROM address (if the customer has more than one address on the blockchain), the TO address for which the exchange will move tokens into, and the amount of the exchange. BNYM wallet will now format the instruction and sign the transfer request with the private key of the address. Subsequently, BNYM will monitor the blockchain to ensure the exchange is completed.

BNYM has additional processes to meet our regulatory and policy requirements. Note: BNYM has established additional processes to satisfy our regulatory obligation, e.g.:

- Allowlisting (aka Whitelisting) recipient (“to”) addresses for compliance
- Historic transaction analysis for AML (Anti Money Laundering)

Digital Wallet - Deposit


Blockchain Addresses
(logical view)
BNY MELLON
Wallet
Continuously monitor
BNYM Client
(associated with address 1217)
DEPOSIT
1217
WITHDRAWAL
2
Transfer
DEPOSIT
2409
WITHDRAWAL
1
Digitally signed transfer instruction using address's (2409) private key
Anyone with an address with tokens can deposit

This diagram outlines the path of a digital wallet deposit.

Step 1 - anyone with an address and tokens can make a deposit to the BNYM Client account associated with address 1217. A transfer is initiated using a digitally signed transfer instruction using address 2409's private key.

Step 2 - a withdrawal (transfer) is made from 2409 and deposited in 1217.

BNYM Focus

Deposits into addresses of our clients is simpler because deposits require no action by the recipient. Anyone can deposit to addresses BNYM manages. BNYM continually monitors addresses for which it manages to ensure deposits are properly identified.

BNYM has additional processes to meet our regulatory and policy requirements.

Note: Though deposits do not require BNYM interaction, BNYM has established additional processes to satisfy our regulatory obligation, e.g.:

- Require client instructions (pre- or post- deposit)
- Compliance checks
- Monitor balances

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.

Now that you have completed this module, you should be familiar with the following:

- Handling Traditional Assets vs Digital Assets
- Digital Wallet Functionality
- Digital Wallet - Withdrawal/Transfer
- Digital Wallet – Deposit