mourant

GUIDE

Cryptocurrency - The operational risks of holding crypto

Last reviewed: February 2022

Operational Risks

The appeal of distributed ledger technology (**DLT**) lies in its ability to replace the need for trust in intermediaries, relying instead on cryptographic proof. The removal of a third party intermediary in transactions on a distributed ledger (**DL**) creates an ecosystem where 'code is law' and which proponents argue can result in increased certainty and immutability. However, the decentralised nature of the system exposes holders of cryptocurrency 'coins' or 'tokens' (**Coins**) to various operational risks.

Public and Private Keys

What are they?

In the absence of a third party intermediary, DLT relies on cryptography to establish trust. Public key cryptography (**PKC**) utilises two 'keys' that together encrypt and decrypt data residing on or moving through the network. In the context of cryptocurrency transactions, the purpose of PKC is to prove that a transaction was not forged, and that any Coins received came from the actual owner of those Coins.

In its most basic form, PKC is analogous to a post office mailbox. A person standing in the sorting room of a post office can see into every mailbox. This individual has the ability to tell if any given mailbox has a letter, a package slip or nothing at all. However, only the person who holds the key to their own specific mailbox can open the box [from the front] and remove whatever mail has been received.

A public key is in effect a mailbox address on the DL. Any person given this address can send 'mail' (Coins) to that specific 'mailbox' (wallet). Transactions on the DL can be tracked using the public key address. A private key unlocks an owner's right to access and transfer Coins.

How do they work?

There is a cryptographic link between the public key and the private key. With a private key, an individual can theoretically create as many public keys as they would like. Some DLs create a new public key for each separate transaction. Reversing the cryptographic process to decipher a private key from a public key is virtually impossible.[1]

When an individual owns Coins, what they actually own is a private key that gives them access to those funds; the Coins themselves are stored on the DL. The private key not only unlocks the right to transfer those Coins, but also acts as a form of signature on the DL to authenticate the fact the Coin-holder initiated the transaction.

[1] Although theoretically possible to do with quantum computing, in practice it would take a supercomputer thousands of years to break the encryption by brute force. This is because public key cryptography is built on the mathematical basis of 'trapdoor one-way functions' (math problems easy to compute in one direction and nearly impossible to reverse). A helpful overview of the relevant cryptography can be found here https://medium.com/coinmonks/private-and-public-key-cryptography-explained-simply-4c374d371736

Public keys – the risk of typos

A public key typically shows as a 30-plus character alphanumeric string.[2] In comparison, a Wi-Fi password is generally only 8-10 characters long. As anyone who has tried to type in a Wi-Fi password can tell you, it can be difficult to correctly input each number, letter and capitalisation in an alphanumeric string on the very first attempt.

Due to the peer-to-peer (**P2P**) nature of DLT, standard safeguards found in the retail financial sector are non-existent on most DLs. For example, consider how most online banking applications verify an inputted sort code and account number against the recipient's account name before transferring funds. P2P systems on the other hand rely on correct input at source and generally do not provide means of checking additional recipient details.

Due to the irreversible nature of DLT protocols, transactions cannot be reversed or cancelled once initiated. Coins sent to the wrong public key address cannot be recalled, and a sender will generally have no means of recourse against a recipient. In addition, it can be nearly impossible to track down the identity of such an erroneous recipient given the pseudononymous nature of parties transacting via DLT.

Private keys – safety first

A private key is hundreds of digits long in binary, and generally shows as a 64 character alphanumeric.[3] If a user loses their private key, they can no longer access their wallet. Because of the decentralised nature of DLT, there is no overarching entity to petition if a private key is lost – the Coins held in that wallet are effectively unrecoverable.[4]

Stories of such private key losses are common, with several unlucky individuals having lost access to hundreds of millions of pounds worth of cryptocurrencies.[5] Developers are often unsympathetic to such plights, with Bitcoin creator Satoshi Nakamoto famously opining "Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone."[6]

One of the key operational risks in this environment lies in the very fact that a private key unlocks the right to transfer Coins - any third party who manages to discover an individual's private key can immediately access and transfer all Coins stored in that wallet to any address they choose. Again, the decentralised nature of DLT effectively eliminates any form of recourse to recover such stolen Coins.

The challenge of storing a private key is to keep it safe from hackers and bad actors, yet generally accessible to its owner. Various methods of storage are available including cold storage (stored off the system on paper, hardware or offline software wallets), hot wallets (stored in a device connected to the internet) or custodial wallets (where the private key is held by a third party).

Smart Contracts

What are smart contracts?

Another application of DLT which has removed the necessity for intermediaries is the developing area of 'smart contracting'. Smart contracts are in effect automated contracts driven by code.

How do they work?

A helpful way to think about smart contracts is in the context of a standard vending machine. When an individual approaches a vending machine wishing to purchase a soft drink, the vending machine is

[2] Example ETH public key: 63FaC9201494f0bd17B9892B9fae4d52fe3BD377 (EXAMPLE ONLY) courtesy of http://www.herongyang.com/Ethereum/Etheruem-Account-Public-Private-Key-Example.html

[3] Example ETH private key: 8da4ef21b864d2cc526dbdb2a120bd2874c36c9d0a1fb7f8c63d7f7a8b41de8f (EXAMPLE ONLY) courtesy of http://www.herongyang.com/Ethereum/Etheruem-Account-Public-Private-Key-Example.html

[4] In very rare instances, hackers may be able to assist in restoring access to certain wallets that have lost private keys. The following article provides an interesting insight into such an attempt: https://www.theverge.com/2022/1/24/22898712/crypto-hardware-wallet-hacking-lost-bitcoin-ethereum-nft

[5] https://www.newyorker.com/magazine/2021/12/13/half-a-billion-in-bitcoin-lost-in-the-dump; https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

[6] The original discussion chain with Satoshi Nakamoto's comment can be found here: https://bitcointalk.org/index.php?topic=198.msg1647#msg1647

programmed such that if the individual enters the requisite amount of coins and selects a soft drink option the machine will either (a) produce the soft drink and keep the coins or (b) prompt the individual for another option and/or return the coins if that particular soft drink is out of stock.

Smart contracts operate in much the same manner. The requisite criteria for a smart contract are encoded such that once specific criteria are met, the contract automatically completes. Smart contracts are commonly used as automatic market makers in decentralised P2P finance such as cryptocurrency swaps.

Risks of smart contracting

The main vulnerabilities to smart contracts are cyber-attacks and technology failures. Most smart contracts depend on off-chain data providing information (for example price feeds). Data storage points are vulnerable to targeted attacks, as are transfer points when data is being moved 'on-chain'.

A common characteristic of decentralised finance projects (which are often made up of complex, interlocking smart contracts) is open source code. This structure allows all users to observe the code in operation and quickly identify any defects. Equally, it allows malicious users to scrutinise and exploit any vulnerabilities in the code.

If, for some reason, a smart contract has an error in the code or is corrupted resulting in the smart contract not completing as intended, individuals are generally unable to seek recourse or mediation via a third party. Rather, the code governing a smart contract is deemed 'law' and any errors in that code would be considered an inherent risk to this manner of contracting.

Reducing operational risks

Owing to the often irreversible nature of DLT transactions and smart contracting, conducting sufficient due diligence before entering into such arrangements is key. A comprehensive review by professional advisors who are familiar with the practical and legal issues, together with the financial and technical operation, will be increasingly important especially where high levels of funding are at stake.

Likewise, where an individual holds significant sums in Coins, utilising a third party professional custodian to safeguard their private key could offer an enhanced degree of security and a level of insurance against loss.

Contacts

A full list of contacts specialising in cryptocurrency can be found here

This guide is only intended to give a summary and general overview of the subject matter. It is not intended to be comprehensive and does not constitute, and should not be taken to be, legal advice. If you would like legal advice or further information on any issue raised by this guide, please get in touch with one of your usual contacts. You can find out more about us, and access our legal and regulatory notices at mourant.com.