

This infographic defines various types of cryptoassets and highlights how the role of cryptoassets may or may not play out in the ongoing Ukraine conflict.



Blockchain/Distributed Ledger

A blockchain, which is a form of distributed ledger technology, is an ever-growing chain (or list) of records called blocks. Each block contains information regarding the block before it. Blockchains are secure by design; blocks are linked together using cryptography, and the data in any given block cannot be altered without also altering all subsequent blocks in the chain. As a result, blockchains are highly resistant to both malicious and accidental manipulation, such as nation state launched cyber-attacks.

Due to their decentralized and immutable nature, data stored in the blockchain is inherently traceable and trackable, enabling transactions for those who have lost access to banking services. Equally, blockchain analytics utilizing machine learning are proving to be a valuable forensic resource, offering greater insight into the activity of illicit and sanctioned actors.



Mining

In the world of cryptoassets, mining refers to the act of extracting new tokens and introducing those tokens onto their respective blockchains. The process involves sophisticated computers solving complex computational mathematical problems; the degree of complexity is dependent on the specifications of the particular cryptoasset.

Cryptoasset mining remains outside of the regulated perimeter, heightening third parties' risk of certain jurisdictions continuing to offer services to Russian state-linked entities. Given Russia's conducive climate for mining operations, it may decide, as Iran did, that mining offers the possibility of revenue generation and the opportunity to move newly minted coins to unknown wallets.



Initial Coin Offerings (ICOs)

A company seeking to raise money to create a new coin, app, or service can launch an ICO to raise funds. Investors buy into an initial coin offering to receive a new token or coin issued by the developers. The digital token issued may represent a share in a firm, a prepayment voucher for future services or, in some cases, offer no discernible value at all. Whilst ICOs have a legitimate function, they are usually completely unregulated and numerous examples have turned out to be fraudulent.

Given the existential growth in cryptoasset scams, it is feasible that criminal ICOs and other fund-raising platforms could be set up to dupe customers into sending funds to fraudulent ventures with links to a Ukrainian cause. Compliance professionals should ensure that customers who send money to support government or humanitarian ventures are confident they are sending to legitimate ventures such as verified wallet addresses.



Exchanges

A cryptoasset exchange (or virtual asset service provider) is a business whose main activity involves (but is not necessarily limited to) offering cryptoassets to retail and institutional customers. Its activities involve exchanging cryptoassets for money, or money for cryptoassets, or simply the exchange of a cryptoasset for another cryptoasset. Some also act as liquidity providers, wallet providers, or financial intermediaries through their peer-to-peer features, and/or offer a variety of other cryptoasset financial instruments.

Cryptoasset exchanges are yet to fall under international Russian or Belarusian sanction regimes, and are not obliged to de-risk customers in those jurisdictions. However, parasite or non-compliant exchanges have been picked out for enabling illicit transactions, some of which have links to Russia and ransomware payments (e.g. SUEX and P2P exchange Chatex).



Wallets

Hardware or software wallets store a user's private and public keys and interface with a blockchain network. Anyone can deposit cryptocurrency in a public address, but funds cannot be removed from an address without the corresponding private key. Private keys represent final control and ownership of cryptocurrency. A hot wallet is connected to the internet and could be vulnerable to online attacks – which could lead to stolen funds – but is faster and makes it easier to trade or spend cryptoassets. A cold wallet is typically not connected to the internet so is more secure but less convenient.

Some exchanges have proactively blocked and reported thousands of illicit Russian/Belarusian wallet addresses to law enforcement to support sanctions enforcement.



Decentralized Finance (DeFi)

DeFi is a blockchain-based form of traditional financial products, which operates peer-to-peer without any intermediary, using smart contracts (DApps). DeFi platforms allow users to trade cryptoassets, use derivatives to speculate on price movements on a wide variety of different assets, generate interest in savings-like accounts, and lend to or borrow from others. Regulation of DeFi is sparse, although FATF has indicated that many apps qualify as centralized through a controlling party.

In theory, this opens up the risk that designated Russian entities could invest and transfer assets without interacting with traditional financial gatekeepers, by transacting directly between DeFi participants. It is feasible that Russia will look to take advantage of DeFi protocols, given their lack of third party authenticated transactions or by hacking protocol vulnerabilities.



Non-Fungible Tokens (NFTs)

NFTs are digital tokens used to prove ownership of unique tangible and intangible items. Since the beginning of the conflict, the Ukrainian Government has solicited donations via several different cryptoassets. As part of their fund-raising efforts, the government has issued a series of NFTs tracking the course of the conflict and has indicated that NFTs may be offered to donors as compensation for earlier donations.

The money laundering potential of NFTs is mostly speculative, but consumers should be aware of a heightened fraud and market abuse risk from “rug pulls” and wash trading schemes.



Central Bank Digital Currency (CBDC)

A CBDC is a digital version of a government-issued fiat currency that is managed by a central bank. Some cryptographers are experimenting with establishing digital currencies which leverage public keys but without any links to a public blockchain which, in theory, would make cryptoassets as untraceable as cash.

Since the start of the Ukraine conflict, Russian authorities have signaled that they have dropped their resistance to a CBDC and are actively exploring the prospect of introducing one, potentially allowing Russian authorities visibility over all its citizens' transactions. The Russian Government has also suggested that it would accept payment for oil and gas via cryptoassets in future.

For further information visit our Ukraine crisis rapid response hub
<http://www.acams.org/ukraine>