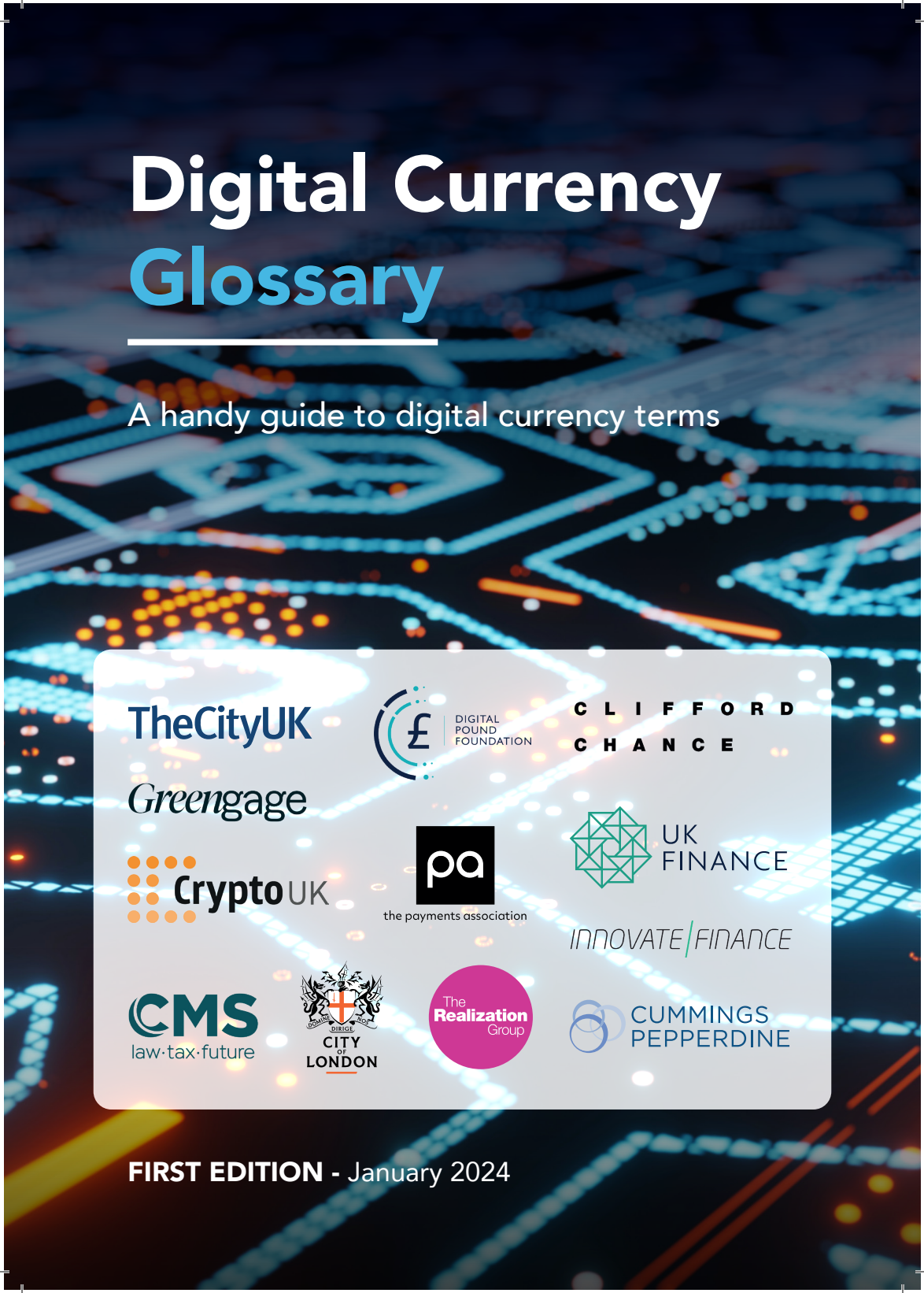
Digital Currency Glossary

A handy guide to digital currency terms



FIRST EDITION - January 2024

Foreword

This glossary has been produced by UK Finance, The Payments Association, Digital Pound Foundation, TheCityUK, Innovate Finance and City of London Corporation, and supported by CryptoUK, CMS, Clifford Chance, Greengage, Cummings Pepperdine and The Realization Group.

Digital currencies have been gaining rapid momentum over the past few years and have the potential to change how society thinks about and uses money. There is no doubt that this is an area of growing interest for many consumers, merchants and financial institutions. The adoption of new forms of regulated digital money across the globe will open many opportunities for the UK to remain competitive in leading the digitisation of the UK's financial services sector. The world's largest financial institutions and fintechs are pouring resources and brainpower into this technological innovation, and the public sector must take note of this paradigm shift.

As a group of trade associations and firms we welcome and stand ready to support the government's plan to make the UK a leading global player in the digital asset and money ecosystem. Our members are united in their desire to enhance the understanding of stakeholders, policymakers and other market participants, including the retail user.

Understanding the language of this new industry and technology will be vital for policy makers and help them to recognise and evaluate the enormous potential of this sector. The consistent use of terms will enable a wide-spread common lexicon that supports a robust understanding of the operational impacts, challenges and potential solutions of new forms of digital money, assets and the underlying technology.

For ease of reference, the glossary has been divided into three (3) sections:

- **Part A: The Basics: Distributed Ledger Technology, Blockchains and their Building Blocks**
- **Part B: Digital Currencies and Cryptoassets**
- **Part C: The Digital Currency Ecosystem**

We hope that this glossary will help to demystify some of the areas under discussion and help the UK to make the best of the opportunities that undoubtedly lie ahead.

Definitions here are written in an easy-to-consume way, and omit the nuances inevitable within complex ecosystems and technologies to maintain overall readability.

We have focused on terms that those in the public and private sector might come across when discussing these issues.

Glossary

Part A - The Basics: Distributed Ledger Technology, Blockchains and their Building Blocks

Algorithm	A set of computational rules that determine a process for executing operations.
Blockchain	A type of distributed ledger technology (DLT) database that is decentralised, distributed and self-proving, where transactions (or ledger changes) are verified and validated in blocks. This data is then linked ("chained") to the previously verified data block, forming a chain. This link makes the ledger, and the data sitting on it, more secure as it is stored cryptographically. Blockchain is a distributed ledger that can store digitised assets - cryptocurrencies, documents, contracts - in a tokenised form. Users have control - they don't have to rely on a third party. Several types of blockchain exist, driven by the nature of their use cases, the type of ecosystem they support, and the source of the assets. The dominance of crypto as the first (and most popular) use case has different power and performance characteristics than, for example, a fiat-only blockchain, or a blockchain used for operational needs, e.g. supply chain documentation.
Consensus	Consensus is required for updates or transactions on blockchains. It refers to the need to validate new data before writing updates of information to the blockchain. Similar to the term "blockchain", there are different types of consensus mechanisms. Early crypto consensus required agreement by the majority of relevant actors on the blockchain as to the status of the ledger, whereas more recent versions of blockchain use distributed consensus mechanisms, relying on a fewer number of nodes required for establishing consensus. Examples of consensus mechanisms include Proof of Work and Proof of Stake.
Cryptography	A method of using algorithms to protect information by having senders make the information unreadable. The recipient must have the right algorithm to reverse the effect and make the information readable. For example, an email is readable to the sender and the recipient, but while the information is in transit it is very difficult to interpret by any intercepting third party.
Decentralised Technology	Blockchain uses decentralised technology - there is no central governing authority that manages a blockchain network. Decentralisation means the network may be more secure and less likely to break down. A centralised database stored on a server may be a target for hackers. In order to attack a blockchain network, a huge amount of computational power and resources is required (at least 51% of all power in the network). Blockchain doesn't rely on third parties, it is maintained by the network participants.

Distributed Ledger Technology (DLT)	DLT is the infrastructure and protocols (rules) that allow independent computers (nodes) in different locations to propose and validate transactions. DLT systems and processes allow computers to update records in a synchronised way across a DLT network. A distributed ledger is a common record of information that is shared across multiple locations. DLT is formed of a network of independent computers – if a record is updated on one of those computers, then the records across all the computers that are part of the network also get updated. DLT allows information, including records of transactions, to be stored securely using cryptography. The protocols are the rules of the distributed ledger. They define how records are added, validated and synchronised. Protocols also validate the rights of a digital asset.
Encryption	The process of converting information or data into code in order to prevent unauthorised access. Encrypting data allows users to protect information by using cryptography or other mathematical modes to scramble it in such a way that only parties who have access to the key can use the data (in this case cryptocurrency funds).
Immutability	Blockchain is immutable and transparent - when the data on the network is recorded, it becomes visible to other participants and cannot be changed. All blocks are connected to each other. No-one can delete, edit, revise, rewrite, update or undo, any of them. Every node (participant) of the network has a copy of the digital ledger. Adding new transactions requires validation, following an agreed consensus mechanism.
Mining	The process by which new cryptoassets enter into circulation and new transactions are confirmed by a blockchain network, it is performed using sophisticated hardware that solves a complex computational maths problem. When a problem is solved, the miner is awarded the next block of cryptoassets and the process recommences with a trickier problem. Computers that verify transactions on the blockchain ledger in exchange for a reward based in cryptocurrency.

Minting	An alternative to mining, the process by which assets are written to a blockchain, where the writer of the asset is a pre-determined trusted entity. In certain use cases, such as an ecosystem of banks, minting is preferred due to performance and power consumption requirements.
Node (Validator)	In the context of cryptocurrency and blockchain, a node is a computer that assists in the running of the blockchain's software so that transactions or transfers can be validated and then recorded. In computer science generally, a node is a device integral to a larger network.
Permissioned DLTs	Permissioned DLTs fall in between private and public DLTs. It requires permission to enter the network but then participants can take part in any activities.
Private DLTs	Private DLTs allow for participants that have been approved by a central authority that has control over the network and its design. Information is not usually available outside the network.
Private Key	The private key is a secret key and must remain known only to the recipient. A private key is somewhat comparable to a pin or verification code. Transactions are conducted using a private key in conjunction with the public key. This grants access to the value of the transaction the payer has stated which is held on the funds you have on a platform. The key pair is mathematically related so that whatever is encrypted with a public or private key can only be decrypted by its corresponding counterpart.

Proof of Stake (PoS)	PoS is a type of consensus mechanism that uses a fraction of the energy of proof of work. In essence, holders of a network token 'stake' (lock their tokens on the blockchain) for the opportunity to be picked to validate a block and thus receive transaction fees as a staking reward. Bad actors risk a portion or all of their locked tokens being taken away while those whose nodes are not online 24/7 and ensuring resilience are also penalised. There may be broader governance considerations with PoS (e.g. 'the 51% problem' where a group or individual owns more than 50% of the cryptocurrency and controls more than 50% of miners, giving them the control to alter the blockchain network).
Proof of Work (PoW)	PoW is a consensus mechanism that is used to validate new information added to a distributed ledger technology platform. It involves solving complex mathematical puzzles, using cryptography, and can use significant computer power (and thus energy consumption). Typically, the validator is rewarded, for example with the cryptoasset that is being used for the transaction it is validating.
Smart Contract	A smart contract is a self-executing contract with terms of the agreement between parties being directly written into lines of code. The code and the agreements exist across a distributed blockchain network and so there are no intermediaries.
Tokenisation	The transformation of the rights to an asset into digital form (tokens). To note, tokenisation can exist separate from DLT. For example the digitisation and tokenisation of traditional securities.
Zero Knowledge Proof	A method for proving that a statement is true without offering further information to the verifier, e.g. confirming an ID without sending over passport or driving licence documents. These are a breakthrough in cryptography in that they help provide higher standards of data protection.

Part B - Digital Currencies and Cryptoassets

Algorithmic Stablecoin	Algorithmic stablecoins do not aim at stabilising their value by referencing one or several other physical assets. Algorithmic stablecoins aim at maintaining a stable value, via protocols, that provide for the increase or decrease of the supply of such cryptoasset in response to changes in demand. The algorithm (a type of mathematical formula) is executed by a computer or smart contract and is the source of stability behind the stablecoin operating by adding or subtracting tokens into the market to maintain a stable value.
Asset-Referenced Tokens	A subset of exchange tokens which include commodity-linked tokens and crypto-backed tokens. Asset-referenced tokens aim at maintaining a stable value by referencing several currencies that are legal tender (typically known as fiat-currency), one or several commodities, one or several cryptoassets or a basket of such assets.
BigTech	Large, well-established technology companies which provide financial products and services or products that are very similar to financial products and can include crypto products.
Bitcoin	The first decentralised cryptocurrency using blockchain technology. It used open-source, peer-to-peer technology to operate with no central authority of banks. Instead, managing transactions and the issuing of bitcoins is carried out collectively by the network.

Central Bank Digital Currency (CBDC)	CBDCs are a digitally native form of Central Bank-issued money. There are a variety of different types of CBDCs however it is to be envisioned by most to be a new form of central bank money. CBDCs are a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value.
Cryptoasset	A digital representation of value or contractual rights, using some form of Distributed Ledger Technology, that can be transferred, stored or traded electronically utilising cryptography. It is said cryptoassets are decentralised since the issuance and transfer of the currency is not controlled by any central bank or actor. Examples of cryptoassets include NFTs and cryptocurrencies.
Cryptoasset Exchange Providers	These are firms which exchange, arrange or make arrangements (whether automated or otherwise) for the exchange of money (i.e. fiat currency) and cryptoassets; or of one cryptoasset for another.
Cryptoasset Service Provider (CASP)	Any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis. Cryptoasset services include the provision of an exchange, including automated processes, enabling the exchange of cryptoassets for money or for one cryptoasset for another cryptoasset and providing custodian services, e.g. through the provision of a custodial wallet to hold the cryptocurrencies.
Crypto-backed Tokens	A subset of asset-referenced tokens which reference their value in relation to other cryptoassets.
Cryptocurrency	A digital currency, using some form of Distributed Ledger Technology, in which value is transferred, stored or traded electronically on a decentralised system using cryptography, and not any central bank or actor. A cryptocurrency is a subset of cryptoasset.

Digital Currency	Also known as virtual currency. A digital representation of value exists electronically and functions as a medium of exchange, a unit of account and a store of value. They are not issued or backed by government or other public authority (unlike Fiat currency) but are issued and usually controlled by their developers and used and accepted among the members of a specific virtual community as a means of payment that can be transferred, stored or traded electronically. Digital currencies include credits for computer games used as a medium of exchange within the computer games where these are issued (and therefore have no economic value), as well as e-money and cryptocurrency. Although initially designed to be used to make payments, many are now held as speculative assets by investors.
Digital Wallet	Digital wallets (or virtual / crypto) wallets. A digital wallet allows you to send, receive, view and spend cryptocurrency and other forms of digital money. A digital wallet isn't quite the digital equivalent of a wallet. It doesn't store your cryptocurrencies or digital money, rather a digital wallet securely stores the private keys and public keys needed to buy, sell and use cryptocurrencies or digital money. To appreciate why this is, unlike physical cash, cryptocurrencies (digital money) never leaves the platform on which it is issued; rather, details of ownership are recorded on the platform, through Public and Private keys of a user that are required to perform a transaction. Thus, a holder needs to have proof of ownership to be able to access and transact the cryptocurrency or digital money.
Direct CBDC	A Central Bank Digital Currency that is issued and distributed via the Central Bank itself. The Central Bank is in charge of all the administrative processes, including account opening and KYC due diligence, customer service and wallet provision and maintenance.

E-money Tokens	E-money is a digital representation of money held in an account and, where the e-money has been tokenised using distributed ledger technology, it is called an e-money token. E-money tokens are primarily used for making payments and are not tradable on an exchange, unlike cryptocurrencies and stablecoins.
Exchange Tokens	Exchange tokens function just like any other cryptocurrency. However, exchange tokens are cryptocurrencies that are issued (minted) by the cryptocurrency exchange platform themselves. Exchange tokens can be bought and traded on secondary markets/different exchanges but must be issued by a centralised cryptocurrency exchange (a company with an executive team that maintains an order book of buyers and sellers).
Governance Tokens	A subset of utility tokens which are used solely by holders to vote on a blockchain or network's decisions, but do not provide any kind of exclusive perks or discount.
Indirect CBDC	A Central Bank Digital Currency that is issued by the Central Bank however distribution responsibilities, including wallet creation, user onboarding, KYC checks and customer service are provided by other banks or regulated intermediaries, called 'Payment Interface Providers (PIPs)'.
Non-Fungible Tokens	These are cryptoassets that represent the proof of title to a unique digital asset. They are digital tokens that are the equivalent of certificates of ownership for virtual (and sometimes physical) assets, such as works of art, collectibles or music.
Payment Interface Provider (PIP)	PIPs would potentially act as intermediaries and support the Central Bank with the distribution of a CBDC, including client onboarding, wallet provision and customer service.
Private Money	Private money or commercial bank money is held in the form of deposits and used for lending by a Commercial Bank.
Public Money	Money that is issued and held by the Central Bank.

Retail CBDC	A retail CBDC (rCBDC) is a type of CBDC that is solely available for businesses and individuals to hold and use for retail transactions. Effectively a digital asset version of everyday physical central bank-issued cash.
Stablecoin	A stablecoin is a digital exchange token with a value that stays close to a specific reference, thus providing the holder with a right to redeem into the specified asset. The most common example is a currency (commonly known as fiat-backed) stablecoin that allows the holder to redeem into a currency such as US Dollars or Pound Sterling. Because a stablecoin can be exchanged into an asset, the price of the stablecoin tends to track that of the asset. For example, a stablecoin that can be redeemed into £1, will generally be valued close to £1. However, this 'stable' value relies on the ability of the stablecoin issuer to redeem; if the issuer is unable to redeem or is perceived not to be able to do this, the value of a stablecoin can rapidly fall. Stablecoin issuers have a variety of methods to financially support their ability to redeem. For example, some stablecoin issuers hold assets ("asset-backed stablecoins", such as cash or bonds, to support redemption). Other stablecoins issuers use computer programs ('algorithms') to control supply in order to maintain a stable value, although this does not in itself support redemption. These are called algorithmic stablecoins.
Synthetic CBDC	A synthetic CBDC (sCBDC) combines elements of both central bank-backed digital currencies and private digital assets. Unlike a traditional CBDC, which is issued and fully controlled by a central bank, a synthetic CBDC involves a collaboration between the central bank and private sector entities. In this model, the central bank provides a digital token that represents the nation's currency, while the private sector is responsible for managing the digital ledger and distribution system. This approach allows for the efficiency and innovation of the private sector to be combined with the stability and trust associated with a central bank.

Tokenised Deposits	Tokenised deposits are the digital representation of existing bank liabilities, held by licensed credit institutions. Tokenised deposits are tied to existing bank deposits and are recorded on distributed ledgers. Tokenised deposits function within the existing traditional banking systems and help to transfer value directly between bank accounts.
Tokens	Tokens are cryptoassets that operate on an existing blockchain network. Tokens are designed to be supported by a specific blockchain network rather than establishing their own new blockchain. For example, the Ethereum Blockchain Network (with its smart contract compatibility) is able to record the transactions of multiple different types of tokens. There is only one 'native coin' to the network and that is the Ether cryptocurrency. All the other cryptoassets recorded on the Ethereum Blockchain Network are 'tokens'.
Utility Tokens	Utility tokens are a sub-category of cryptoassets that intend to provide digital access to a specific good or service that is only accepted by the issuer of the specific utility token. Utility tokens can have non-financial purposes related to the operation of the issuer's digital platform and digital services. For example, digital advertising or digital file storage. They do not provide the rights or features associated with a security token (e.g. share or ownership rights), and do not function as a means of payment - though they can be traded on cryptoasset trading venues for investment purposes.
Wholesale CBDC	A wholesale CBDC (wCBDC) is a type of CBDC that central banks, commercial banks and other institutions (that have accounts with a central bank) can use. wCBDCs are designed to enable settlement between banks and other institutions directly. This type of CBDC is not available to the general public.

Part C - The Digital Currency Ecosystem

Cryptocurrency Native	A crypto native is a person or business that has its roots in decentralisation, blockchain, distributed ledgers etc. at the end of the spectrum, whilst at the other it refers to those whose political philosophy is maybe libertarian and in some cases even peacefully anarchic. (NB There is no settled definition and meaning tends to be context specific).
Custodian Wallet Providers	These are firms that provide services to safeguard, and to safeguard and administer, cryptoassets or private cryptographic keys on behalf of its customers, or which hold, store and transfer cryptoassets. They need to be registered with the FCA for this business.
DAO	Decentralised Autonomous Organisation, initially developed for creating a trustless organisation, now refers to any community led trustless ecosystem built on blockchain (See also 'Consensus' definition).
DeFi	Short for "decentralised finance", an umbrella term for the provision of financial applications that is achieved directly between two parties without the need for financial intermediaries, that often uses technology based on distributed ledgers and 'smart contracts'. The system removes the controls that the traditional finance sector has on money, financial products, and financial services since they are replaced by code for verification of provenance, execution of contractual terms and settlement between counterparties.

Digital Settlement Asset (DSA)	According to the Financial Services and Markets Act, a DSA means a digital representation of value, whether or not cryptographically secured, that – (a) can be used for the settlement of payment obligations, (b) can be transferred, stored or traded electronically, and (c) uses technology supporting the recording or storage of data (which may include distributed ledger technology. A DSA is a digital asset whose primary utility is for payment and settlement. Essentially these are digital assets that are forms of money (digital money) or similar to money (cryptocurrencies). This does not mean that digital settlement assets cannot be used for other purposes, for example holding cryptocurrencies for investment purposes.
Fiat currency	Central Bank or government-backed money, e.g. Pound Sterling.
Fiat on ramp/ off ramp	Payment rails that facilitate fiat money getting to cryptocurrency exchanges to convert to cryptocurrency, and vice versa.
FinTech	An umbrella term describing technology-enabled innovation in financial services, regardless of the nature of size of the entity providing the services, that could result in new business models, applications, processes and products.
Fungibility	Within the context of digital money, fungibility is how replaceable a currency is with another currency.
Initial Coin Offering (ICO)	Also known as a token sale or a coin sale. A digital way of raising finance online from the public using digital currency and DLT. The issuer issues a proprietary digital coin or token against payment in a cryptocurrency, like Bitcoin or Ether. The digital coin or token issued is related to a specific firm or project. It may represent a share in a firm, a pre-payment voucher for future services or have no discernible value at all. ICOs vary widely in design and types and are often projects that are in a very early stage of development.

Interoperability	Interoperability within the context of digital money relates to how the different banking and payment systems are able to interact with each other given the level of technical compatibility.
MiCA	The European Union's Markets in Cryptoassets Regulation. This is a set of rules covering crypto-assets which have been agreed by the European Parliament. It aims to regulate the crypto-asset environment in-line with other financial assets and services and to protect consumers.
P2P	Peer to Peer - participants are connected to each other with no central control or intermediary. This term can relate to transactions and to the architecture itself.
Virtual Asset Service Providers	A VASP is any natural or legal person who, as a business, conducts activities or operations for or on behalf of another natural or legal person such as: - exchange between virtual assets and fiat currencies; - exchange between one or more forms of virtual assets; - transfer of virtual assets; - safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; - participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset VASPs include cryptocurrency exchanges and digital wallet providers, and even some financial institutions, including banks dealing with crypto assets.

Web3	Web3 is the next generation of the internet, based on decentralised technologies like blockchain. It empowers users with data ownership and enables new types of applications and services through the use of digital currencies and tokens. These digital assets play a vital role in facilitating value exchange, enabling economic models, and promoting user engagement within the decentralised ecosystem.

This document contains the opinions of the parties involved in its collation and should not be construed as anything more. It is not advice and should not be treated as such, nor should it or its contents be relied on in any manner. No guarantees are given of completeness, accuracy, usefulness or timeliness. The terms covered in this document are not exhaustive and nor are they intended to be. Not everyone will share our opinions on the terms defined in this agreement. None of the parties involved in the production of this document bear or assume any responsibility or liability for any errors or omissions.

Acknowledgements

AUTHORS

City of London Corporation	www.cityoflondon.gov.uk
Digital Pound Foundation	www.digitalpoundfoundation.com
The Payments Association	www.thepaymentsassociation.org
TheCityUK	www.thecityuk.com
UK Finance	www.ukfinance.org.uk
Cummings Pepperdine	www.cummingspepperdine.com
Greengage	www.greengage.co

CONTRIBUTORS

Clifford Chance	www.cliffordchance.com/home.html
CMS	www.cms.law/en/gbr

REVIEWERS

Members of the authoring associations	
Innovate Finance	www.innovatefinance.com
Crypto UK	www.cryptouk.io
The Realization Group	www.therealizationgroup.com