VERSION 1.0

COALITION OF AUTOMATED LEGAL APPLICATIONS

SUMMARY

The following definitions are not a reflection of the current law in any particular jurisdiction. They represent the Working Group's suggestions of accurate techno-legal descriptions for various key terms that are used in the regulatory dialogue about distributed ledger technology.

While the definitions are intended to be technically accurate, the focus is to provide standardized terminology for the commercial application or use of the technology. The objective is to promote the creation of activities-based regulatory frameworks that avoid the 'blanket-approach' to regulating the technology and accurately assesses the risk of particular commercial activities.

GLOSSARY

TERM	DEFINITION/CHARACTERISTICS
Cold Storage	A process where private keys are both generated and stored in offline environments. Storage may be on paper or saved electronically as a text file.
Consensus	A term that refers to the way in which transactions on a Distributed Ledger are confirmed, which may include proof-of-work (Mining), proof-of-stake, Byzantine agreement system, and Federated Byzantine Agreement, among other variations.
Control	The ability to unilaterally execute a transfer on a Distributed Ledger, which may involve holding a sufficient number of keys. *Note: Some key-holders in an m-of-n Multi-Sig transaction may have negative control. They are able to prevent a transfer from happening, but they are unable to unilaterally execute a transfer.* *Note: Technology enables different arrangements and numbers of keys and access control, allowing control to be contractually mandated.*
Conversion Service	A platform or service where operator is buying/selling cryptocurrency or crypto-assets directly to/from the Client.
Crypto-asset	A claim/right to something of value, represented by a crypto-token (e.g. an ounce of gold, the deed to a car). *Note: The FinCEN definition of cryptocurrency in the United States may include some crypto-assets.*
Crypto-token	The unit of account on a Distributed Ledger.

Cryptocurrency	A crypto-token used as a currency, medium of exchange, or a store of monetary value. *Note: in the United States, FinCEN considers cryptocurrency to have the following characteristics:* • *Issuance;* • *Redemption or withdrawal mechanism; or* • *Sale of the crypto-token.*
Cryptocurrency Marketplace	A platform which connects buyers and sellers of cryptocurrency and clears and settles trades of cryptocurrency.
Cryptosecurity	A security issued as a crypto-token. *Note: 'Cryptosecurity' is used to capture scenarios where the token is intended to be issued as a security.*
Custodial Control	Control of a crypto-asset or cryptocurrency other than by the owner.
Digital Currency	A digital representation of value that is used as a currency, medium of exchange, or a store of monetary value, including Cryptocurrencies and Virtual Currencies. *Note: There is a difference between digital currency and virtual currency.*
Distributed Application	A software application where functions are executed by Consensus. *Note: some Distributed Applications are commonly referred to as Smart Contracts. However, see below for the definition of Smart Contract. Distributed Applications include crowdfunding and marketplace applications.*
Distributed Ledger	A database maintained (updated) and stored by multiple independent parties. Transfers on a distributed ledger are generally made final when the ledger is updated. *Note: A Distributed Ledger can be permissioned or permission-less. Permission refers to how the system works with respect to validating transactions. In a permissioned system, you need to be vetted to validate a transaction.*
Escrow	The holding of client Funds with the ability to unilaterally execute transfer of those Funds, but only according to specific instruction from the client.

Exchange	A platform with a built in settlement process where clients buy and sell cryptocurrencies or crypto-assets from one another, which commonly involves provision of Escrow services.
Fiat Currency	A medium of exchange that has been formally adopted by a government.
Funds	A broad term meant to refer to any medium of exchange, including Fiat Currency, Digital Currency, Cryptocurrency and Virtual Currency.
Genesis Block	The initial state of the Distributed Ledger.
Hierarchical Deterministic (HD) Wallet	A wallet where there is a hierarchy of keys. The “core secret” initial key generates all the other keys.
Hosted Wallet (Service controlled)	Software mechanism for managing private keys where the service hosts and Controls the private keys and acts on instruction from the client.
Hosted Wallet (client controlled)	Software mechanism for managing private keys that is hosted by a third party service, but the client maintains exclusive Control of private keys.
Hot Wallet	A software mechanism for managing private keys that is in some way connected to the Internet. As opposed to keys stored in a “cold storage” environment, keys managed by a hot wallet can be instantly used to sign transactions.
Issue	There is tension between the legal and technical understanding of what it means to “issue” a crypto-token. Legal definitions of “issuance” often refer to the concept of circulation, distribution and dissemination or otherwise making a crypto-token available. However, the technical process for “issuing” a crypto-token on a decentralized platform is significantly different. For example, a Distributed Ledger protocol may “issue” tokens to miners or validators as a reward for validating transactions on the platform (e.g. bitcoin). Validators in a consensus protocol issue tokens for their participations in the consensus protocol. It may also involve the creation of a script that other people may use to generate a genesis block. From this point, the protocol will self-issue the crypto-tokens to miners or validators as a reward for validating transactions on the platform (e.g. bitcoin).

Key Holder	A person or service which holds one or more private keys. *Note: A person or service may hold another person's private keys for a number of purposes (e.g. redundant backup, validation) but will not always hold sufficient keys to have positive or negative Control (e.g. Multi-Sig)*
Marketplace	A platform which connects buyers and sellers of goods and services but does not clear and settle these trades. *Note: This may or may not involve the buying and selling of cryptocurrencies.*
Mining	A method for reaching Consensus whereby the computational effort by which transactions on a proof-of-work Distributed Ledger are confirmed and added to the ledger. Computers engaging in mining are called "miners".
Mining Pool	An arrangement in which two or more miners "pool" their computational (hashing) power together to increase their chances of confirming the next block of transactions before another miner or mining pool.
Multi-Sig(nature)	A software mechanism requiring multiple keys to execute a transfer on a Distributed Ledger (e.g. 2-of-3, or 3-of-5).
Non-hosted Wallet	A software mechanism for managing private keys that is hosted and run locally by the client.
Smart Contract	A distributed application that has the requisite legal requirements to be recognized as a contract.
Virtual Currency	A digital representation of value that is centrally issued and controlled by the issuer. *Note: In the United States, FinCEN uses the term "Virtual Currency" more broadly than it is used in this glossary. Specifically, FinCEN's definition of Virtual Currency refers to both centralized and decentralized virtual currency, cryptocurrency, and crypto-assets.*
Wallet	A software mechanism for managing private keys associated with Crypto-tokens.

A PROJECT BY

BLOCKCHAIN WORKSHOPS

WORKING GROUP CONTRIBUTORS

Amor Sexton, Juan Llanos (Multiple Startups), Tim Swanson (R3CEV), Richard Levin (Bryan Cave), Erik Voorhees (Shapeshift.io), Ryan Singer, Byron Gibson (Mirror), Jonathan Levin (Chainalysis), Jillian Friedman (Friedman Law), Reuben Bramanathan (Coinbase), Lowell Ness (Perkins Coie), Dax Hansen (Perkins Coie), Carla Reyes (Perkins Coie), Andrew Beal (Crowley Corporate Attorneys), James Smith (Elliptic), Ola Doudin (BitOasis), Amy Kim (Buckley Sandler), Angus Champion de Crespigny (Ernst & Young), Pamela Morgan (Empowered Law/Third Key Solutions).

THE BLOCKCHAIN WORKSHOPS ARE SUPPORTED BY OUR ACADEMIC PARTNERS

UCL

cnrs dépasser les frontières

Berkman The Berkman Center for Internet & Society at Harvard University

CERSA

mit media lab

STANFORD UNIVERSITY

香港科技大學 THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

WWW.COALA.GLOBAL