|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | FG-AI4H-F-025-A01 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | Plenary |  |
| **DOCUMENT** |
| **Source:** | FG-DLT |
| **Title:** | Updated baseline text: D1.1 - Distributed ledger technology terms and definitions |
| **Purpose:** | Discussion |
| **Contact:** | Heung Youl Youm Soonchunhyang Univ.Korea (Republic of)  | Tel: +82-41-530-1328Fax: +82-41-530-1494E-mail: hyyoum@sch.ac.kr  |
| **Contact:** | Mee Yeon Kim Soonchunhyang Univ.Korea (Republic of)  | Tel: +82-41-530-1328Fax: +82-41-530-1494E-mail: 17kmy@sch.ac.kr  |
| **Contact:** | Skylar HurwitzJeluridaSwitzerland | E-mail: skylar@jelurida.com  |

|  |  |
| --- | --- |
| **Keywords:** | Terms and definitions; ledgers; distributed ledger technology; |
| **Abstract:** | This document provides an outcome document for D1.1 - Distributed Ledger Technology terms and definitions.  |

This document provides an outcome document for D1.1 - Distributed Ledger Technology terms and definitions at the 1-4 April 2019 Madrid FG DLT meeting. This document was updated based on DLT-I-169. The following updates and suggestions were made at the meeting:

* The clause 6.24 on mining and the clause 6.40 on wallet were updated.
* Comments on clause 6.35 on smart contract and clause 6.39 on tokenomics were presented for consideration by future conference calls.
* Comments on clause 6.7 on BFT and clause 6.8 on compliance were presented for consideration by future conference calls.
* Several clauses requiring attentions highlighted in yellow were presented – some are for further consideration (e.g., node) and contributions are invited.
* A new term “blockchain as a service” was added for consideration by future conference calls.
* Suggested edits from Skylar Hurwitz were accepted, and comments from Skylar Hurwitz were added as NOTE for further consideration.

The plan is to hold at least 3 conference calls after the April 2019 FG DLT meeting to finalize this document until end of July, 2019. The intent is to delete all NOTEs referencing some document in the final version of this document, which will be submitted to the final FG DLT meeting, Geneva, 29 July – 1 August 2019.

Annex A: Base document

Baseline distributed ledger technology terms and definitions

# 1 Scope

This document contains a baseline set of definitions of terms commonly used in distributed ledger technology (DLT). The definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity. The rationale for some of the key terms/definitions may be included in Annex A.

# 2 References

The following ITU-T Recommendations and other references through reference in this text, constitute provisions of this document.

# 3 Definitions

This clause is intentionally left blank.

# 4 Abbreviations and acronyms

This Document uses the following abbreviations:

DLT Distributed Ledger Technology

PII Personally Identifiable information

# 5 Conventions

This clause is intentionally left blank.

# 6 Terms and definitions

**6.1 Account**:Representation of an entity whose data is recorded on a distributed ledger

NOTE – [b-ISO/TC 307] defines ‘DLT account’ as “representation of an entity whose data is recorded on a distributed ledger,” with a note “An account often holds smart contracts or digital assets.”

Editor’s NOTE – The definition will be generalized later.

**6.2 Address:** Identifier for entity(ies) performing transactions or other actions in a blockchain or distributed ledger network.

NOTE – **[b-Y.2091]**:An address is the identifier for a specific termination point and is used for routing to this termination point.

NOTE – [b-ISO/TC 307] defines ‘address’ as “identifier for accounts participating in a transaction in a blockchain or distributed ledger network” and added a note “The identifier may be implemented as a string of alphanumeric characters derived from a user’s public key using a cryptographic hash function and be usedto receive and send transactions on a blockchain or distributed ledger network. It may also be represented as a scannable QR code”

**6.3 Application[b-Y.2091]:** A structured set of capabilities, which provide value-added functionality supported by one or more services.

**6.4 Bitcoin**: An example of a blockchain using Proof of Work.

**6.5 Block**: Individual data unit of a blockchain, composed of a collection of transactions and a block header.

NOTE – A block may be mutable and considered as the digital entity described in clause 3.2.2 in [b-X.1255], however, it can be applied to other networks or other computational facilities.

NOTE – [b-X.sct-dlt] defines ‘block’ as “A data structure for a ledger record containing a set of one or more transactions and a header which contains data including the hash of the previous block in the chain.”

NOTE – [b-X.sa-dlt] defines ‘block’ as “A set of validated transactions” referencing [b-NIST].

NOTE – [b-ISO/TC 307] defines ‘block’ as “data structure comprising transaction records and a block header.” There is an note stating that “Transaction records within a block are sometimes referred to as comprising the body of the block to differentiate them from the block header” for this term.

NOTE – Consider the definition ‘block’ as “Data containing a set of one or more time-stamped transactions and, possibly, additional information.”

NOTE – [b-DIN 16597] defines ‘block’ as “individual unit of a blockchain, composed of a collection of transactions and a block header.”

NOTE – [b-NIST] defines ‘block’ as “A data structure containing a block header and block data.”

**6.6 Blockchain**: A type of distributed ledger which is composed of digitally recorded data arranged as a continuously growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

NOTE – Call for contribution.

NOTE – Consider the definition ‘blockchain’ as “A peer to peer distributed ledger based on a group of technologies for a new generation of transactional applications which may maintain a continuously growing list of cryptographically secured data records hardened against tampering and revision.”

NOTE – Consider the definition ‘blockchain’ as “A model that construct chained-block data structure which cannot be tampered with and can be traced in peer-to-peer networks through transparent and trustworthy rules.”

NOTE – Consider the definition ‘blockchain’ as “A ledger where data is recorded in blocks in such a way that each new block includes information about the previous block.”

NOTE – [b-X.sct-dlt] defines ‘Blockchain’ as “A peer to peer distributed ledger technology for a new generation of transactional applications which maintains a continuously growing list of cryptographically secured data records hardened against tampering and revision. NOTE 1 - Blockchain can help establish trust, accountability and transparency while streamlining business processes.

NOTE - Categorized by types of participants, blockchains can be divided as public blockchains, consortium (or permissioned) blockchains and private blockchains.”

NOTE – [b-X.strdlt] defines ‘Blockchain’ as “The technology underlying bitcoin and other cryptocurrencies—a shared digital ledger, or a continually updated list of all transactions. Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e, without a central repository) and usually without a central authority. [Draft NISTIR 8202]” referencing [b-DFS] and [b-NIST].

NOTE – [b-ISO/TC 307] defines ‘Blockchain(s)’ as “distributed ledger with confirmed and validated blocks organized in an append-only, sequential chain using cryptographic links” with a note, “blockchains are designed to be tamper resistant and to create final and definitive (immutable) records”

NOTE – [b-ISO/TC 307] defines ‘blockchain system(s)’ as “system that implements a blockchain.”

**6.x      Blockchain as a Service (BaaS):** A cloud service category in which the capabilities provided to the cloud service customer are the ability of consensus, smart contract, transaction, crypto engine, block record storage, peer-to-peer connectivity and management using blockchain.

**6.7 Byzantine Fault Tolerance:** Property that enables distributed ledgers to continue operating properly even in cases where intentional malicious activities exist.

NOTE – **[b-X.sa-dlt]**: Dependability of a fault-tolerant distributed computing systems, where components may fail and there is imperfect information on whether a component is failed, or where there are malicious attempts to harm the system or components within the system.

NOTE – [b-ISO/TC 307] defines ‘fault tolerance’ as “property that enables a system to continue operating properly even if some of its components fail”

NOTE – Consider the definition ‘procedure of reaching consensus on the basis of the Byzantine agreement’ as “Consensus procedure based on the Byzantine agreement protocol.”

**6.8 compliance[b-ISO 2394]**: fulfilment of specified requirements

Editor’s NOTE- Please send this term to WG2 and WG4 for the review.

**6.9 consensus:** agreement that a set of [transaction] records is valid

NOTE – [b-X.sradlt] defines ‘consensus’ as “In the case of decentralization, a consensus is reached on transaction events, namely, the validity of a transaction without a central organization.”

NOTE – Consider the definition ‘consensus algorithm’ as “The calculation method used by each node in blockchain system to reach a consensus.”

NOTE – [b-ISO/TC 307] defines ‘consensus’ as “agreement among nodes that a transaction is valid and that there is a consistent set and a guaranteed ordering of the transactions to be stored in the distributed ledger” with a note, “Consensus does not necessarily mean that all nodes agree.”

NOTE – [b-ISO/TC 307] defines ‘consensus mechanism’ as “rules and procedures by which consensus is reached”

Editor Note) This term could be generalized to consider the various consensus protocol.

**6.10 cross-chain interoperability:** The ability of two or more distributed ledger systems to operate with one another.

[Skylar Hurwitz’s comment - Question:

Is this referencing the ability of two different DLT tokens to interoperate with one another (for example, many ERC20s are not compatible with one another, even though they are built on the same blockchain protocol)

OR

Is this referencing the ability of two different DLT protocols to interoperate with one another (Bitcoin to Ethereum)?

Suggestion:

Define 2 terms:

Cross-token interoperability

Cross-protocol interoperability]

**6.11 digital signature[b-ITU-T X.800|ISO 7498-2]:** Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

NOTE – Consider the definition ‘digital signature’ as “Data appended to data units, or cryptographic changes made to data units, which allows the recipient of the data unit to confirm the origin and integrity of the data and protect the data from being forged.”

**6.12 distributed application:** Application that runs in a distributed computing environment.

NOTE – [b-ISO/TC 307] defines ‘distributed application (or ledger application or blockchain application)’ as “application that runs on a distributed system.”

[Skylar’s comment - How do we define “distributed”? The definition for distributed application and distributed ledger both use the word distributed, but there is no definition of this term. What makes something “distributed”?]

**6.13 distributed ledger:** A type of ledger, that is shared, replicated, and synchronized in a distributed manner.

NOTE – Consider the definition ‘distributed ledger’ as “An asset database that can be co-managed and shared across multiple sites, geographies, or networks of multiple agencies.”

NOTE – [b-X.tfspd-dlt], [b-X.stov] and [b-X.sadlt] define ‘distributed ledger’ as “electronic data that has been replicated, shared, synchronized and stored by consensus in physically separate multiple places (e.g. states, organizations, etc.)”

NOTE – Consider the definition ‘distributed ledger technology’ as “A collection of technologies that enable distributed ledgers.”

NOTE – [b-X.srdrm-dlt], [b-X.sa-dlt] and [b-X.das-mgt] define ‘distributed ledger technology’ as “a shared digital ledger, or a continually updated list of all transactions” referencing ITU-T FG-DFS-Glossary. [b-X.sa-dlt] and [b-X.das-mgt] add a note “This is the technology underlying Bitcoin and other crypto currencies.”

NOTE – [b-X.ss-dlt] defines ‘DLT’ as “A peer to peer distributed ledger technology for a new generation of transactional applications which maintains a continuously growing list of cryptographically secured data records hardened against tampering and revision.

NOTE – [b-ISO/TC 307] defines ‘distributed ledger(s)’ as “ledger that is shared and synchronized in a distributed manner.” In addition of that, [b-ISO/TC 307] defines distributed ledger technology, distributed ledger network, distributed ledger system, distributed ledger technology platform, distributed system separately.

NOTE 1 - DLT can help establish trust, accountability and transparency while streamlining business processes.

NOTE 2 - DLTs can be classified three types (i.e. public, consortium and private) based on the relationship of the participants and the way to provide services.”

**6.14 DPoS(Delegated Proof of Stake):** each token holder determines the accounting right of the blockchain by voting, similar to the election of the board of directors. All nodes whose votes exceed the agreed votes become system trustees, forming a “board of directors” and alternately signing blocks. If a director misses the chance to sign a block, the nodes vote for the others. Those directors that miss the chance to sign a block are disqualified and others can join the board.

**6.15 fork:** creation of two or more different versions of a distributed ledger.

NOTE - [NISTIR 8202] defines “A change to blockchain network’s software (usually the consensus algorithm). The changes may be backwards compatible”.

Editor’s note – There are two types forks. See 6.18 and 6.36.

**NOTE - [b-NIST]**: A change to blockchain software and implementation.

NOTE – [b-ISO/TC 307] defines ‘fork’ as “creation of two or more different versions of a distributed ledger.”

**6.16 genesis block:** A block added to the blockchain during the initial data record

**6.17** **governance [b-ISO/IEC 38500]**: system of directing and controlling

Editor’s NOTE- Please send this term to WG2 and WG4 for the review.

**6.18** **hard fork:** Change to the protocol or rules that result in a fork that is not backward compatible.



Figure 1 - hard fork

NOTE – [NISTIR 8202] defines ‘hard fork’ as “A change to a blockchain implementation that is not backwards compatible. Non-updated nodes cannot continue to transact with updated nodes.”

Editor’s note – Call for contribution.

NOTE – [b-ISO/TC 307] defines ‘hard fork’ as “change to the protocol that results in a fork”

**6.19 hash function** **[b-NIST]**: A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and

2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

**6.20 hashing** **[b-NIST]**: A method of calculating a relatively unique output (called a *hash digest*) for an input of nearly any size (a file, text, image, etc.). The smallest change of input, even a single bit, will result in a completely different output digest.

**6.21 immutable** **[b-ISO/TC 307]**: Property of blockchain and distributed ledger systems that ledger records can only be added, but not removed or modified, and are designed not to allow changes to historical data over time.

Editor Note – Call for contribution on this term.NOTE – [b-ISO/TC 307] defines ‘immutability’ as “property of blockchain and distributed ledger systems that ledger records can only be added, but not removed or modified, and are designed not to change over time”

**6.22 ledger**: Information store that keeps final and definitive (immutable) records of transactions.

NOTE – [b-ISO/TC 307] defines ‘ledger’ as “information store that keeps final and definitive (immutable) records of transactions.”

NOTE – Consider the definition ‘ledger’ as “A collection of data stored in a structured electronic form for the purpose of its processing and accounting” on the basis of the terms GOST R 7.0.8-2013

**6.23 Merkle tree[b-NIST]:** A data structure where the data is hashed and combined until there is a singular root hash that represents the entire structure.



Figure 2 - Example of a Merkle tree

NOTE – [b-X.sradlt] defines ‘merkle tree’ as “Merkle tree commonly known as Hash Tree, a tree that stores hash values. The leaves of a Merkle tree are the hash values of data blocks (such as collections of files or files). The non leaf node is the hash of its corresponding sub node concatenation string.”

NOTE – [b-ISO/TC 307] defines ‘Merkle tree’ as “tree in which every leaf node is labelled with the hash value of a data block and every non-leaf node is labelled with the hash - value of the labels of its child nodes”

**6.24 mining[b-X.sct-dlt]**: A reward-seeking /validation activity in some consensus mechanisms (e.g., POW), which operates through certain types of consensus mechanisms.

NOTE – [b-ISO/TC 307] defines ‘mining’ as “reward-seeking activity in some consensus mechanisms” with a note, “Participation in mining is often incentivized by block rewards”

**6.25 node:** Device or process that participates in a distributed ledger network

NOTE – **[b-X.sct-dlt]**: A collection of one or more functions (e.g., routing, the DLT database storage, verification, mining). Nodes connect to others and form a network.

NOTE – [b-X.stov] defines ‘node’ as “server with database which maintains distributed ledger”, while [b-X.strdlt] defines it as “Any computer running distributed ledger technology software is called node.”

NOTE – [b-ISO/TC 307] defines ‘node(s)’ as “device or process that participates in a distributed ledger network” with a note, “Nodes can store a complete or partial replica of the distributed ledger.”

**6.26 participant**: An actor who can access the ledger: read records or add records to.

[Skylar comment - I read this in two different ways with the current grammar. Here are two options with clearer grammar:

Option1: An actor who can access, read, or add records to the ledger.

Option 2: An actor who can access the ledger with reading or writing privileges.]

NOTE – [b-ISO/TC 307] defines ‘DLT user(s)’ as “entity that uses services provided by a distributed ledger system”

**6.27 Peer-to-Peer [b-ISOTC 307]:** relating to, using, or being a network of equal peers that directly share information and resources with each other without relying on a central entity

NOTE - In the context of a distributed ledger system, peers are nodes.

NOTE – [b-X.sradlt]: Peer-to-peer networking (P2P) is an application that runs on a personal computer and shares files with other users across the Internet. P2P networks work by connecting individual computers together to share files instead of having to go through a central server.

NOTE – [b-ISO/TC 307] defines ‘peer-to-peer’ as “relating to, using, or being a network of equal peers that share information and resources with each other directly without relying on a central entity” with a note “In the context of a distributed ledger system, peers are nodes.”

**6.28 permission [b-NIST]**: Intended allowable user actions (e.g., participate, read, write, execute).

**6.29 permissioned ledger**: A ledger where actors must have permission granted by some governance entity(ties) for access and authority to act.

NOTE – When a new record is added, the ledger’s integrity is checked by a limited consensus process.

NOTE – [b-X.strdlt] defines ‘permissioned’ as “DLT systems’ characteristics which nodes need permission to participate the DLT network and/or users need permission to use the DLT service provided by the DLT system.”

NOTE – [b-ISO/TC 307] defines ’permissioned Distributed Ledger System’ as “Distributed Ledger System where permissions are required for some capabilities to use the system or permissions are required for some capabilities to operate the system.”

**6.30 permissionless distributed ledger system [b-ISO/TC 307]**: distributed ledger system where permissions are not required to use or operate the system.

NOTE – A good example of permissionless ledger is the Bitcoin and Ethereum blockchains, where any user can join the network and start mining.

NOTE – [b-X.strdlt] defines ‘permissionless’ as “DLT systems’ characteristics which nodes and users do not need any permission to participate the DLT network and use the DLT services provided by the DLT system.”

NOTE – [b-ISO/TC 307] defines ‘permissionless distributed ledger system’ as “distributed ledger system where no permissions are required to use or operate the system.”

**6.31 proof of work**: consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to correctly verify.

NOTE – Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hash cash proof of work system.

NOTE – Consider the definition ‘proof of work’ as “The consensus procedure based on solving a certain problem with a given level of computational complexity, while the correctness of the received response can be confirmed by the validator. As a rule, verification of the correctness of the solution is effectively a solvable problem”

Editor’s NOTE-FG-DLT WG3 defines the same term as “commonly known as mining. PoW can be simply understood as providing a proof that you have done a certain amount of work. PoW requires the node to carry out a certain amount of computation to obtain the accounting right, which means that it takes a certain amount of time to be consumed by the computer and calculates a verifiable result through the mathematical operation. The node sends the data that needs to be recorded in this round. After verification, the other nodes in the whole network store the data together.”

**6.32 proof of stake**: consensus process, where an existing stake in DLT system (e.g. the amount of that currency that you hold) is used to reach consensus.

Editor Note) The terms for other consensus mechanisms such as PBFT which are used in the current well known platforms should be added. It is agreed that the terms definition related to specific brand names should be avoided.

NOTE – Consider the definition ‘proof of stake’ as “The consensus procedure based on estimating the number of conventional units of the Information system that are associated with a user at a certain point in time”

Editor’s NOTE – FG-DLT WG3 defines the term as “PoS allows the so-called ‘token holders’ to replace the miners, Accountant is the holder of relevant tokens, and accounting right is their ‘Stake’. A typical PoS reduces the difficulty of mining in equal proportion to the percentage and time tokens that each node occupies in order to find the ‘verifiable result’ and determine the ownership of accounting rights faster.”

**6.32 Public key cryptography [b-ISO/IEC 2382]:** Cryptography in which a public key and a corresponding private key are used for encryption and decryption, where public key is disseminated, and private key is known only to the key owner.

NOTE – Users can digitally sign data with their private key, and the resulting signature can be verified by anyone using the corresponding public key.

**6.33 public distributed ledger system**: Distributed ledger system in which any node (device or process) can participate in the operation of the system

NOTE – [b-ISO/TC 307] defines ‘public distributed ledger system’ as “distributed ledger system in which any node (device or process) can participate in the operation of the system” and ‘public user distributed ledger system’ as “distributed ledger system in which any user can use the system.”

**6.34 private distributed ledger system**: Distributed ledger system in which a controlled and limited set of nodes participate in the operation of the system

NOTE – [b-ISO/TC 307] defines ‘private distributed ledger system’ as “distributed ledger system in which a controlled and limited set of nodes participate in the operation of the system” and ‘private user distributed ledger system’ as “distributed ledger system in which a controlled and limited set of DLT users can use the system”

**6.35 smart contract**: Computer program recorded on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and invoked by specific applications..

Editor Note) This was updated to reflect the comment at the May 2018 FG-DLT meeting.

NOTE – Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

NOTE – Consider the definition ‘smart contract’ as “A contract defined in digital form that automatically enforces the terms.”

NOTE – [b-X.sradlt] defines ‘smart contract’ as “In a smart contract approach, an asset or currency is transferred into a program, and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof.”

NOTE – [b-X.das-mgt] defines ‘smart contract’ as “a computer program that is part of distributed ledgers to directly controls the transfer of digital assets or equivalents between stakeholders under certain conditions”

NOTE – [b-X.strdlt] defines ‘smart contract’ as “A smart contract is a collection of code and data that is deployed with a set of rules to which parties involved agreed to interact with each other in a network.”

NOTE – [b-ISO/TC 307] defines ‘smart contract’ as “computer program recorded on a distributed ledger system wherein consensus about the effects of any execution of the program is recorded on the distributed ledger system. Note 1 to entry: A smart contract may or may not be intended to represent terms in a contract in law nor be legally recognized. Note 2 to entry: This definition considers smart contracts only in the context of distributed ledger systems. It is recognized that smart contracts are not restricted to distributed ledger systems and the term may have a different meaning in other contexts. A definition was proposed by Nick Szabo in 1994. Under this definition a smart contract may also run outside of distributed ledger systems as a contract automation tool that could be run on any computer system which 1) records contractual activities and related transactions and 2) may support automatic execution of certain transactions.”

NOTE – Consider the definition ‘smart contract / chaincode’ as “a set of conditions and a sequence of actions described in accordance with Information system policies and procedures. The fulfillment of all agreed conditions, depending on the specific state (states) of the Information system (including a result of checking external conditions with respect to the Information system), entails the automatic execution of a predetermined sequence of actions. The execution of this sequence of actions, in turn, also leads to a change in the state of the Information system”

**6.36** **soft fork**: Change to the protocol or rules that result in a fork that is backward compatible.



Figure 3 - soft fork

NOTE – [b-ISO/TC 307] defines ‘soft fork’ as “A soft fork is backward-compatible; that is, DLT nodes running new version of the consensus mechanism will recognize as validated ledger records and blocks from DLT nodes running older versions. A series of soft forks can become a hard fork by default..”

NOTE – [NISTIR 8202] defines ‘soft fork’ as “A change to a blockchain implementation that is backwards compatible. Non-updated nodes can continue to transact with updated nodes.”

**6.37 sub-distributed ledger[b-ISO/TC 307]**: Logically separate set of transaction records within the same DLT system that create a virtual chain using cryptographic links.

NOTE – [b-ISO/TC 307] defines ‘subchain’ as “logically separate set of transaction records within the same blockchain system that create a virtual chain using cryptographic links. Note 1 to entry: A subchain may also be known as a channel. Note 2 to entry: Each subchain may be owned by a different entity and may be accessible to a different set of DLT users. Nodes may be set up so that some nodes participate in certain subchains and not in other subchains. The result of this configuration is that the distributed ledger on some nodes contains transactions for that subchain while the distributed ledgers on other nodes do not.”

**6.38 token[b-ISO/TC 307]**: digital asset held within a distributed ledger system.

NOTE – [b-ISO/TC 307] defines ‘token’ as “representation of a digital asset using metadata where cryptocraphic techniques are used to regulate the generation of the digital asset and to verify transfer of ownership or other state changes to the status of the digital asset. Note 1 to entry: A token is typically owned by the holder of an associated private key, which can be transferred by using the private key. Note 2 to entry: A token includes metadata that describes the digital asset or other form of value or permissions.”

**6.39 tokenomics:** economics of a DLT based token

Editor’s NOTE – Please send WG3 for the review

NOTE-Please refer those two description 2)Tokenomics is a framework for how digital tokens are used by blockchain projects and other innovative organizations. Synonym include token economics, and economics of tokenization ( <http://cryptocapitalnews.com/tokenomics-101-understanding-token-sales-and-other-new-models-of-blockchain-based-financing-for-the-new-economy/>

NOTE – need to definition of **token ecosystem** (Lisa will contribute definition)

Editor Note – Call for contribution on this term

**6.40 wallet:** Software and/or hardware used to generate, manage and store both private and public keys and addresses, which enable DLT users to transact. Some wallets may interact with smart contracts and allow single and/or multi-signature.

[NOTE- paper wallet is one type of wallet, which contains public key and/or private key, being printed out onto paper.]

[Sklar comment - In WG3, we must note whether project governance is through Law/agreement or through Tokenomics. Here in this section, the tokenomics definition is currently written in a broad way that would seem to apply to all DLT systems; however, WG3 implies tokenomics as relevant only to public networks. How can we align the terms across these sections?]

Editor Note) It could be updated to consider the hardware wallet. Need to clarify whether to consider “paper wallet” in the definition of “wallet” [at Rio FG DLT meeting].

Editor NOTE- Please consider a comment that paper wallet can be used with any system. It is generally used for backup.

Editor’s NOTE – Please consider that there is web wallet which may not be categorized into hardware or software wallet.

NOTE – [b-ISO/TC 307] defines ‘wallet’ as “application used to generate, manage and store private and public keys. Note 1 to entry: A wallet can be implemented as a software or hardware module. Note 2 to entry: In some cases, a wallet can be used to generate, manage and store other crypto-assets.”

Editor note) the terms on mining, confirmation, token should be defined.

Editor Note) The terms and definition in TC 307 should be reviewed for further addition and to avoid significant inconsistence.

Appendix I

Key points and rationale for DLT basic terminology

 (To be provided)

Editor Note) The contribution for this Appendix I are asked from members of this FG.

Appendix II

Comparative analysis of major terms definitions

|  | [b-BB] | [b-BGB] | [b-BBT] | [b-BTG] | [b-BBG] | [b-X.1255] | [b-NIST] |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Botcoin | The specific collection of technologies used by Bitcoin’s ledger, a particular solution. Note that the currency is itself one of these technologies, as it provides the miners with the incentive to mine. | a cryptocurrency that runs on a (1) global peer to peer network, is (2) decentralised (no single entity can control it), it’s (3) open source (wallet & transaction verification), (4) bypassing middlemen or central authority, with (5) no issuer or acquirer, (6) anyone with a computer or smartphone can use it | A digital currency most notable due to its popularity and success, although it was not the first virtual currency |  |  |  |  |
| Block | - | - | A block chain implementation consists of two kinds of records: transactions and blocks. Transactions are the actual data to be stored in the block chain, and blocks record and confirm when and in what sequence transactions became journaled database. | Blocks are found in the Bitcoin block chain. Blocks connect all transactions together. Transactions are combined into single blocks and are verified every ten minutes through mining. Each subsequent block strengthens the verification of the previous blocks, making it impossible to double spend bitcoin transactions (see double spend below). | - | According to DLT-I-048, a “block” be defined as a “digital entity”as specified in Recommendation ITU-T X.1255: as follows: An entity represented as, or converted to, a machine-independent data structure consisting of one or more elements in digital form that can be parsed by different information systems; the structure helps to enable interoperability among diverse information systems in the Internet. |  |
| Blockchain | A type of distributed ledger, comprised of unchangable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then ‘chained’ to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions. | Shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls. It is a cryptographed, secure, tamper resistant distributed database. It solves a complex mathematical problem to exist. A blockchain is a perfect place to store value, identities, agreements, property rights, credentials, etc. Once you put something like a Bitcoin into it, it will stay there forever. It is decentralized, disintermediated, cheap and censorship resistant. Applications of Blockchain: Bitcoin (cryptocurrency), Namecoin (wants to replace the entire DNS system of the Internet), or Sia (a decentralized cloud storage), Ethereum (Turing complete Virtual Machine where you can run any smart contract); Any centralized service like eBay, Dropbox can potentially be built in a decentralized way using blockchain technology, considerably lowering transaction costs | A network of processors combined to create a multi-purpose permissionless public ledger that rewards computing power suppliers with a token of value (See Blockchain and AltChain). Also called a permissionless distributed database or permissionless distributed ledger. | The Bitcoin block chain is a public record of all Bitcoin transactions. You might also hear the term used as a “public ledger.” The block chain shows every single record of bitcoin transactions in order, dating back to the very first one. The entire block chain can be downloaded and openly reviewed by anyone, or you can use a block explorer to review the block chain online. | A type of distributed ledger that is shared across a business network |  |  |
| Cryptocurrency | A form of digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Furthermore, cryptocurrencies operate independently of a central bank. | - | Another name for digital currency or the more accepted virtual currency that is a form of currency produced and secured by cryptology. | - | - |  |  |
| Distributed ledgers | A consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions | - | - | - | A type of database, or system of record, that is shared, replicated, and synchronized among the members of a network. |  |  |
| Ledger | An append-only record store, where records are immutable and may hold more general information than financial records. | - | - | - | - |  |  |
| Participant | An actor who can access the ledger: read records or add records to. | - | - | - | - |  |  |
| Permissioned Ledger, private blockchain | A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger’s integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger. | A fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc. internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired | A privately owned and operated AltChain | - | - |  |  |
| Proof-of-Stake | An alternative to the proof-of-work system, in which your existing stake in a cryptocurrency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine. | A method by which a cryptocurrency blockchain network aims to achieve distributed consensus. While the proof-of-work (PoW) method asks users to repeatedly run hashing algorithms or other client puzzles, to validate electronic transactions, proof-of-stake asks users to prove ownership of a certain amount of currency (their “stake” in the currency). Peercoin was the first cryptocurrency to launch using proof-of-Stake. Other prominent implementations are found in BitShares, Nxt, BlackCoin, NuShares/NuBits and Qora. Ethereum has planned a hard fork transition from PoW to PoS consensus. Decred hybridizes PoW with PoS and combines elements of both in an attempt to garner the benefits of the two systems and create a more robust notion of consensus. With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). In the case of Bitcoin, with Proof of Stake, the resource that’s compared is the amount of Bitcoin a miner holds – someone holding 1% of the Bitcoin can mine 1% of the “Proof of Stake blocks”. Instead of sacrificing energy to mine a block, a user must prove they own a certain amount of the cryptocurrency to generate a block. The more stake you own, the more likely you are to generate a block. In theory, this should prevent users from creating forks because it will devalue their stake and it should save a lot of energy. Proof of Stake sounds like a good idea, but ironically, there is the “Nothing at Stake” problem. Since mining Bitcoins is costly, it is not smart to waste your energy on a fork that won’t earn you any money, however with Proof of Stake, it is free to mine a fork | - | - | - |  |  |
| Proof-of-Work | A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work. | An economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. The concept may have been first presented by Cynthia Dwork and Moni Naor in a 1993 journal. The term “Proof of Work” was first coined and formalized in a 1999 paper by Markus Jakobsson and Ari Juels. A key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle or CPU pricing | - | - | - |  |  |
| Smart Contracts | Contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system. |  | - | - | Govern interactions with the ledger, and they can allow network participants to execute certain aspects of transactions automatically |  |  |
| Transaction Block | A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain. | - | - |  | - |  |  |
| Unpermissioned ledgers | Unpermissioned ledgers such as Bitcoin have no single owner — indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state | A blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is. As a substitute for centralized or quasi-centralized trust, public blockchains are secured by crypto economics – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These blockchains are generally considered to be “fully decentralized” | The Blockchain (bitcoin blockchain) | - | - |  |  |

**Bibliography**

In developing this list of DLT terms and definitions, reference has been made to a large number of DLT publications, work and glossaries that already exist. The list is far from exhaustive but includes:

[b-DFS] Focus Group Technical Report ITU-T FG-DFS, Digital Financial Services (DFS) Glossary

[b-X.1255] Recommendation ITU-T X.1255:2009, Framework for discovery of identity management information

[b-Y.2091] Recommendation ITU-T Y.2091:2011, Terms and definitions for next generation networks

[b-ITU-T X.800|ISO 7498-2] Recommendation ITU-T X.800|ISO 7498-2:1991, Security architecture for Open Systems Interconnection for CCITT applications

[b-X.das-mgt] Draft Recommendation ITU-T X.das-mgt, Security framework for the data access and sharing management system based on the distributed ledger technology

[b-X.sa-dlt] Draft Recommendation ITU-T X.sa-dlt, Security assurance for Distributed Ledger Technology

[b-X.sct-dlt] Draft Recommendation ITU-T X.sct-dlt, Security capabilities of, and threats to Distributed Ledger Technology

[b-X.sradlt] Draft Recommendation ITU-T X.sradlt, Security framework for distributed ledger technology

[b-X.srdrm-dlt] Draft Recommendation ITU-T X.srdrm-dlt, Security requirements for digital rights management based on distributed ledger technology

[b-X.ss-dlt] Draft Recommendation ITU-T X.ss-dlt, Security Services based on Distributed Ledger Technology

[b-X.stov] Draft Recommendation ITU-T X.stov, Security threats to online voting using distributed ledger technology

[b-X.strdlt] Draft Recommendation ITU-T X.strdlt, Security threats and requirements of digital payment services based on distributed ledger technology

[b-X.tfspd-dlt] Draft Recommendation ITU-T X.tfspd-dlt, Technical framework for secure software programme distribution mechanism based on distributed ledger

[b-BB] [Blockchain Glossary - Blockchain Technology Guide](http://www.blockchaintechnologies.com/blockchain-glossary)

[b-BGB] [Blockchain Glossary for Beginners - Blockchain Basics - BlockchainHub](https://blockchainhub.net/blockchain-glossary/)

[b-BBT] [Bitcoin & Blockchain Terminology | dinbits](http://news.dinbits.com/p/dinbits-terminology.html)

[b-BTG] [Bitcoin terms glossary – Blockchain Support Center](https://support.blockchain.com/hc/en-us/articles/213276463-Bitcoin-terms-glossary)

[b-BBG] [Blockchain basics: Glossary and use cases - IBM](http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html)

[b-NIST] [Draft NISTIR 8202: 2018, Blockchain Technology Overview](https://csrc.nist.gov/publications/detail/nistir/8202/draft)

[b-ISO/IEC 2382] ISO/IEC 2382:2015, Information technology – Vocabulary

[b-ISO/TC307] ISO/TC 307 22739(CD) Blockchain and distributed ledger technologies – Terminology

[b-DIN 16597] German National Standard DIN SPEC 16597:2018 Terminology for blockchain

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_