|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | FG-AI4H-025-A04 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | Plenary | Zanzibar, 3-5 September 2019 |
| **DOCUMENT** |
| **Source:** | FG-DLT |
| **Title:** | Updated baseline text: D3.2 - Overview of existing platforms and mapping to distributed ledger technology reference architecture |
| **Purpose:** | Discussion |
| **Contact:** | Paulo BrizolaMultiledgersBrazil | E-mail: paulo@multiledgers.com |
| **Contact:** | Hu Ning OnchainChina | Email: hehehu@gmail.com |

|  |  |
| --- | --- |
| **Keywords:** | Distributed Ledger Technologies; Reference Architecture Mapping |
| **Abstract:** | This document contains the updates made on draft ITU-T FG DLT deliverable D3.2 “Overview of existing platforms and mapping to distributed ledger technology reference architecture” during the Madrid meeting. |

This template aims to define key features of the DLT-based platform that mapping to DLT reference architecture from technical perspectives.

**Section 1 Summary**

|  |
| --- |
| Platform summary |
| Platform ID | *Ethereum/ETH…* |
| Status/Revision | *Proposed; Alpha / Beta;V1.0, …* |
| Type | *Public, Consortium…* |
| Domain | *Financial, IoT, Healthcare…* |
| Description | *Further description if any* |

**Section 2 Governance & Compliance Functions**

|  |
| --- |
| Platform governance |
| Governance Type | *Permissioned; Permissionless;* *Hybrid;**…* |
| Chain Network Admin | *NA/Community (public); Entity (Consortium/Private), …* |
| Pledge (cost of malicious action) | *Stake; …* |
| Description | *Further description if any* |

|  |
| --- |
| Platform trust endorsement policy |
| Type | *Law/Agreement; Tokenomics[[1]](#footnote-1);*  |
| Tool | *Token ID; Contract ID; …* |
| Policy | *Policy to support governance* |

|  |
| --- |
| Economic Model (optional) |
| Price Model to Deploy Contracts and do Transactions  | *Charged by transaction, mandatory to have tokens, inflationary system* |
| Who pays the costs of the network | *Users; Developers; Nodes* |
| Monetary Policy of Tokens | *Finite or infinite token supply; Total of tokens; Pre-Isssued or not; How much issued per blocks;*  |
| Rights of Tokens  | *Property rights, rights to specific IP, rights to part equity ownership* |

**Section 3 Application**

|  |
| --- |
| Platform Smart Contract mechanism |
| Language | *Java; Solidity; Kotlin; Go; ...* |
| Turing Complete? | *…* |
| Compiler | *C#; Java; Solidity; …* |
| Runtime VM | *EVM; NEOVM; JVM; WASM; …* |
| DevTools | *IDE; Build framework; Test framework; …* |
| Extra Tool(s) | *Explorer (Block data view); Speed-test; …* |
| Lifecycle | *Describe…* |
| Description | *Further description if any* |

**Section 4 Protocol**

|  |
| --- |
| Platform AAA Management |
| Account type | *Identity; address; …* |
| Distributed ID | *using an established PKI structure, a digital identity encapsulated in an X.509 digital certificate* |
| AAA support | *Fabric CA;**Membership Service Providers,*  |
| Description | *Further description if any* |

|  |
| --- |
| Platform Consensus Mechanism |
| Algorithm | *PoW; PoS; BFT; …* |
| Consensus mode | *Event; State* |
| Management solution | *Internal; external* |
| Description | *Further description if any* |

|  |
| --- |
| Platform Ledger Management |
| Model | *UTXO; balance; …* |
| Extra | *MPT support; …* |
| Description | *Further description if any* |

**Section 5 Resources**

|  |
| --- |
| Node Management |
| Node Role | *EP; Normal; …* |
| Joining | *Describe node joining process* |
| Leaving | *Describe node leaving process* |
| Role changing | *Describe node role changing process* |
| Description | *Further description if any* |

|  |
| --- |
| Platform Data Storage Mechanism |
| Mass storage mitigation[[2]](#footnote-2) | *Solutions to resolve/mitigate this problem, if any…* |
| Decentralized Data Storage Support | *SIA; IPFS…* |
| Data Privacy Solution | *ZKP; MPC…* |
| Tamper Proof (tamper cost) | *Mechanism and tamper cost hypothesis* |
| Description | *Further description if any* |

|  |
| --- |
| Platform Network Management |
| Node Scalability | *Node scale* |
| Network Structure | *Distributed; Flexible; …* |
| Network Discovery Protocol | *Kademlia-like; Private …* |
| Byzantine Node Accepted?  | *Yes; No* |
| P2P?  | *Yes; No* |
| Data Exchange Protocol | *Gossip; ...* |
| Description | *Further description if any* |

**Section 6 Utils**

|  |
| --- |
| Platform Messaging Mechanism |
| Protocol Type | *RPC; LTCP; …* |
| Description | *Further description if any* |

|  |
| --- |
| Platform Crypto Libraries |
| Secure Network Connection Type | *SSL; TLS; …* |
| Cipher Suites | *ECDSA; EdSA; ECDSA; RSA; AMCL; ...*  |
| Description | *Further description if any* |

**Section 7 Operation & Maintenance**

|  |
| --- |
| Platform system management – Node |
| Log | *…* |
| Monitoring |  |
| Description | *[Operation and Maintenance] Further description if any* |

|  |
| --- |
| Platform system management – Chain Network |
| Permission Control | *…* |
| Auditing |  |
| Supervisory Support | *…* |
| Description | *[Operation and Maintenance] Further description if any* |

**Section 8 External Resource Management**

|  |
| --- |
| Platform External Resource Management |
| Interoperation solution | *Non-DLT system; 3rd DLT system; …* |
| Description | *Further description if any* |

**Section 9 Extensions**

|  |
| --- |
| Platform Extensions - optional |
| *[the following list can be duplicated for multiple extensions]* |
| Name | *Name of the extension if any* |
| Extension type[[3]](#footnote-3) | *Internal; external* |
| Extension mode[[4]](#footnote-4) | *Scalability (horizontal); capability (vertical)* |
| Solution | *[external] side-chain; off-chain; mutli-chain**[internal] child-chain; sharding* |
| Serve domain | *Horizontal: sharding; non-DLT system; …**Vertical: storage; …* |
| Description | *Further description if any* |

1. Alternative term: economic incentives. Depends on the terms in the output of D1.1, if the term of tokenomics has clear definition, use tokenomics, otherwise, economic incentives [↑](#footnote-ref-1)
2. On chain storage cost much, solution/mechanism to resolve the problem of large cost of mass storage from node perspective. E.g., data maintenance, data storage and data cleaning. [↑](#footnote-ref-2)
3. Standing from DLT system instance perspective, any extension inside the instance is marked as “internal”, while any extension outside the instance is marked as “external” [↑](#footnote-ref-3)
4. All extension instances are equal (with similar capability and functional features), targeting for the scalability of DLT instance, marked as “horizontal”; extensions with different functional features, targeting to enforce the capability of DLT instance, marked as vertical. Extension type and mode pair(s) is/are used to describe the extension as to the whole DLT system. E.g., sharding (internal – horizontal), lightening – BTC (external – vertical), Corda Contract (internal – vertical). [↑](#footnote-ref-4)