Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 4, 2021

H. Nakajima
Mercari R4D
M. Kusunoki
JDD
K. Hida
JBA
Y. Suga
Advanced Security Div, IIJ
T. Hayashi
Lepidum

December 31, 2020

Terminology for Cryptoassets
draft-nakajima-crypto-asset-terminology-05

Abstract

This document provides terminology used in cryptoassets.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 4, 2021.

Copyright Notice

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Our goal with this document is to improve our understanding on a set of terms which frequently used in documents which related to cryptoassets. Mutual understanding about terminology may help to reach a consensus on issues we're trying to solve.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terms and Definitions

address: An identifier to represent a public key in a blockchain network.

administrator: It is a person who conducts operational maintenance of the system with the authority to change the system settings. From the viewpoint of mutual checking, there are administrators with different authorities depending on the subjects to be

managed. See also: operator.

asymmetric cryptography: Defined in [RFC4949] as "A modern branch of cryptography (popularly known as "public-key cryptography") in which the algorithms use a pair of keys (a public key and a

private key) and use a different component of the pair for each of two counterpart cryptographic operations (e.g., encryption and decryption, or signature creation and signature verification). "

block: A basic unit of the blockchain. A set of transactions on a blockchain which contains a cryptographic hash value of the previous block.

blockchain: An ordered series of data chains constructed that attackers cannot alter by cryptographic algorithms. A type of distributed ledger.

confirmation: Approval works defined by the consensus algorithm. A status that blocks and transactions in a certain block are approved by miners and users of the blockchain network.

consensus: Agreements among nodes in the blockchain network.

cryptoasset: A digital representation of values that can be exchanged or transferred digitally, realized by a distributed ledger such as blockchain utilizing cryptography or similar technology.

cryptoassets custody service: Business to manage the kind of cryptoassets.

cryptoassets custodian: The business entities that operate the cryptoasset custody business.

cryptoassets custody system: The information system that responsible for the cryptoasset custody business.

cryptoassets exchange: A function for exchanging fiat currencies and cryptoassets, and also exchanging cryptoassets with each other.

cryptoassets exchange service provider: A business entity that

operates a cryptoasset exchange.

deterministic wallet: See: wallet

digital signature: Defined in [RFC4949] as "A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity."

distributed ledger: A distributed database about cryptoassets with agreed processed.

double spending: Defined in [MasteringBitcoinOnline] as "result of successfully spending some money more than once." fiat currency: Currency which has been established by the government or other authorities.

fork: A branch of a ledger. Ledger branching may occur accidentally or by specification changes.

accidental fork: A case where a block is accidentally mined at about the same time, and a plurality of chains coexist temporarily. It occurs on a daily basis and converges to the longest chain by re-org.

soft fork: A branch caused by specification change of blockchain. It does not affect wallet implementation.

hard fork: A branch caused by a specification change without the forward compatibility of the blockchain, which may affect the wallet implementation in addition to the miner. There is a case where a plurality of chains continue to coexist permanently because there is no consensus between developers regarding the case where the majority of nodes stay in the specification change by following the hard fork, we call it split. Examples of typical splits include the division of Ethereum and Ethereum Classic in The DAO case of 2016, the division of Bitcoin and Bitcoin Cash in 2017, and so on. The new coin born by division is called a fork coin.

genesis block: An initial block on a blockchain. Genesis block may

differ to distinguish chains.

hash value: Defined in [RFC4949] as "The output of a hash function."

hash rate: Amount of a hash value which node is able to generate per unit of time (generally per second)

hierarchy deterministic wallet: See: wallet

mining: A process to append a received transaction to a block by validating a transaction with agreed consensus rules such as proof-of-work and proof-of-stake.

miner: A network node which contributes its resources to mining.

multisignature: Defined in [MasteringBitcoinOnline] as "requiring more than one key to authorize a bitcoin transaction". In this scope, the transaction is not limited to a bitcoin transaction.

node: A device that connects to the blockchain network.Note that the node has a different meaning in the context of expression about the Merkle tree.

off-chain transaction: The movement of value outside of the blockchain

on-chain transaction: The movement of value on the blockchain

operator: It is a person who performs routine tasks based on authority as a normal task. See also: administrator.

orphan block: Defined in [MasteringBitcoinOnline] as "Blocks whose parent block has not been processed by the local node, so they can't be fully validated yet."

permissioned-chain: A blockchain that only specified members can join the blockchain network.

permissionless-chain: See: permissioned-chain

public-chain: An open blockchain that anyone can retrieve all of

blocks and transactions without special privileges.

public key: Defined in [RFC4949] as "The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography."

private-chain: In contrast with "public-chain", A closed blockchain that only qualified users can access blocks and make transactions.

private key: Defined in [RFC4949] as "The secret component of a pair of cryptographic keys used for asymmetric cryptography."

proof-of-stake: Defined in [MasteringBitcoinOnline] as "method by which a cryptocurrency blockchain network aims to achieve distributed consensus."

proof-of-work: Defined in [MasteringBitcoinOnline] as "A piece of data that requires significant computation to find."

reorganization: The convergence into one chain based on a certain consensus from multiple chains that are temporarily branched.

reward: Value by the blockchain network which assigned to a miner who successfully validates a transaction. Rules may differ among blockchains and consensus rules.

side-chain: See off-chain

smart contract: A guaranteed digital procedure that automatically enforced on a blockchain network.

soft fork: See: fork

token: 1) Data that represents the amount of cryptoassets like ERC20 specification, 2) Data used in the API as one of the factors with the authentication process.

transaction: Defined in [MasteringBitcoinOnline] as "More precisely, a transaction is a signed data structure expressing a transfer of value."

incoming transaction: Transfer of cryptoassets from other addresses to one's own address.

outgoing transaction: Transfer of cryptoassets from one's own address to other addresses.

validation: Checking the accuracy and consistency of given transactions and blocks. Specifically, it is general to verify the integrity of data to be digital-signed and also the integrity of other transactions and blocks. By verifying a transaction repeatedly, it is possible to verify blocks in the transaction.

validated: See: validation

validator: See: validation

wallet: A mechanism that handles a key pair of a public key and a secret key used for transmitting cryptoassets and such a key pair.

hot wallet: A wallet that is online connected to the network, the key is activated, and operators can coin out the cryptoassets by automatic processing.

cold wallet: A wallet that is disconnected from the network and the key is inactivated. It can not be coined out unless there is an explicit operation by the operator. The frequency of outgoing coins is limited. Between hot wallet and cold wallet, there are various intermediate forms such as a wallet that is online, but requires manual operation at the time of signing a transaction, the wallet that is offline but the operation is automated, and warm wallet.

4. Symbols and abbreviated terms

AML Anti-Money Laundering

API: Application Programming Interface

CFT: Counter Financing of Terrorism

DAO: Distributed Autonomous Organization

DLT: Distributed Ledger Technologies

HD: Hierarchy Deterministic (wallet)

PKI: Public Key Infrastructure

5. Security Considerations

This document defines terminology for cryptoassets. Therefore, there is no security considerations.

6. IANA Considerations

None.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[MasteringBitcoinOnline] Antonopoulos, A., "Mastering Bitcoin", March 2018, <https://github.com/bitcoinbook/bitcoinbook>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

7.3. URIs

[ref-1] , <https://cgtf.github.io/>.

Acknowledgments

Thanks to members of the Cryptoassets Governance Task Force [ref-1] for help and feedback.

Authors' Addresses

Hirotaka Nakajima
Mercari, Inc. R4D
Roppongi Hills Mori Tower 21F
6-10-1 Roppongi
Minato, Tokyo 106-6125
JAPAN

Email: nunnun@mercari.com

Masanori Kusunoki
Japan Digital Design, Inc.
Nihonbashi Talk Building
3-3-5, Nihonbashi-Hongokucho
103-0021
JAPAN

Email: masanori.kusunoki@japan-d2.com

Keiichi Hida
Japan Blockchain Association

Email: hida@jba-web.jp

Yuji Suga
Advanced Security Division, Internet Initiative Japan Inc.
Iidabashi Grand Bloom,
2-10-2 Fujimi
Chiyoda, Tokyo 102-0071
JAPAN

Email: suga@iij.ad.jp

Tatsuya Hayashi
Lepidum Co. Ltd.

Email: hayashi@lepidum.co.jp