Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 4, 2019

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

December 31, 2018

Terminology for Cryptoassets
draft-nakajima-crypto-asset-terminology-01

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, 2019.

Copyright Notice

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 authority to change system setting. From the viewpoint of mutual checking, there are administrators with different authorities depending on the subjects to be managed.

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 previous block.

blockchain: A digital ledger about transactions for cryptoassets.

confirmation: (For transactions,) checking correctness of a transaction in the mainchain.

consensus: Coincidence the way of thinking.

cryptoassets: Cryptographically guaranteed value.

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 money: Currency which has been established by government or other authorities.

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

accidental fork: An accidental fork is 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 soft fork may influence the implementation of a miner in branches caused by specification change of block chain, but does not affect wallet implementation.

hard fork: A hard fork is a branch caused by a specification change without forward compatibility of the block chain, 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 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 is a network node which contributes its resources to mining.

miner: See: mining

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

node: A device that connects to blockchain network.

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.

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 public 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 permissioned 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: Invalidation process of branched blockchains.

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: An unforgeable data object.

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

validation: Checking correctness and consistency of given data.

validated: See: validation

validator: See: validation

wallet: A wallet is an implementation that handles a key pair of a public key and a secret key used for transmitting a virtual

currency and such a key pair. In this document, the latter is distinguished and called wallet implementation.

hot wallet: It is a wallet that is online connected to the network, the key is activated, and you can coin out the virtual currency by automatic processing.

cold wallet: Normally it is disconnected from the network and the key is inactivated and it is a wallet that can not be coined out unless there is an explicit operation by the operator. Frequency of outgoing coins is limited.

Between Hot Wallet and Cold Wallet, there are various intermediate forms such as wallet that is online, but requires manual operation at the time of signing a transaction, wallet that is offline but

operation is automated, and warm wallet There are also sometimes called.

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

[1] https://vcgtf.github.io/

Acknowledgments

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

Authors' Addresses

Hirotaka Nakajima
Mercari, Inc. R4D
Roppongi Hills Mori Tower 25F
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