CREACOIN仕様書 Version0.1 2014/09/06

# 与件構造

## 要約値

### SHA256

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | hash | 要約値 | byte[] | 32 |
| 合計 |  |  |  | 32 |

### SHA256^2

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | hash | 要約値 | byte[] | 32 |
| 合計 |  |  |  | 32 |

### RIPEMD160.SHA256

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | hash | 要約値 | byte[] | 20 |
| 合計 |  |  |  | 20 |

### X14

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | hash | 要約値 | byte[] | 32 |
| 合計 |  |  |  | 32 |

### X15

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | hash | 要約値 | byte[] | 32 |
| 合計 |  |  |  | 32 |

## 鍵

### ECDSA256公開鍵

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | pubkey | 公開鍵 | byte[] | 72 |
| 合計 |  |  |  | 72 |

### ECDSA256秘密鍵

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | privkey | 秘密鍵 | byte[] | 104 |
| 合計 |  |  |  | 104 |

### ECDSA256鍵対

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | pubkey | ECDSA256公開鍵 | byte[] | 72 |
| 2 | privkey | ECDSA256秘密鍵 | byte[] | 104 |
| 合計 |  |  |  | 176 |

### Secp256k1公開鍵

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | pubkey | 公開鍵 | byte[] | 65 |
| 合計 |  |  |  | 65 |

### Secp256k1秘密鍵

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | privkry | 秘密鍵 | byte[] | 32 |
| 合計 |  |  |  | 32 |

### Secp256k1鍵対

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | pubkey | Secp256k1公開鍵 | byte[] | 65 |
| 2 | privkey | Secp256k1秘密鍵 | byte[] | 32 |
| 合計 |  |  |  | 97 |

## 電子署名

### ECDSA256署名

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | signature | ECDSA256署名 | byte[] | 64 |
| 合計 |  |  |  | 64 |

### Secp256k1署名

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | signature | Secp256256k1署名 | byte[] | 65 |
| 合計 |  |  |  | 65 |

## 口座

### 口座

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | name.length | 口座名の長さ | int | 4 |
| 4 | name | 口座名 | string |  |
| 5 | description.length | 口座の説明の長さ | int | 4 |
| 6 | description | 口座の説明 | string |  |
| 7 | keyPair | ECDSA256鍵対 | ECDSA256KeyPair | 176 |
| 合計 |  |  |  |  |

＜バージョン1＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | name.length | 口座名の長さ | int | 4 |
| 4 | name | 口座名 | string |  |
| 5 | description.length | 口座の説明の長さ | int | 4 |
| 6 | description | 口座の説明 | string |  |
| 7 | keyPair | Secp256k1鍵対 | Secp256k1KeyPair | 97 |
| 合計 |  |  |  |  |

### 匿名口座名義

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | accounts.length | 口座数 | int | 4 |
| 4-1 | accounts[i].length | 口座の長さ | int | 4\*n |
| 4-2 | accounts[i] | 口座一覧 | Account  Version0 |  |
| 合計 |  |  |  |  |

＜バージョン1＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | accounts.length | 口座数 | int | 4 |
| 4-1 | accounts[i].length | 口座の長さ | int | 4\*n |
| 4-2 | accounts[i] | 口座一覧 | Account  Version1 |  |
| 合計 |  |  |  |  |

### 顕名口座名義

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | accounts.length | 口座数 | int | 4 |
| 4-1 | accounts[i].length | 口座の長さ | int | 4\*n |
| 4-2 | accounts[i] | 口座一覧 | Account  Version0 |  |
| 5 | name.length | 口座名義人の長さ | int | 4 |
| 6 | name | 口座名義人 | string |  |
| 7 | keyPair | ECDSA256鍵対 | ECDSA256KeyPair | 176 |
| 合計 |  |  |  |  |

＜バージョン1＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | accounts.length | 口座数 | int | 4 |
| 4-1 | accounts[i].length | 口座の長さ | int | 4\*n |
| 4-2 | accounts[i] | 口座一覧 | Account  Version1 |  |
| 5 | name.length | 口座名義人の長さ | int | 4 |
| 6 | name | 口座名義人 | string |  |
| 7 | keyPair | Secp256k1鍵対 | Secp256k1KeyPair | 97 |
| 合計 |  |  |  |  |

### 口座名義一覧

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | anonymousAccountHolder | 匿名口座 | AnonymousAccountHolder |  |
| 4 | pseudonymousAccountHolders.length | 顕名口座数 | int | 4 |
| 5-1 | pseudonymousAccountHolders[i].length | 顕名口座の長さ | int | 4\*n |
| 5-2 | pseudonymousAccountHolders[i] | 顕名口座一覧 | PseudonymousAccountHolder[]  Version0 |  |
| 6 | candidatePseudonymousAccountHolders.length | 顕名口座候補数 | int | 4 |
| 7-1 | candidatePseudonymousAccountHolders[i].length | 顕名口座候補の長さ | int | 4\*n |
| 7-2 | candidatePseudonymousAccountHolders[i] | 顕名口座候補一覧 | PseudonymousAccountHolder[]  Version0 |  |
| 合計 |  |  |  |  |

## 取引

### 取引入力

・バージョンあり

・バージョン保存なし

＜バージョン0＞

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | prevTxBlockIndex | 取引入力への参照（ブロック番号） | long | 8 |
| 2 | prevTxIndex | 取引入力への参照（ブロック内の取引番号） | int | 4 |
| 3 | prevTxOutputIndex | 取引入力への参照（取引内の取引出力番号） | int | 4 |
| 4 | senderSignature | 送付者の電子署名 | Ecdsa256Signature | 64 |
| 5 | senderPubKey | 送付者の公開鍵 | Ecdsa256PubKey | 72 |
| 合計 |  |  |  | 152 |

＜バージョン1＞

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | prevTxBlockIndex | 取引入力への参照（ブロック番号） | long | 8 |
| 2 | prevTxIndex | 取引入力への参照（ブロック内の取引番号） | int | 4 |
| 3 | prevTxOutputIndex | 取引入力への参照（取引内の取引出力番号） | int | 4 |
| 4 | senderSignature | 送付者の電子署名 | Secp256k1Signature | 65 |
| 合計 |  |  |  | 81 |

### 取引出力

・バージョンあり

・バージョン保存なし

＜バージョン0＞

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | receiverPubKeyHash | 受取人の公開鍵の要約値（口座番号） | Sha256Ripemd160Hash | 20 |
| 2 | amount | 額面価格 | long | 8 |
| 合計 |  |  |  | 28 |

### 貨幣生成取引

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | txOutputs.length | 取引出力の集合の要素数 | int | 4 |
| 4 | txOutputs | 取引出力の集合 | TransactionOutput[] | 28n |
| 合計 |  |  |  | 12+28n  n=1 => 40  n=2 => 68 |

### 貨幣移動取引

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | txOutputs.length | 取引出力の集合の要素数 | int | 4 |
| 4 | txOutputs | 取引出力の集合 | TransactionOutput[] | 28n |
| 5 | txInputs.length | 取引入力の集合の要素数 | int | 4 |
| 6 | txInputs | 取引入力の集合 | TransactionInput[]  Version0 | 152m |
| 合計 |  |  |  | 16+28n+152m  n = 1, m = 1 => 196 |

＜バージョン1＞

・破損検査あり

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | check | 破損検査用要約値 | byte[] | 4 |
| 3 | txOutputs.length | 取引出力の集合の要素数 | int | 4 |
| 4 | txOutputs | 取引出力の集合 | TransactionOutput[] | 28n |
| 5 | txInputs.length | 取引入力の集合の要素数 | int | 4 |
| 6 | txInputs | 取引入力の集合 | TransactionInput[]  Version1 | 81m |
| 合計 |  |  |  | 16+28n+81m  n = 1, m = 1 => 125 |

## ブロック

## ノード情報

### 初期ノード情報

・バージョンなし

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | hex.length | 難読化された初期ノード情報の長さ | int | 4 |
| 2 | hex | 難読化された初期ノード情報 | string | 76? |
| 合計 |  |  |  | 80? |

＜hexの内容＞

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | ipAddress | IPアドレス | IPAddress | 4 |
| 2 | portNumber | ポート番号 | ushort | 2 |
| 3 | network | ノードが所属するネットワーク | Network | 4 |
| 合計 |  |  |  | 10 |

### ノード情報

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | hex.length | 難読化された初期ノード情報の長さ | int | 4 |
| 3 | hex | 難読化された初期ノード情報 | string | 76? |
| 4 | participation | 参加日時 | DateTime | 8 |
| 5 | publicRSAParameters.length | 通信用RSA公開鍵の長さ | int | 4 |
| 6 | publicRSAParameters | 通信用RSA公開鍵 | string | 1679? |
| 合計 |  |  |  | 1775? |

## 通信文

### 冒頭

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | isInBound | 接続を受け付けているノードか？ | bool | 1 |
| 3 | nodeInfo.length | ノード情報の長さ（ただし、isInBoundがtrueの場合のみ） | int | 0 or 4 |
| 4 | nodeInfo | ノード情報（ただし、isInBoundがtrueの場合のみ） | NodeInformation  Version0 | 0 or 1775? |
| 5 | creaVersion | クライアントのバージョン | int | 4 |
| 6 | protocolVersion | 通信手順のバージョン | int | 4 |
| 7 | client.length | クライアント名の長さ | int | 4 |
| 8 | client | クライアント名 | string |  |
| 9 | isTemporary | 一時接続か？（一時接続でない場合は常時接続） | bool | 1 |
| 合計 |  |  |  |  |

### 冒頭返信

・バージョンあり

・バージョン保存あり

＜バージョン0＞

・破損検査なし

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| 1 | version | バージョン | int | 4 |
| 2 | nodeInfo.length | ノード情報の長さ | int | 4 |
| 3 | nodeInfo | ノード情報 | NodeInformation  Version0 | 1775? |
| 4 | isSameNetwork | ノードが所属するネットワークが同一か？ | bool | 1 |
| 5 | isCorrectNodeInfo | 冒頭通信文で受け取ったノード情報が正しいか？ | bool | 1 |
| 6 | correctNodeInfo.length | 正しい相手のノード情報の長さ（ただし、isCorrectNodeInfoがfalseの場合のみ） | int | 0 or 4 |
| 7 | correctNodeInfo | 正しい相手のノード情報（ただし、isCorrectNodeInfoがfalseの場合のみ） | NodeInformation  Version0 | 0 or 1775? |
| 8 | isOldCreaVersion | クライアントのバージョンが古いか？ | bool | 1 |
| 9 | isAlreadyConnected | 既に接続しているか？ | bool | 1 |
| 10 | protocolVersion | 通信手順のバージョン | int | 4 |
| 11 | client.length | クライアント名の長さ | int | 4 |
| 12 | client | クライアント名 | string |  |
| 合計 |  |  |  |  |

＜署名対象＞

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 与件項目 | 説明 | 型 | 長さ[byte] |
| ＜k番目の取引入力（全n個）＞ |  |  |  |  |
| 3k+1 | prevTxBlockIndex | 取引入力への参照（ブロック番号） | long | 8 |
| 3k+2 | prevTxIndex | 取引入力への参照（ブロック内の取引番号） | int | 4 |
| 3k+3 | prevTxOutputIndex | 取引入力への参照（取引内の取引出力番号） | int | 4 |
| 小計 |  |  |  | 16n |
| ＜k番目の被参照取引出力（全n個）＞ |  |  |  |  |
| 3n+k+1 | receiverPubKeyHash | 前の受取人（＝送付者）の公開鍵の要約値（口座番号） | Sha256Ripemd160Hash | 20 |
| 小計 |  |  |  | 20n |
| ＜k番目の取引出力（全m個）＞ |  |  |  |  |
| 4n+2k+1 | receiverPubKeyHash | 受取人の公開鍵の要約値（口座番号） | Sha256Ripemd160Hash | 20 |
| 4n+2k+2 | amount | 額面価格 | long | 8 |
| 小計 |  |  |  | 28m |
| 合計 |  |  |  | 36n+28m |

＜P2Pノードの参加＞

・通信の暗号化に使用するRSA鍵ペアを生成する。

・ポート番号が0でない場合

・IPアドレスを取得する。

・IPアドレスが取得できた場合

・初期ノード情報を作成する。

・初期ノード情報を（初期ノード登録所に）登録する。

・ノード情報を作成する。

・接続の待ち受けを開始する。

・他のノードの初期ノード情報を取得する。

・常時接続を確立する。

＜P2Pノードの離脱＞

・何もしない。

＜新しい接続の開始（接続要求側）＞

・ヘッダを送信する。

・ヘッダの返信を受信する。

・相手の所属ネットワークが自分の所属ネットワークと異なる場合

・通信を終了する。

・既に相手と接続している場合

・通信を終了する。

・自身のノード情報のIPアドレスが間違っている疑いがある場合

・＜未実装＞

・他のノードの状態に関する情報を更新する。

・相手が申告したクライアントのバージョンが自分のクライアントのバージョンより大きい場合

・＜未実装＞

・通信手順のバージョンを決定する（自分と相手が対応しているバージョンの中で最も大きいものを選択する）。

（１）バージョンが0の場合

（ア）一時接続の場合

・（一時）通信を実行する。

・常時接続を行う設定の場合

・相手が常時接続したいかどうか返信を受け取る。

・相手が常時接続したい場合

・常時接続可能かどうか判断する。

・常時接続可能かどうか相手に伝える。

・常時接続可能な場合

・常時接続に移行する。

（イ）常時接続の場合

・相手が常時接続可能かどうか（常時接続の要求を受け入れ可能かどうか）返信を受け取る。

・相手が常時接続可能な場合

・常時接続に移行する。

・通信を終了する（ただし、常時接続に移行した場合を除く）。

＜新しい接続の開始（接続受理／拒否側）

・ヘッダを受信する。

・ヘッダのノード情報のIPアドレスと実際の相手のIPアドレスが一致しない場合

・相手のノード情報を適切に更新する

・ヘッダの返信を送信する。

・相手の所属ネットワークが自分の所属ネットワークと異なる場合

・接続を拒否する（通信を終了する）。

・既に相手と接続している場合

・接続を拒否する（通信を終了する）。

・＜未実装＞不良ノードは拒否する？

・他のノードの状態に関する情報を更新する。

・相手が申告したクライアントのバージョンが自分のクライアントのバージョンより大きい場合

・＜未実装＞

・通信手順のバージョンを決定する（自分と相手が対応しているバージョンの中で最も大きいものを選択する）。

（１）バージョンが0の場合

（ア）一時接続の場合

・（一時）通信を実行する。

・常時接続を行う設定の場合

・相手と常時接続すべき（したい）か判断する。

・常時接続したいかどうかを相手に伝える。

・相手と常時接続したい場合

・相手の返信（常時接続可能かどうか）を受信する。

・相手が常時接続可能な場合

・常時接続に移行する。

（イ）常時接続の場合

・常時接続可能かどうか（相手からの常時接続の要求を受け入れるかどうか）判断する。

・常時接続可能かどうかを相手に伝える。

・常時接続可能な場合

・常時接続に移行する。

・通信を終了する（ただし、常時接続に移行した場合を除く）。