



Dunitier Blockchain Protocol

Les bases du protocole





Documents

La communication entre noeuds ou entre les clients et les noeuds s'effectue par envoi de documents.

Différents types :

- Identity
- Revocation
- Certification
- Membership
- Transaction
- Block



Identity

Un document Identity est envoyé pour déclarer une identité, c'est à dire lier une clé publique **PUBLIC_KEY** à une chaîne de caractères **USER_ID** représentant l'identité (un pseudo). C'est cette identité à laquelle feront référence des certifications dans le processus d'acceptation des membres.

```
Version: 10
Type: Identity
Currency: CURRENCY_NAME
Issuer: PUBLIC_KEY
UniqueID: USER_ID
Timestamp: BLOCK_UID
SIGNATURE
```



Identity

Ex: identité “lolcat” liée à la clé “HgTTJL...”

```
Version: 10
Type: Identity
Currency: beta_brousouf
Issuer: HgTTJLAQ5sqfknMq7yLPZbehtuLSsKj9CxnW7k8QvYJd
UniqueID: lolcat
Timestamp: 32-DB30D958EE5CB75186972286ED3F4686B8A1C2CD
J3G9oM5AKYZNLAB5Wx499w61NuUoS57JVccTShUbGpCMjCqj9yXXqNq7dyZpDWA6BxipsiaMZhuJMeBfCznzyci
```



Revocation

Un document Revocation est envoyé quand le détenteur d'une identité souhaite la supprimer, pour une raison ou pour une autre : identité faite par erreur, ou dont la sécurité est compromise, etc.

```
Version: 10
Type: Revocation
Currency: CURRENCY_NAME
Issuer: PUBLIC_KEY
IdtyUniqueID: USER_ID
IdtyTimestamp: BLOCK_UID
IdtySignature: IDTY_SIGNATURE
REVOCATION_SIGNATURE
```

Revocation

Ex: pour notre identité “lolcat”, la révocation sera celle-ci. A noter, une révocation contient l'identité qu'elle révoque, un noeud recevant cette révocation peut ainsi vérifier la validité de l'identité avant de la révoquer.

```
Version: 10
Type: Identity
Currency: beta_brousouf
Issuer: HgTTJLAQ5sqfknMq7yLPZbehtuLSsKj9CxwN7k8QvYJd
UniqueID: lolcat
Timestamp: 32-DB30D958EE5CB75186972286ED3F4686B8A1C2CD
J3G9oM5AKYZNLAB5Wx499w61NuUoS57JVccTShUbGpCMjCqj9yXXqNq7dyZpDWA6BxipsiaMZhuJMeBfCznzyci
```

```
Version: 10
Type: Revocation
Currency: beta_brousouf
Issuer: HgTTJLAQ5sqfknMq7yLPZbehtuLSsKj9CxwN7k8QvYJd
IdtyUniqueID: lolcat
IdtyTimestamp: 32-DB30D958EE5CB75186972286ED3F4686B8A1C2CD
IdtySignature: J3G9oM5AKYZNLAB5Wx499w61NuUoS57JVccTShUbGpCMjCqj9yXXqNq7dyZpDWA6BxipsiaMZhuJMeBfCzn
SoKwoa8PFFCDJWZ6dNCv7XstezHcc2BbKiJgVDXv82R5zYR83nis9dShLgWJ5w48noVUHimdngzYQneNYSMV3rk
```



Certification

Pour avoir le droit d'utiliser le réseau, une identité doit être certifiée par plusieurs identités existantes dans le cadre d'une "toile de confiance" (Web of Trust).

Ces certifications sont appliquées par des identités à des identités, et se déclare au travers d'un document. Là encore l'identité certifiée est contenue dans le document.

```
Version: 10
Type: Certification
Currency: CURRENCY_NAME
Issuer: PUBLIC_KEY
IdtyIssuer: IDTY_ISSUER
IdtyUniqueID: USER_ID
IdtyTimestamp: BLOCK_UID
IdtySignature: IDTY_SIGNATURE
CertTimestamp: BLOCK_UID
CERTIFIER_SIGNATURE
```




Certification

Ex: L'identité "lolcat" certifiée par une identité dont la clé publique est "DNann...". On remarque que l'identité à certifiée est incluse dans la certification, mais pas l'identité certifiante : en effet, pour avoir une valeur une certification ne peut être prodiguée que par une identité déjà connue.

```
Version: 10
Type: Identity
Currency: beta_brousouf
Issuer: HgTTJLAQ5sqfknMq7yLPZbehtuLSsKj9CcxWN7k8QvYJd
UniqueID: lolcat
Timestamp: 32-DB30D958EE5CB75186972286ED3F4686B8A1C2CD
J3G9oM5AKYZNLAB5Wx499w61NuUoS57JVccTShUbGpCMjCqj9yXXqNq7dyZpDWA6BxipsiaMZhuJMeBfCznzyci
```

```
Version: 10
Type: Certification
Currency: beta_brousouf
Issuer: DNann1Lh55eZMEDXeyt59bzHbA3NJR46DeQYCS2qqdLV
IdtyIssuer: HgTTJLAQ5sqfknMq7yLPZbehtuLSsKj9CcxWN7k8QvYJd
IdtyUniqueID: lolcat
IdtyTimestamp: 32-DB30D958EE5CB75186972286ED3F4686B8A1C2CD
IdtySignature: J3G9oM5AKYZNLAB5Wx499w61NuUoS57JVccTShUbGpCMjCqj9yXXqNq7dyZpDWA6BxipsiaMZhuJMeBfCznzyci
CertTimestamp: 36-1076F10A7397715D2BEE82579861999EA1F274AC
SoKwoa8PFfCDJWZ6dNCv7Xs tezHcc2BbKiJgVDXv82R5zYR83nis9dShLgWJ5w48noVUHimdngzYQneNYSMV3rk
```



Membership

Pour intégrer un le WoT, un membre qui possède une identité doit déclarer sa volonté de l'intégrer, ce au travers de l'émission d'un document Membership.

```
Version: VERSION
Type: Membership
Currency: CURRENCY_NAME
Issuer: ISSUER
Block: M_BLOCK_UID
Membership: MEMBERSHIP_TYPE
UserID: USER_ID
CertTS: BLOCK_UID
SIGNATURE
```

IN ou OUT (pour se désinscrire).



Transaction

Les transactions sont au coeur de la notion de propriété de la monnaie dans une blockchain. C'est leur agrégation dans la blockchain qui certifie l'origine du montant de chaque identité.

Dans Dunitier, la capacité à posséder de l'argent n'est pas liée au fait de faire partie de la communauté. Il suffit de posséder la clé privée permettant de dépenser un montant dans une transaction.

Chaque transaction réfère à de précédentes transaction pour prouver qu'elle possède les fonds qu'elle dit transférer, et donne des conditions pour que cet argent soit dépensé.



Transaction

Les premiers champs sont habituels dans les documents d'unité.

- Locktime: tps avant d'être inclus dans la blockchain
- Issuers: clés publiques d'identités voulant dépenser
- Inputs: Tx précédentes, sources de l'argent
- Unlocks: "clés" données aux transactions précédentes pour débloquent leurs fonds
- Outputs: sorties d'argent, contenant des conditions pour être débloquentées par les Unlocks de futures tx
- SIGNATURES: signatures certifiant les identités du champ Issuers

```
Version: VERSION
Type: Transaction
Currency: CURRENCY_NAME
Blockstamp: BLOCK_UID
Locktime: INTEGER
Issuers:
PUBLIC_KEY
...
Inputs:
INPUT
...
Unlocks:
UNLOCK
...
Outputs:
AMOUNT:BASE:CONDITIONS
...
Comment: COMMENT
SIGNATURES
...
```

Transaction

Ex: Ici, l'identité liée à la clé "**HsLSh..**" veut distribuer 30 beta_brousouf de la tx "**8361C9...**"
Si on va voir cette transaction, il est à parier qu'il y ait une entrée du champ Output =
30:0:SIG(HsLSh...) rendant cette tx valide. Elle les envoie ensuite à "**BYfW...**" et s'en garde 5 (envoie à elle même) en l'écrivant dans le champ Output sous la forme 25:0:SIG(BYfW...)

```
Version: 10
Type: Transaction
Currency: beta_brousouf
Blockstamp: 204-00003E2B8A35370BA5A7064598F628A62D4E9EC1936BE8651CE9A85F2E06981B
Locktime: 0
Issuers:
HsLShAtzXTVxeUtQd7yi5Z5Zh4zNvbu8sTEZ53nfKcqY
Inputs:
30:0:T:8361C993631BED4733972ED7538E41CCC33660F554E3C51963E2A0AC4D6453D3:3
Unlocks:
0:SIG(0)
Outputs:
25:0:SIG(BYfWYFrSyjpvFysgu19rGK3VHBkz4MqmQbNyEuVU64g)
5:0:SIG(HsLShAtzXTVxeUtQd7yi5Z5Zh4zNvbu8sTEZ53nfKcqY)
Comment: First transaction
```

```
42yQm4hGTJYwkPg39hQAUGP6S6EQ4vTfxdJuxKEHL1ih6YHiDL2hcwrFgBHjXLRgxRhj2VNVqqc6b4JayKqTE14r
```

Transaction

Pour débloquent des sources d'argent, on utilise des fonction de locking/unlocking.

Dans le champ Unlocks, ces fonctions sont séparées par des espaces : chacune s'applique à une fonction de lock dans le champ Output auquel l'index fait référence.

Dans le champ Outputs, on les sépare par des opérateurs logiques pour combiner les conditions à remplir.

```
Version: 10
Type: Transaction
Currency: beta_brousouf
Blockstamp: 204-00003E2B8A35370BA5A7064598F628A62D4E9EC1936BE8651CE9A85F2E06981B
Locktime: 0
Issuers:
HsLShAtzXTVxeUtQd7yi5Z5Zh4zNvbu8sTEZ53nfKcqY
CYYjHsNyg3HMRMpTHqCJAN9McjH5BwFLmDKGV3PmCuKp
9WYHTavLlpmhunFCzUwiiq4pXwvgG65ysjZnjz9H8yB
Inputs:
40:2:T:6991C993631BED4733972ED7538E41CCC33660F554E3C51963E2A0AC4D6453D3:2
70:2:T:3A09A20E9014110FD224889F13357BAB4EC78A72F95CA03394D8CCA2936A7435:8
20:2:D:HsLShAtzXTVxeUtQd7yi5Z5Zh4zNvbu8sTEZ53nfKcqY:46
70:2:T:A0D9B4CDC113ECE1145C5525873821398890AE842F4B318BD076095A23E70956:3
20:2:T:672045B5318777CC52CD38B424F3E40DDA823FA0364625F124ABAE0030E7B5B:5
15:2:D:9WYHTavLlpmhunFCzUwiiq4pXwvgG65ysjZnjz9H8yB:46
Unlocks:
0:SIG(0)
1:HXH(7665798292)
2:SIG(0)
3:SIG(0) SIG(2)
4:SIG(0) SIG(1) SIG(2)
5:SIG(2)
Outputs:
120:2:SIG(BYfwYFrSyjpvfFysgu19rGK3VHBkz4MqmQbNyEuVU64g)
146:2:SIG(DSz4rgncXCytsUMW2JU2yhLquZECd2XpEkpP9g5HyAx)
49:2:(SIG(6DyGr5LFtFmbaJYRvcs9WmBsR4cbJbJ1EV9zBbqG7A6i) || HXH(3EB4702F2AC2FD3FA4FDC46A4FC05AE8CDEE1A85))
Comment: ----@@@---- (why not this comment?)
42yQm4hGTJYwkPg39hQAUGP6S6EQ4vTfXdJuxKEHL1ih6YHiDL2hcwrFgBHjXLRgxRhj2VNVqqc6b4JayKqTE14r
2D96KZwNUvVtcapQPq2mm7J9isFcDCfykwJpVEZwBc7tCgL4qPyu17BT5ePozAE9HS6YvYj51f62Mp4n9d9dkzJoX
2XiBDpuUdu6zCPWGzHXXy8c4ATSSc fFQG9DjmqMZUxDZvt1Dp4m2N5oHYVU foPdrU9SLk4qxi65RNrfCVnvQtQJk
```

Transaction

```
Issuers:
HsLShAtzXTVxeUtQd7yi5Z5Zh4zNvbu8sTEZ53nfKcqY
CYYjHsNyg3HMRMpTHqCJAN9McjH5BwFLmDKGV3PmCuKp
9WYHTavL1pmhunFCzUwiiq4pXwvgG65ysjZnjz9H8yB
Inputs:
40:2:T:6991C993631BED4733972ED7538E41CCC33660F554E3C51963E2A0AC4D6453D3:2
70:2:T:3A09A20E9014110FD224889F13357BAB4EC78A72F95CA03394D8CCA2936A7435:8
20:2:D:HsLShAtzXTVxeUtQd7yi5Z5Zh4zNvbu8sTEZ53nfKcqY:46
70:2:T:A0D9B4CDC113ECE1145C5525873821398890AE842F4B318BD076095A23E70956:3
20:2:T:67F2045B5318777CC52CD38B424F3E40DDA823FA0364625F124B4BE0030E7B5B:5
15:2:D:9WYHTavL1pmhunFCzUwiiq4pXwvgG65ysjZnjz9H8yB:46
Unlocks:
0:SIG(0)
1:XXH(7665798292)
2:SIG(0)
3:SIG(0) SIG(2)
4:SIG(0) SIG(1) SIG(2)
5:SIG(2)
Outputs:
120:2:SIG(BYfWYFrSyjppvFysgu19rGK3VHBkz4MqmQbNyEuVU64g)
146:2:SIG(DS44rgncXCytsUMW2JU2yhlquZEC02XpEkpP9G5HyAx)
49:2:(SIG(6DyGr5LFtFmbaJYRvcs9WmBs94cbJbJ1EV9zBbqG7A6i) || XXH(3EB4702F2AC2FD3FA4FDC46A4FC05AE8CDEE1A85))
42yQm4hGTJYwkPg39hQAUGp6S6EQ4vTfXdxJuxKEHL1ih6YHiDL2hcwrFgBHjXLRgxRhj2VNVqqc6b4JayKqTE14r
2D96KZwNUvVtcapQPqQ2mm7J9isFcDcfykWjPVEZwBc7tCg14qPyu17BT5ePozAE9HS6Yvj51f62Mp4n9d9dkzJoX
2XiBDpuUdu6zCPWgZHXxy8c4ATSScFfQG9DjmqMZUxDZVt1Dp4m2N5oHYVUfoPdrU9SLk4qxi65SRNrfCVnvQtQJk
```

déblocage

blocage

- **SIG**: dans un Unlock, SIG(index) débloquent une condition Output = SIG(pubkey) où Issuers[index] = pubkey, et bien sûr pubkey vérifiée par la signature du document.
- **XXH**: fonction de déblocage portant sur un mdp. La condition Output=XXH(HASH) est débloquée par un Unlock = XXH(PASSWORD) avec SHA256(PASSWORD)=HASH.



Transaction

- CLTV: condition pour débloquent l'argent après une certaine date.
Output=CLTV(TIMESTAMP)
- CSV: condition pour débloquent l'argent après un certain delai. Output=CSV(Delay)

```
Version: 10
Type: Transaction
[...]
Outputs
25:2:CLTV(1489677041)
```




Block

Les transactions sont accumulées au sein de blocks, représentés par des documents Blocks. Les informations importantes sont: