Blockchain

Sylvain Conchon

Laboratoire Méthodes Formelles

Université Paris-Saclay, CNRS, ENS Paris-Saclay

sylvain.conchon@universite-paris-saclay.fr

INTRODUCTION À TEZOS

Tezos

La blockchain Tezos est publique et open-source. Elle est dédiée au développement de smart contractsq et à la cryptomonaie `tez` (XTZ).

Tezos

La blockchain Tezos est publique et open-source. Elle est dédiée au développement de smart contractsq et à la cryptomonaie `tez` (XTZ).

Caractéristiques principales :

Tezos

La blockchain Tezos est publique et open-source. Elle est dédiée au développement de smart contractsq et à la cryptomonaie `tez` (XTZ).

Caractéristiques principales :

- Un protocole reposant sur un consensus de type preuve d'enjeu (*Liquid proof of stake*), très peu consommateur d'énergie.

Tezos

La blockchain Tezos est publique et open-source. Elle est dédiée au développement de smart contractsq et à la cryptomonaie `tez` (XTZ).

Caractéristiques principales :

- Un protocole reposant sur un consensus de type preuve d'enjeu (*Liquid proof of stake*), très peu consommateur d'énergie.
- Un système de gouvernance intégré au protocole (*self-amending governance*) qui lui permet d'évoluer régulièrement, en toute transparence et de manière démocratique (par des votes).

Tezos

La blockchain Tezos est publique et open-source. Elle est dédiée au développement de smart contractsq et à la cryptomonaie `tez` (XTZ).

Caractéristiques principales :

- Un protocole reposant sur un consensus de type preuve d'enjeu (*Liquid proof of stake*), très peu consommateur d'énergie.
- Un système de gouvernance intégré au protocole (*self-amending governance*) qui lui permet d'évoluer régulièrement, en toute transparence et de manière démocratique (par des votes).
- Développé en OCaml, ce qui permet en particulier de faciliter le dévelopopement et la vérification formelle de son implémentation.

Tezos

La blockchain Tezos est publique et open-source. Elle est dédiée au développement de smart contractsq et à la cryptomonaie `tez` (XTZ).

Caractéristiques principales :

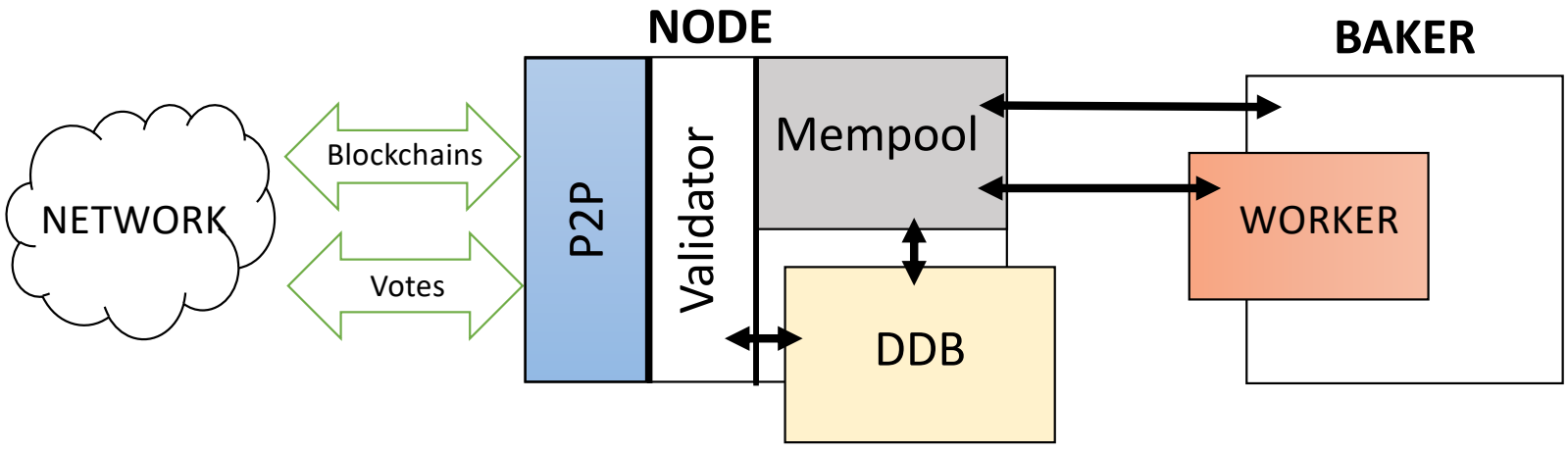
- Un protocole reposant sur un consensus de type preuve d'enjeu (*Liquid proof of stake*), très peu consommateur d'énergie.
- Un système de gouvernance intégré au protocole (*self-amending governance*) qui lui permet d'évoluer régulièrement, en toute transparence et de manière démocratique (par des votes).
- Développé en OCaml, ce qui permet en particulier de faciliter le développopement et la vérification formelle de son implémentation.
- Son langage de smart contracts, Michelson, est purememt fonctionnel et limite certaines attaques (reentrancy).

Liquid Proof of stake

LPoS est une évolution de DPos (Delegated Proof of Stake) qui permet un acteur de déléguer ses droits de baking (proportionnels aux tokens possédés) sans que les délégués aient la garde de ses tokens.

Le principal intérêt de cette variante est que les acteurs qui délèguent peuvent récupérer leurs tokens en dépôt à tout moment (contrairement au mécanisme dans Ethereum).

Architecture simplifiée de Tezos



Fonctionnement d'un nœud

- communique et échange des blockchains (complètes ou seulement les têtes) avec les autres nœuds
- Maintient la meilleure version de la blockchain qu'il a obtenu
- Passe les opérations reçues aux bakers avev qui il est connecté

Fonctionnement d'un baker

- reçoit les deux blocs de tête de la blockchain du Mempool (seuls 2 bocs sont nécessaires dans Tenderbake)
- implémente l'algorithme de consensus pour décider de voter (ou non) sur cette tête
- récupère les votes envoyés par les autres nœuds dans le Mempool pour vérifier l'obtention d'un quorum

Comptes en Tezos

Contrairement au modèle UTXO de Bitcoin, Tezos manipule un ensemble de comptes, avec chacun :

- une adresse
- une somme d'argent accumulée

Il existe deux types de comptes dans Tezos :

- un implicite qui est lié à un manager possédant une **clé publique** ; Le hash de cette clé produit une adresse qui commence par **tz1**.
- un smart contract qui sont créés (on dit originés) à l'aide d'une opération spéciale appelée origination. Ces comptes n'ont pas de clés (publiques/privées) et leur adresse commence par **kt1**.

  Un smart contract est associé à un programme écrit dans le langage Michelson et à un état mémoire.

Opérations (1/2)

En Tezos, les nœuds du réseau envoient des opérations. Cette notion rassemble

- les transactions : transferts de jetons ou appels de smart contracts ;
- les originations de contrats ;
- les votes des bakers ;
- les propositions de blocs ;
- etc.

Les opérations sont enregistrées dans les blocs de la blockchain.

Opérations (2/2)

Une opération prend la forme d'un message avec (au moins) les informations suivantes :

- amount : montant envoyé
- destination : adresse (kt1, tz1) de destination
- parameters : si kt1, paramètres passés au smart contract
- counter : un compteur pour éviter les *replay attacks*
- fee : chaque opération a un coup pour l'utilisateur

Format d'une opération (1/2)

Exemple d'une opération pour appeler un smart contract :


```
{
    "branch": "BMXRpSqjJ9HnEeaSXj3YzM9jqB4kqDZemtJBGGqn5Sa9MepV1k7",
    "contents": [
        {
            "kind": "transaction",
            "source": "tz1YWK1gDPQx9N1Jh4JnmVre7xN6xhGGM4uC",
            "fee": "6678",
            "counter": "942780",
            "gas_limit": "63669",
            "storage_limit": "75",
            "amount": "0",
            "destination": "KT1S5hgipNSTFehZo7v81gq6fcLChbRwptqy",
            "parameters": {
                "entrypoint": "sellLand",
                "value": {
                    "prim": "Pair",
                    "args": [
                        {"int": "100000000"},
                        {"int": "11"}
                    ]
                }
            }
        }
    ]
}
```

Format d'une opération (2/2)

branch fait référence à un bloc récent (supposé valide) pour contrer les attaques de réorganisation de la blockchain.

fee contient les frais de transaction

gas_limit estimation du coup en gaz d'une transaction ; cette limitation permet d'éviter les exécution trop longues (voire infinies)

storage_limit quantité maximum de mémoire allouée par un appel de smart contract

Traitement d'une opération Tezos