NUNES DA COSTA Jordan

BARON Paul

JAYR Reynald

DEWERDT Aurelien

BitBet: BlockChain de paris sportifs

# Présentation du contexte

Dans le cadre de notre mastère et de la majeure Blockchain, nous avons pu développer un projet que nous avons nommé Bit bet. C’est un programme blockchain permettant de parier sur les rencontres sportives majeures comme le tennis, le football ou encore le Basketball via des cryptomonnaies. Les différentes mises des cryptomonnaies versées se retrouvent dans un pot qui sera redistribué pour les différentes personnes ayant eu le bon résultat et selon un ratio de ce que nous avons parié. Prenons l’exemple d’un match de tennis entre Nadal et Federer, les différents parieurs vont utiliser la blockchain et placer leurs mises (en cryptomonnaies) sur l’un des deux joueurs. Une fois le résultat du match entré et validé dans la blockchain, les joueurs ayant trouvé le bon résultat se redistribue la totalité du pot en fonction de leur mise initiale.

Dans le cadre de la Blockchain, un problème se pose : Qui peut certifier le résultat d’un match et permettre la répartition et la récupération des gains ? Nous avons référencé 3 solutions qui vous seront décrites ci-dessous. La Blockchain a pour particularité d’être coupé du monde extérieur. En effet, la blockchain ne permet pas la collecte de données provenant de sources externes, c’est même un obstacle à cause de son fonctionnement.

# Les différentes possibilités de validation des paris

## La mise en place d’un Oracle

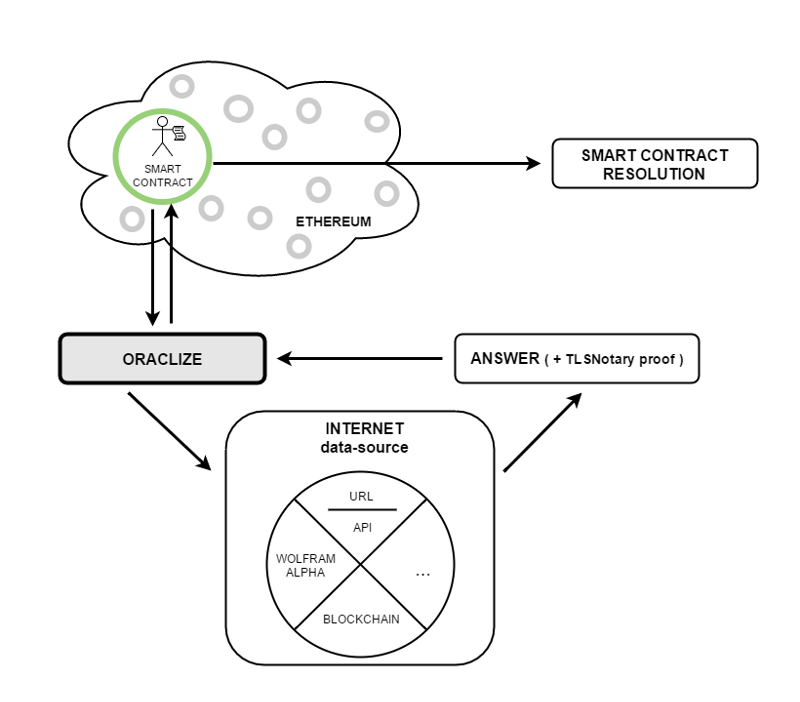
L’Oracle est un service ou une personne qui sert de référent à la Blockchain. Il est chargé d’entrer manuellement une donnée extérieure dans la blockchain afin de valider dans notre cas un résultat sportif. Le service ou la personne va récupérer les informations du match afin de l’insérer dans la blockchain à l’endroit approprié. Lorsque le smart-contract réceptionne les informations, il va aller chercher les données sur la blockchain, aux différentes adresses prévues pour les matchs et va permettre la décision de récupérer ou non les gains en fonction du résultat. Si nous avons le bon résultat, alors nous gagnons une somme du pot définis au prorata et en fonction de la somme que nous avions parié au départ.

L’intervention d’un Oracle, pose de nombreuses questions : Qui est cet Oracle ? comment lui accorder de la crédibilité et de la confiance ?

L’oracle est généralement rémunéré et provient d’une personne ou d’une société qui répond spécifiquement aux informations qu’il doit valider. Son but étant de renseigner l’information demandée. Cependant, cette personne peut être désignée par les participants de la blockchain et notamment du smart-contract ou par la personne qui a créé le smart-contract lui-même. Nous lui accordons une confiance ultime.

Si aucune information de résultat n’est renseignée, alors le contrat est annulé et chacun récupère sa mise de départ. Lorsqu’une information, un résultat est entré et enregistré dans la blockchain, le programme va prendre comme base cette information afin de valider ou non les éventuels gains gagnés. Si le résultat est positif pour l’utilisateur, celui-ci aura alors un bouton lui permettant de récupérer ses gains.

Afin de garantir la fonction de l’Oracle et que celle-ci ne prenne pas trop d’ampleur, nous faisons appel à un oraclise. Il fonctionne de la manière suivante:



“Le fonctionnement d’Oraclize”

Selon la définition, “l’*Oraclize* et les oracles similaires fonctionnent avec une « preuve d’honnêteté » (*TLS Notary proof*) qui garantit que la donnée entrée sur la blockchain est identique à celle qui a été récupérée par Oraclize. Comme la blockchain, cette preuve est publique et vérifiable par l’utilisation de méthodes cryptographiques. Cela signifie que si Oraclize entre un jour dans la blockchain une donnée non-conforme à la donnée récupérée sur le serveur, cette information « malhonnête » sera immédiatement repérable par n’importe quelle personne au fait de ces techniques. ”.

Pour conclure sur l’Oracle, nous pouvons dire qu’il en existe deux types: des Oracles publics ou privés et ils vont avoir pour rôle de jouer un rôle déterminant dans le développement des applications décentralisées notamment par la validation de faits extérieurs.

## Faire appel à une API

## 

Nous avons également la possibilité de nous baser sur des API sportives qui serviront de références à la validation d’un pari et donc d’un smart contract. En effet, avec les différentes possibilités de validation que nous avons cité précédemment, nous pourrons permettre aux différentes personnes de voir le résultat directement dans la blockChain. Dans notre cas, les résultats sont validés dans le smart-contract par une entité supérieure. Les API ont pour but d’avoir un rôle complémentaire à la Blockchain et peuvent même être considéré comme des maillons forts en terme de sécurité et de fiabilité. En effet, le stockage, le chiffrement et la validation des transactions d’une chaîne de blocs doivent aussi avoir des connexions et des intégrations avec le monde extérieur et notamment les API web. Les API et notamment les API en liens avec le sport nous servent ici de références, elles sont des processus transactionnels essentiels de la Blockchain. Cependant les API restent compliquées à mettre en place sans des infrastructures de gestion appropriées. A travers notre projet Bibtet, nous avons créé différents smart-contrat dont un avec un 'oracle' qui joue comme autorité, en recevant les infos de l'API. Une fois les matchs terminés, l'API indique au smart-contract (notre oracle) les différents résultats. De nouvelles API apparaissent constamment de nos jours et sont utilisées notamment pour les transactions liées à la cryptomonnaie.

## La mise en place d’une plate-forme comme projet Augur

Augur est un “marché de prédiction décentralisé basé sur la Blockchain Ethereum”, il permet de parier sur des événements qui se produise ou non comme par exemple les événements sportifs et de parier sur le vrai ou faux, le oui ou non ou encore le gagnant perdant. La particularité de ce projet est que la validation d’un événement est réalisé par les utilisateurs eux-mêmes. En effet, les utilisateurs d’Augur utilisent des tokens de réputation nommé REP pour juger de leur réputation sur le marché. Selon le résultat d’un événement, les utilisateurs vont rendre compte par eux même du résultat en utilisant leur jeton.

Contrairement au système de l’Oracle et de l’autorité suprême, le résultat d’un événement n’est pas communiqué par une autorité centrale, mais par les différents utilisateurs. Lorsque les utilisateurs donnent et valident le bon résultat de l’événement, alors les utilisateurs reçoivent un bonus et gardent leurs jetons, dans le cas contraire, les utilisateurs le perdent et peut payer une “amende”. Cette option rend pratiquement l’erreur impossible.

## Conclusion

A travers ce projet, nous avons pu apprendre et nous familiariser avec le concept de la BlockChain et des cryptomonnaies. BitBet nous a permis de voir qu’il était dans un premier temps illégal de réaliser ce type de transactions dans la blockchain mais grâce à ce projet, nous avons surtout pu identifier les différentes validations possibles d’événements à la Blockchain. Nous avons identifié trois solutions, la première était d'utiliser un oracle qui a pour objectif d’être impérial et ne pas être contesté, tout dépend de son intégrité et sa capacité à valider les différents résultats. La seconde était la mise en place d’une API qui viendrait se greffer comme élément externe à la BlockChain afin de valider les résultats des matchs et confrontations. Enfin, la dernière solution était de se baser sur le projet Augur et notamment sur le fait de laisser la main aux différents utilisateurs de valider un résultat. Suite à celui-ci l’utilisateur se verrait récompensé ou pénalisé en fonction du résultat qu’il a communiqué. Nous avons pu aborder différentes solutions dans la mise en place technique de notre projet, nous avons utilisé et créée un smart-contrat dédié à l’oracle pour la validation des résultats. afin que celui-ci puisse valider correctement le résultat de tel ou tel confrontation, nous avons utilisé un élément extérieur à la blockchain: une API comportant les différents résultats de match de tennis.