Blockchain

Smart Contracts

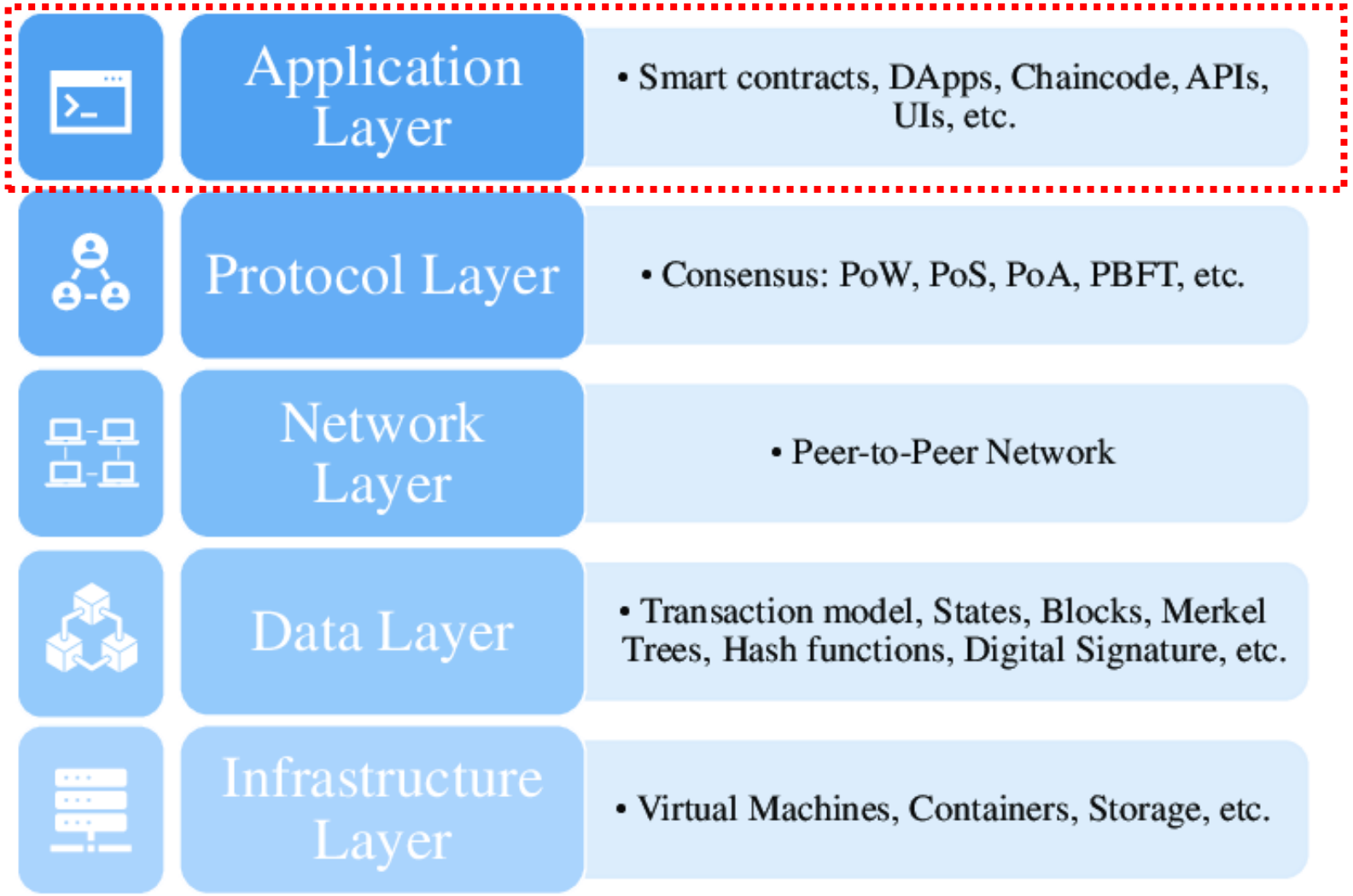
Contrats intelligents

العقود الذكية

Fondamentaux des smart contracts

- Qu'est-ce qu'un smart contract ?
- Quelle est la différence entre un smart contract et un contrat traditionnel ?
- Quels sont les avantages principaux des smart contracts ?
- Sur quelle blockchain les smart contracts sont-ils principalement déployés ?

Les couches de blockchain



Pourquoi le Smart Contrat ?

Un **contrat traditionnel** est un accord légal entre deux ou plusieurs parties qui crée des obligations et peut être exécuté par voie judiciaire en cas de non-respect.

Composantes d'un contrat traditionnel

- **Offre:** C'est le point de départ de toute négociation contractuelle. L'offre **est une proposition** qui doit être suffisamment précise pour permettre à l'autre partie de **l'accepter ou de la refuser**.
- **Acceptation:** L'acceptation l'accord sans réserve de l'offrant aux termes de l'offre. Elle doit être claire, **inconditionnelle** et portée à la connaissance de l'offrant.
- **Considération :** La considération est l'élément qui donne à un contrat sa force obligatoire. C'est l'échange de quelque chose de valeur entre les parties contractantes. Cette valeur peut être de nature **monétaire (prix),** mais elle peut aussi être constituée d'une promesse, d'un **service** ou d'une renonciation à un droit.

Etape du processus de formation d'un contrat

1) Intention de créer des relations légales : Ce premier élément est fondamental. Il signifie que les parties qui signent un contrat ont l'intention de se créer des obligations légales réciproques. Sans cette intention, il n'y a pas de contrat au sens juridique du terme.

- **Exemple** : Dans un contrat de vente, les deux parties doivent clairement exprimer leur intention de conclure une relation légale, ce qui les lie juridiquement à exécuter leurs obligations respectives, comme payer le prix ou livrer un bien.

Etape du processus de formation d'un contrat

2) Accord (Agreement) : Il s'agit d'un accord mutuel des parties sur les termes du contrat. Cet accord se manifeste généralement par une **offre** et une **acceptation**.

- **Exemple** : Un vendeur propose de vendre une voiture pour 100 000 DA à un acheteur, et l'acheteur accepte cette offre. L'accord est formé lorsque l'acheteur exprime son consentement sans condition, rendant l'offre du vendeur valide.

Etape du processus de formation d'un contrat

3) Considération : La considération est l'échange de quelque chose de valeur entre les parties. Ce peut être de l'argent, un bien, un service, ou même une promesse.

- **Exemple** : Dans l'achat de la voiture, l'acheteur s'engage à payer 100 000 DA en échange de la voiture que le vendeur s'engage à livrer.

  Cette somme d'argent représente la **considération** pour le contrat.

Etape du processus de formation d'un contrat

4) Capacité juridique (Legal capacity) : Les parties doivent être majeures et avoir leurs droits civils pour pouvoir conclure un contrat.

- **Exemple** : Si l'acheteur de la voiture **est un mineur** ou une personne sous tutelle, il pourrait **ne pas être capable de conclure ce contrat sans l'accord de ses parents ou tuteurs**. Cela garantirait que l'acheteur a la capacité juridique pour s'engager dans l'achat.

Etape du processus de formation d'un contrat

5) Légalité de l'objet du contrat (Legality of objects of the contract) : L'objet du contrat ne doit pas être illégal et doit être réalisable.

- **Exemple** : Si le vendeur propose une voiture volée à l'acheteur, l'objet du contrat serait illégal, car il porte sur un bien volé. Dans ce cas, **le contrat serait nul**, et **l'acheteur ne pourrait pas être tenu responsable de l'achat.**

Etape du processus de formation d'un contrat

6) L'accord authentique est une décision libre, éclairée et volontaire, donnée de manière autonome pour une action précise et pouvant être retirée à tout moment.

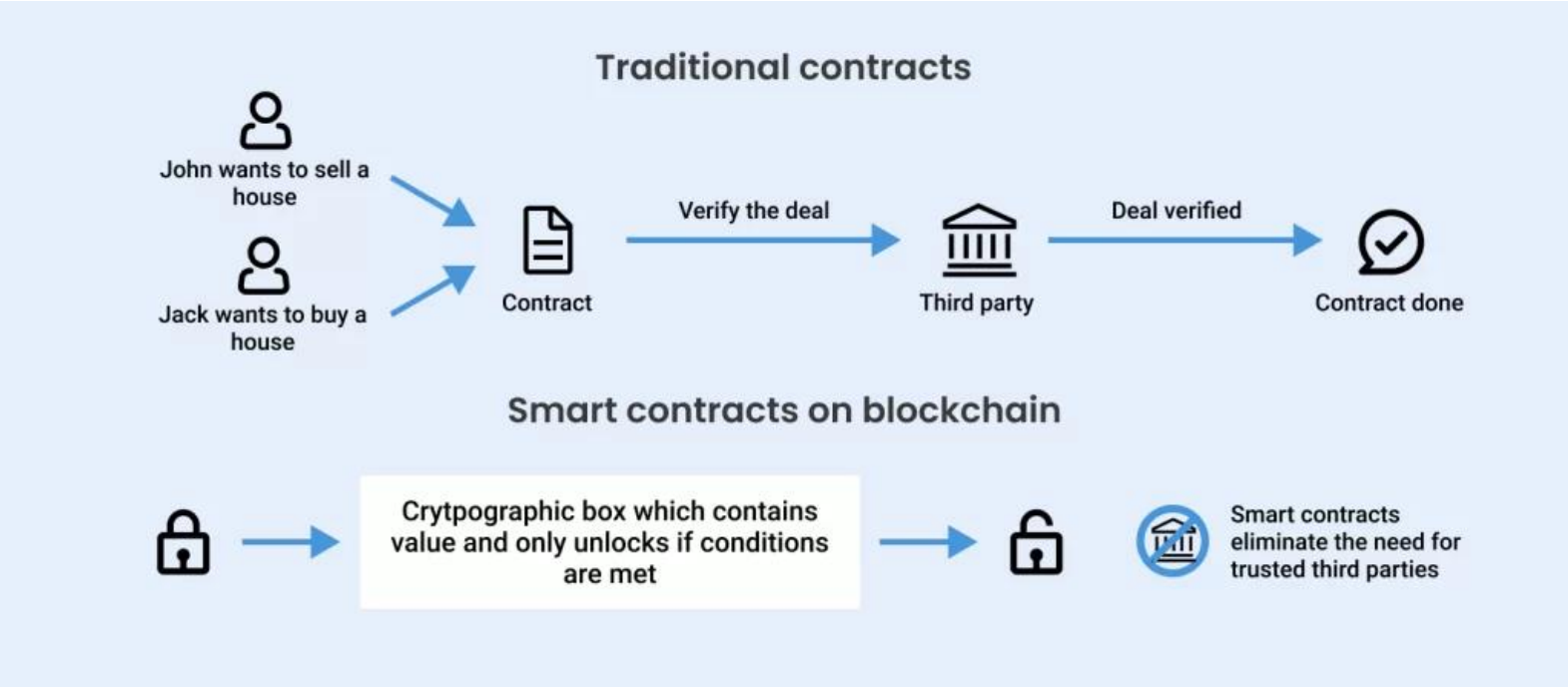
- **Exemple** : L'acheteur choisit d'acheter la voiture librement, sans pression. Si le vendeur avait menacé l'acheteur ou donné de fausses informations, l'accord de l'acheteur ne serait pas valable. Par exemple, si l'acheteur avait été trompé sur l'état de la voiture (comme un défaut caché), **il pourrait contester l'accord**

Etape du processus de formation d'un contrat

- **7) La légalité de l'objet du contrat** signifie que l'objet ou la finalité du contrat doit être conforme à la loi et à l'ordre public. Un contrat ne peut pas être valide si son objet implique une activité illégale, immorale ou interdite par la législation
    - **Exemple** : Dans l'exemple de l'achat de la voiture, l'objet du contrat est licite tant que la voiture est légalement acquise et qu'il n'y a pas de violation de la loi, comme la vente d'une voiture volée ou l'achat d'un véhicule avec des documents falsifiés

Besoin de traduire l’engagement contractuel en code informatique ??!!

Pourquoi le Smart Contrat ?

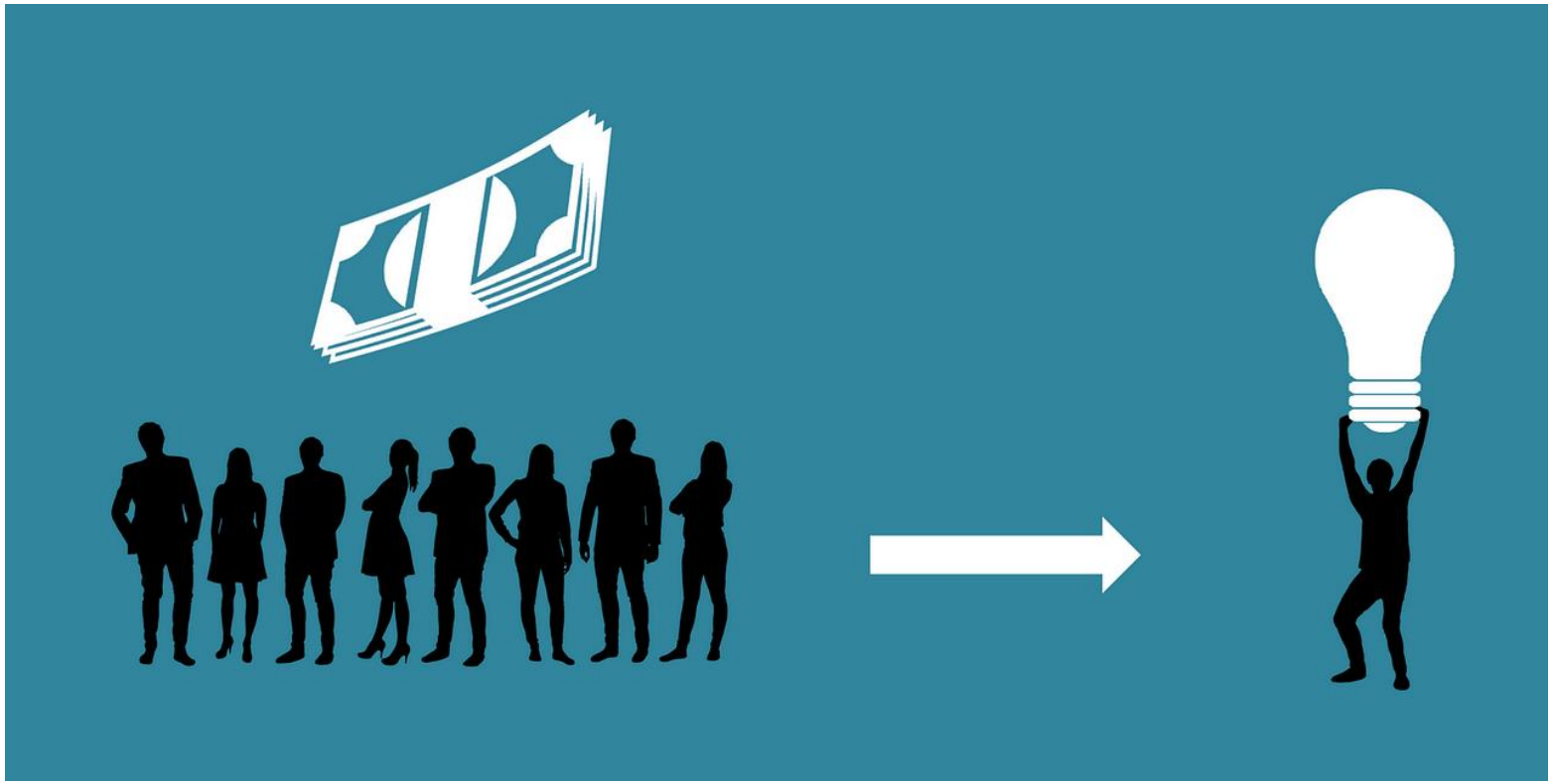


- Décentralisation
- Immutabilité
- Transparence
- Automatisation
- Réduction des coûts
- Sécurité

Pourquoi le Smart Contrat ?

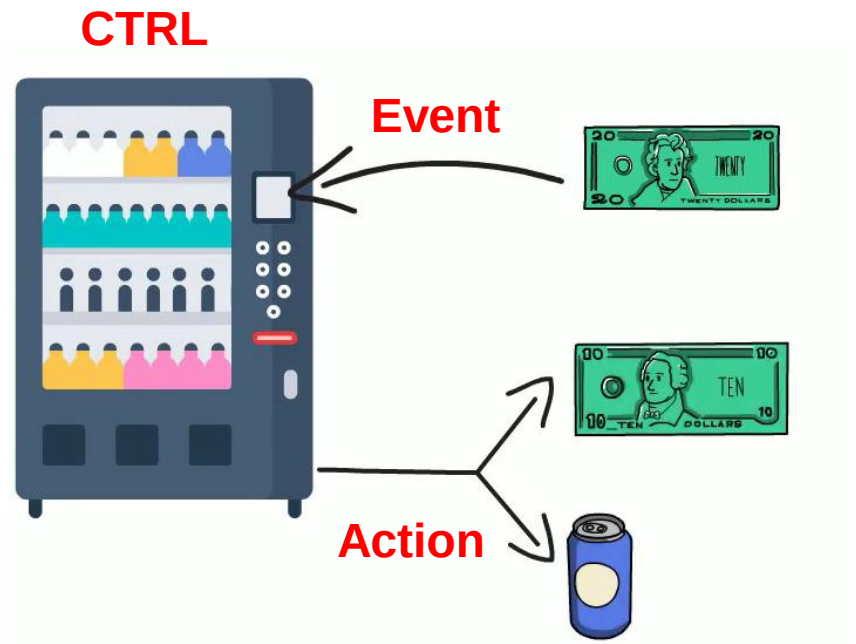
Problème de confiance ?

Exemple
de **crowdfunding**



Le **crowdfunding** cherche des financements, tandis que le **crowdsourcing** cherche des contributions en termes d'idées ou de travail.

Illustration des exemples avec le paradigme ECA



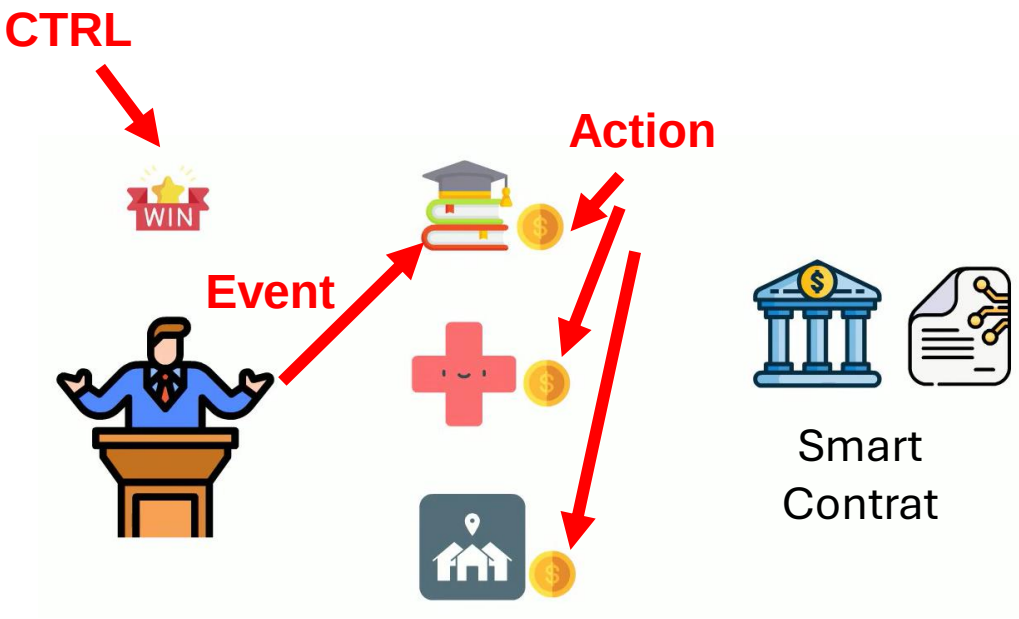


Illustration des exemples avec le paradigme ECA

Illustration des exemples avec le paradigme ECA

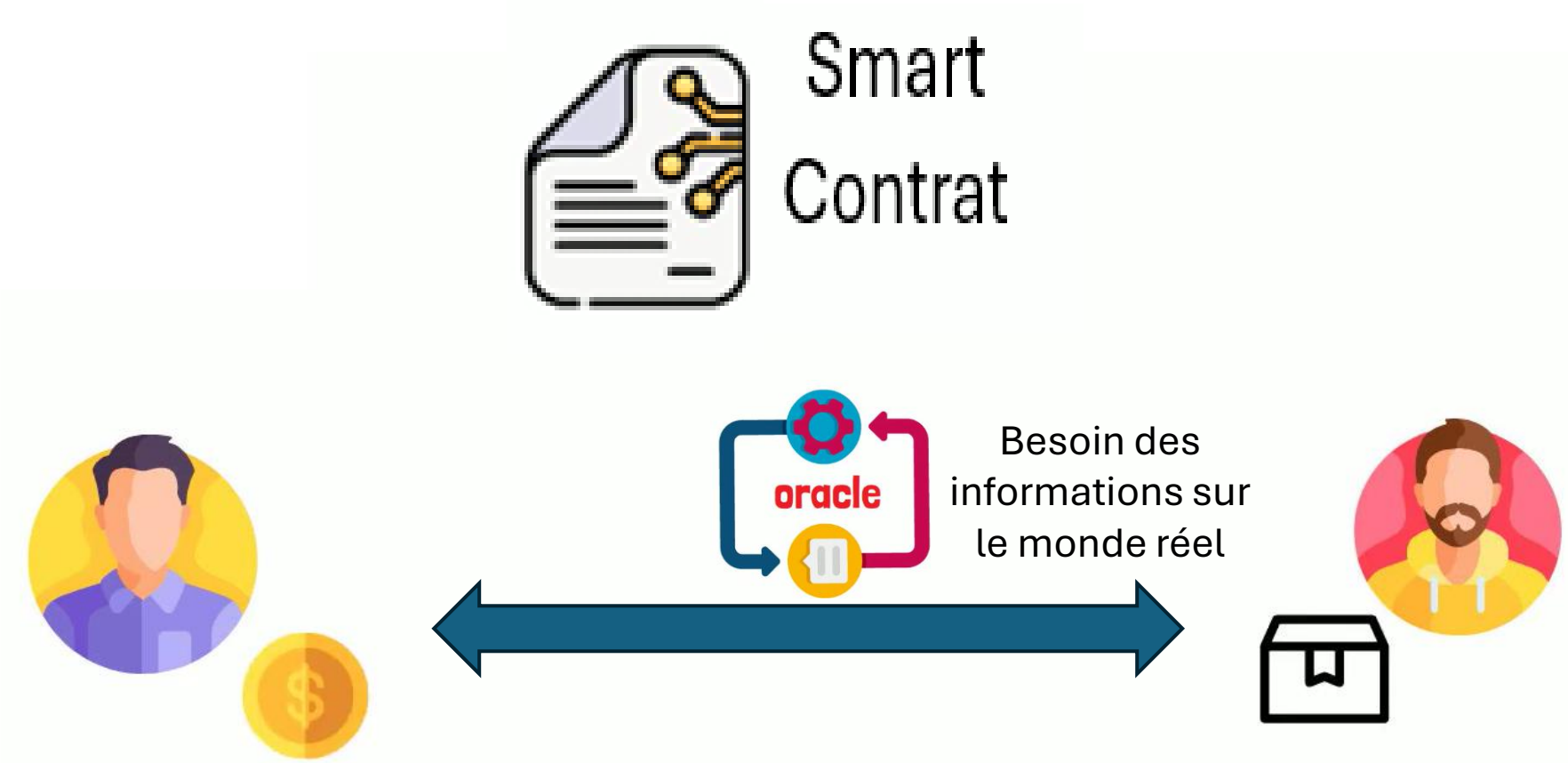
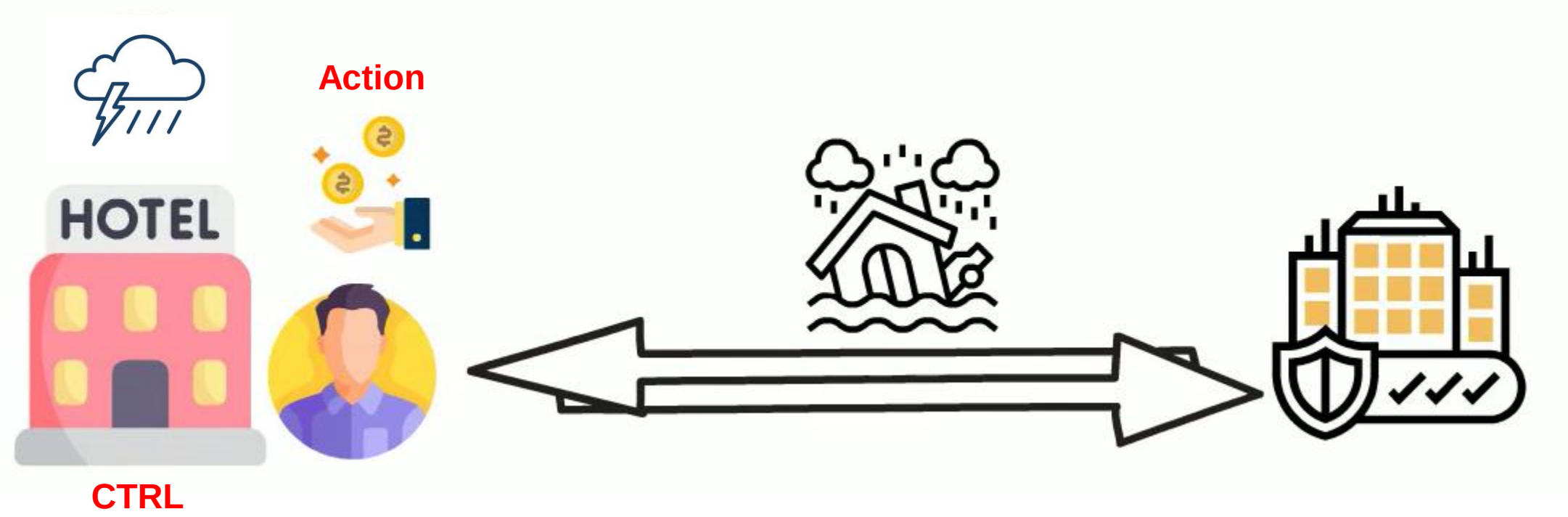


Illustration des exemples avec le paradigme ECA

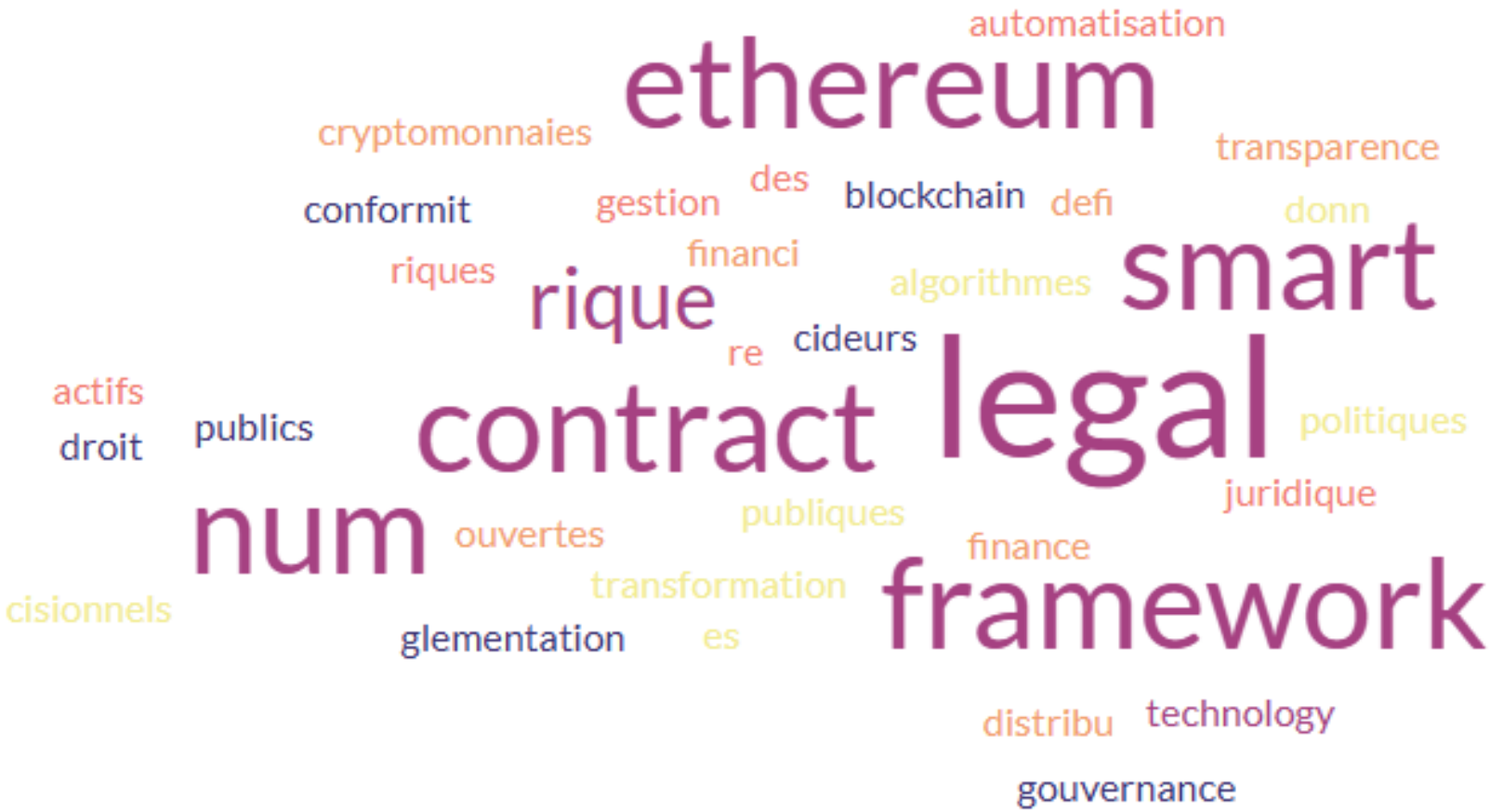


Le smart contract, une nouvelle technologie

- « Vers la disparition de certains métiers » (Mme de Silguy, sur *Blockchain, la nouvelle révolution numérique*).

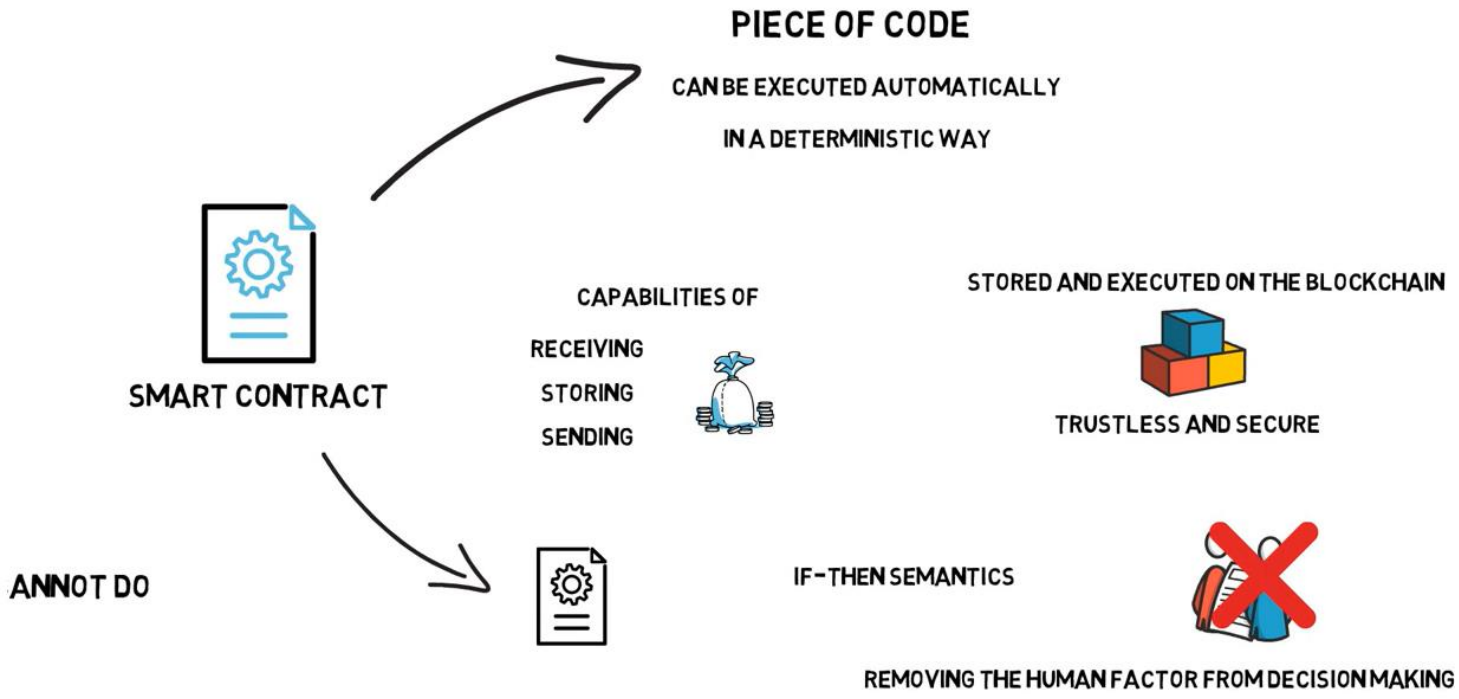
- Influence du numérique dans la redéfinition de professions judiciaires et juridiques

- Le smart contract est une application construite sur une technologie plus large, la BLOCKCHAIN.


automatisation
ethereum
cryptomonnaies
transparence
des
gestion
blockchain
defi
donn
conformit
financi
riques
rique
algorithmes
smart
re
cideurs
legal
actifs
contract
publics
politiques
droit
juridique
num
publiques
ouvertes
finance
framework
transformation
cisionnels
glementation
es
distribu
technology
gouvernance

Pourquoi faire confiance au smart contract ?

- **Définition :** Les smart contracts sont des programmes stockés sur une blockchain qui s'exécutent lorsque des conditions prédéfinies sont remplies.
- **Objectif :** Ils automatisent l'exécution d'accords, garantissant que tous les participants peuvent immédiatement vérifier le résultat sans avoir recours à des intermédiaires ni subir de délais.



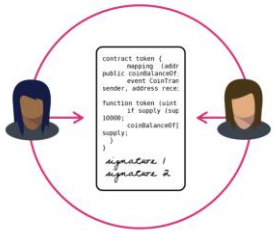
Smart contract

Le terme de *smart contract* a été popularisé par l'informaticien dans son article de 1997, « *The Idea of Smart Contracts* ».

Smart contract ≠ **Contrat**

Smart contract = **Programme**

Df. Le *smart contract* peut être défini comme un protocole informatique ayant pour objet de conclure, exécuter ou mettre un terme automatiquement à un contrat. *Le smart contract* désigne donc la technologie qui répond à cet objectif et non le contrat lui-même.



La technologie qu'est le *smart contract* repose sur la *blockchain*. C'est à partir de celle-ci (et notamment de la *blockchain* Ethereum) que les *smart contracts* sont créés (rédaction en langage de programmation).

Les contrats intelligents sont les transactions effectuées sur un réseau blockchain.Ils doivent être compilés et migrés vers le réseau. Les contrats sont vérifiés au fur et à mesure de leur téléchargement sur le réseau et sont cohérents sur toutes les machines pour garantir leur validité.

Quel intérêt présente le smart contract ?

- **Le smart contract est <u>efficace</u>** : il permet l'accomplissement automatique de l'obligation
- **Le smart contract est <u>rapide</u>** :l'exécution ne nécessite pas l'intervention des parties
- **Le smart contract est <u>sûr</u>** : grâce aux caractéristiques de la blockchain.
- **Garantie par la force** : L'obligation du contrat est assurée par le code informatique et non par le droit traditionnel.
- **Transparence** : Les transactions sont visibles et vérifiables par toutes les parties concernées.
- **Limitation des risques en cascade** : Contrairement aux contrats traditionnels, les risques de défaillance sont réduits grâce à l'automatisation.
- **Élimination des coûts et des intermédiaires** : Les contrats intelligents suppriment les frais liés aux intermédiaires, réduisant ainsi les coûts.

Points faibles des contrats intelligents

- **Bugs dans le code** : En cas d'erreur ou de bug, il peut être très difficile, voire impossible, de corriger ou réparer le contrat une fois déployé.
- **Irreversibilité** : Une fois qu'un contrat est activé, les actions déclenchées sont souvent irréversibles, ce qui peut poser des problèmes si le contrat contient une erreur.
- **Complexité technique** : La conception et le déploiement de contrats intelligents nécessitent des compétences avancées en programmation, ce qui peut limiter leur adoption.
- **Absence de flexibilité juridique** : Les contrats intelligents sont rigides, ils exécutent strictement le code sans prendre en compte des situations inattendues ou des ambiguïtés légales.

Contrat classique Vs **Smart contract**

Critère	Contrat classique	Smart contract
Définition	Accord formel entre deux ou plusieurs parties, régi par des lois.	Programme auto-exécutant qui applique automatiquement les termes d'un contrat.
Nature	Juridique, écrit ou oral, nécessitant parfois des témoins ou des notaires.	Informatique, codé en langage de programmation.
Exécution	Requiert des intermédiaires (avocats, juges, notaires) pour faire respecter les termes.	Exécute automatiquement les actions définies dans le code, sans intermédiaires.
Sécurité	Dépend des parties et de l'autorité légale (tribunaux).	Sécurisé par la blockchain, impossible à modifier une fois déployé.
Temps d'exécution	Peut prendre du temps pour être exécuté, selon la complexité et les parties impliquées.	Instantané et automatique dès que les conditions sont remplies.
Coûts	Peut entraîner des frais juridiques, notariaux et autres.	Réduit les coûts en supprimant les intermédiaires.
Transparence	Peut être privé ou public, selon les parties et les conditions.	Totalement transparent sur la blockchain pour tous les participants.
Modifiabilité	Peut être modifié ou résilié selon l'accord des parties.	Ne peut pas être modifié une fois le contrat déployé.
Dépendance à des tiers	Nécessite des intermédiaires légaux pour sa validation.	Ne dépend pas d’intermédiaires, fonctionne de manière autonome.

Quelques potentialités offertes par le smart contract

- La fonction de registre pour l'administration consiste à enregistrer et archiver les documents officiels pour assurer la traçabilité et la gestion des informations.

- Le domaine de l’assurance

- D’autres domaines : douaniers, gestion de la chaine logistique (supply chain), en lien avec les objets connectés, etc.

Quelques potentialités offertes par le smart contract

- **Secteur bancaire et financier :** Automatisation des prêts, paiements, et transactions sécurisées sans intermédiaires.
- **Immobilier :** Simplification des transactions immobilières, de la gestion des contrats de location à l'achat/vente de biens.
- **Santé :** Gestion sécurisée des dossiers médicaux, automatisation des paiements pour soins de santé et suivi des prescriptions.
- **Propriété intellectuelle :** Protection des droits d'auteur et des brevets, avec des paiements automatiques pour l'utilisation de créations.
- **Énergie :** Gestion des contrats d'énergie, y compris la gestion de la production et de la consommation décentralisées d'énergie.
- **Éducation :** Certification et vérification des diplômes, des parcours d'apprentissage, et des qualifications professionnelles.
- **Art et divertissement :** Gestion des droits d'auteur pour les œuvres musicales, vidéos, et autres créations, avec des paiements automatiques pour les redevances.

Comment fonctionne un smart contract ?

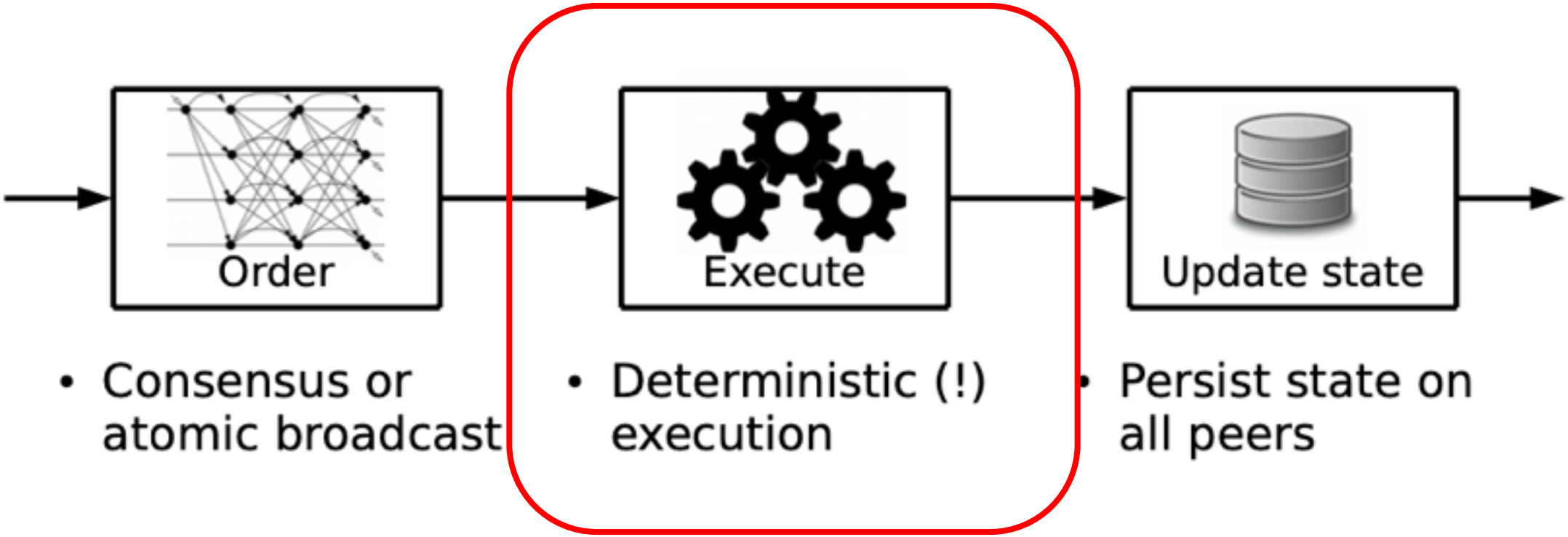
- **Contrat autoexécutant :** il traduit l'engagement contractuel en code informatique pour assurer son exécution automatique

- **Protocole informatique de type :**

« si… [ex. telle condition est vérifiée],

alors… [ex. telle conséquence se produira] » *(« if… then… »)*.

Comment fonctionne un smart contract ?



Source:https://arxiv.org/pdf/1801.10228.pdf

EVM OPCODE (Operation Code) vs Solidity

Ethereum Virtual Machine Operation Code (EVM OPCODE)

- Low level
- Stack-based language
- Similar to Machine Code/Assembly

Usually people write contracts in high level language like Solidity and compile them to OPCODE.

Solidity

- High level
- Solidity can be compiled to OPCODE
- Similar to C++, Java, etc.

OPCODE (Operation Code)

OPCODE is identified by a byte (00 - FF).

This is the current OPCODE in use.

00	01	02	03	04	05	06	07	08	09	0A	0B	-	-	-	-
10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	-	-
20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F
40	41	42	43	44	45	-	-	-	-	-	-	-	-	-	-
50	51	52	53	54	55	56	57	58	59	5A	5B	-	-	-	-
60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F
70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F
80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F
90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	9F
A0	A1	A2	A3	A4	-	-	-	-	-	-	-	-	-	-	-
B0	B1	B2	-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
F0	F1	F2	F3	F4	F5	-	-	-	-	FA	-	-	FD	-	FF

Implémentation

Plateforme est souvent associée aux smart contracts

- **Ethereum** est une plateforme décentralisée basée sur la blockchain, permettant de créer et d'exécuter des smart contracts et des applications décentralisées

- **Langage de programmation est souvent utilisé pour écrire des smart contracts sur Ethereum**

- **Solidity** est un langage de programmation pour écrire des smart contracts sur la blockchain Ethereum.

Traduction en langage informatique

- **Commencer par définir une structure :**

code Solidity

```
struct Bettor {
  address addr;
int8 temperature;
   uint value;
        }
```

➢ **Puis inscrire la relation contractuelle en langage informatique dans la structure :**

code Solidity

```
Bettor private bettor1;
Bettor private bettor2;
uint private betEndTime;
TemperatureOracle private tempOracle;
// end bet and reimburse both bets
function kill() external {
// only bettor1 or bettor2 can end the bet
if(msg.sender != bettor1.addr && msg.sender != bettor2.addr) return;
bettor1.addr.send(bettor1.value);
bettor2.addr.send(bettor2.value);
suicide(msg.sender);
}
function betOn(int8 temperature) external {
if(winnerPaid || now > betEndTime) {
// bet already over, reimburse sent value
msg.sender.send(msg.value);
return;
} if(msg.sender == bettor1.addr) {
// message was sent by bettor 1
bettor1.temperature = temperature;
bettor1.value += msg.value;
} else if(msg.sender == bettor2.addr) {
// message was sent by bettor 2
bettor2.temperature = temperature;
bettor2.value += msg.value;
} else {
// message wasn't sent by either bettor, abort the transaction.
throw;
// the winner gets the whole balance of the contract
uint payOut = address(this).balance;
```

Questions juridiques

- **Les défis posés par le droit des contrats aux smart contracts (encore et encore…)**

- **Le paiement**

- **La preuve**

- **La responsabilité**

Questionnements juridiques et techniques sur les smart contracts

Les défis posés par la technique aux smart contracts

- **La sécurité de la blockchain** (attaque des 51%). Et la question de la confiance…

- **La capacité de la technique** (dépasser le stade du prototype, passage à l'échelle)

- **Les défis posés par le droit des contrats aux smart contracts**

- Absence de **subjectivité** dans le langage informatique (délai raisonnable, meilleurs efforts…)

- Les smart contracts sont **immuables,** sans correction possible ultérieure

- **Les défis posés par le droit des contrats aux smart contracts (encore)**

- Essor des smart contracts dans les **contrats d'adhésion,** certainement plus que dans les **contrats de gré à gré** (art. 1110 du Code civil)

- Intérêt d'obtenir une exécution plus rapide, sûre et efficace.

- **Quid des tempéraments légaux et jurisprudentiels pour protéger la partie faible ?**

Questions ?!!