

Le chiffrement homomorphe

la solution pour la confidentialité des données en IA et blockchain

ZAMA

Zama
est
leader
dans le
FHE

	La + grande équipe R&D en FHE	75 employés, 37 PhDs.
	Technologie état de l'art	22 brevets, 30+ publications.
	Open source	Tout le code de Zama est open-source et les avancées cryptographiques sont publiées
	Financement	Levée de \$70M : Multicoïn, Protocol Labs, Metaplanet, Lunar Ventures, ...
	Communauté dynamique	3000+ développeurs utilisent nos produits open source products et contribuent à notre ecosystem.
	Leadership experimenté	Dr Rand Hindi (CEO, serial entrepreneur), Dr Pascal Paillier (CTO, FHE co-inventor), Prof Nigel Smart (CAO, Prof. KU Leuven), Dr Marc Joye (CSO, 100 publications).

IA et confidentialité

Z

Can you keep a secret?

C

As an AI language model, I am unable to keep secrets in the traditional sense. It's important to avoid sharing personal or sensitive information in our conversations.

Une conversation réelle with ChatGPT-4

Opportunités perdues

TECH

Amazon, Apple, and 12 other major companies that have restricted employees from using ChatGPT

Aaron Mok Jul 11, 2023, 5:38 PM GMT+2

➦ Share

🔖 Save



Blockchains et confidentialité

- Adresses pseudonymes
- Montants en clair

Transactions	Internal Txns	Erc20 Token Txns	Erc721 Token Txns	Erc1155 Token Txns	Analytics	Comments
Latest 25 ERC-20 Token Transfer Events						
View All						
Txn Hash	Age	From	To		Value	Token
 0x61bac8ed64cf49ff537...	1 hr 8 mins ago	 Uniswap V2: KCAL 2		 vitalik.eth	2,500	 Step.app (KCAL)
 0xd9f47a344e278579cb...	1 hr 15 mins ago	Justin Sun		 vitalik.eth	25,143,213.150843308745475521	 Step.app (KCAL)
 0xdea02c32d141997aaa...	12 hrs 57 mins ago	 plamer.eth		 vitalik.eth	1	 AssangeDAO (JUSTIC...)
 0x74205c19a313ba8865...	1 day 11 hrs ago	 Uniswap V2: SEGA 3		 vitalik.eth	227,158,544.808096280091774569	 SEGA (SEGA)
 0xad5c19e1af6de6508e...	2 days 20 hrs ago	0xad29c28a868c945caf9...		 vitalik.eth	21,420	 ERC-20 (BASTAR...)
 0x1014024546d2e94f39...	3 days 4 mins ago	 Uniswap V2: ALIS 2		 vitalik.eth	153,473.76198500365822856	 Acropolis DA... (ALIS)
 0xbffdb2fcd52e96f136c7...	3 days 24 mins ago	 vitalik.eth		 OlympusDAO: DAO Funds	40,323.284453294043855726	 Acropolis DA... (ALIS)

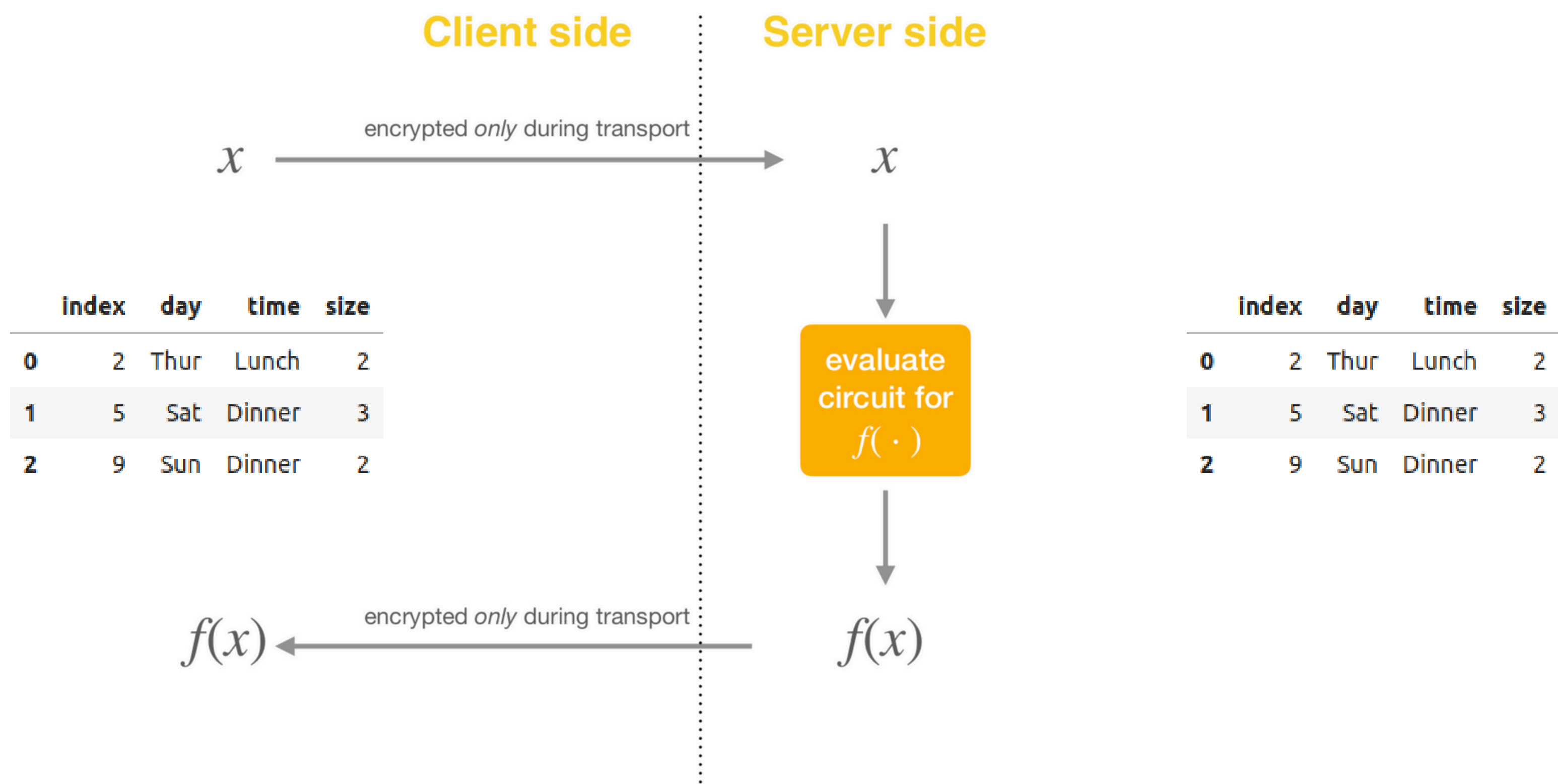
Avantages des blockchains

-  Règlement rapide
-  Atomicité
-  Réglementation programmable
-  Interopérabilité des systèmes de trading

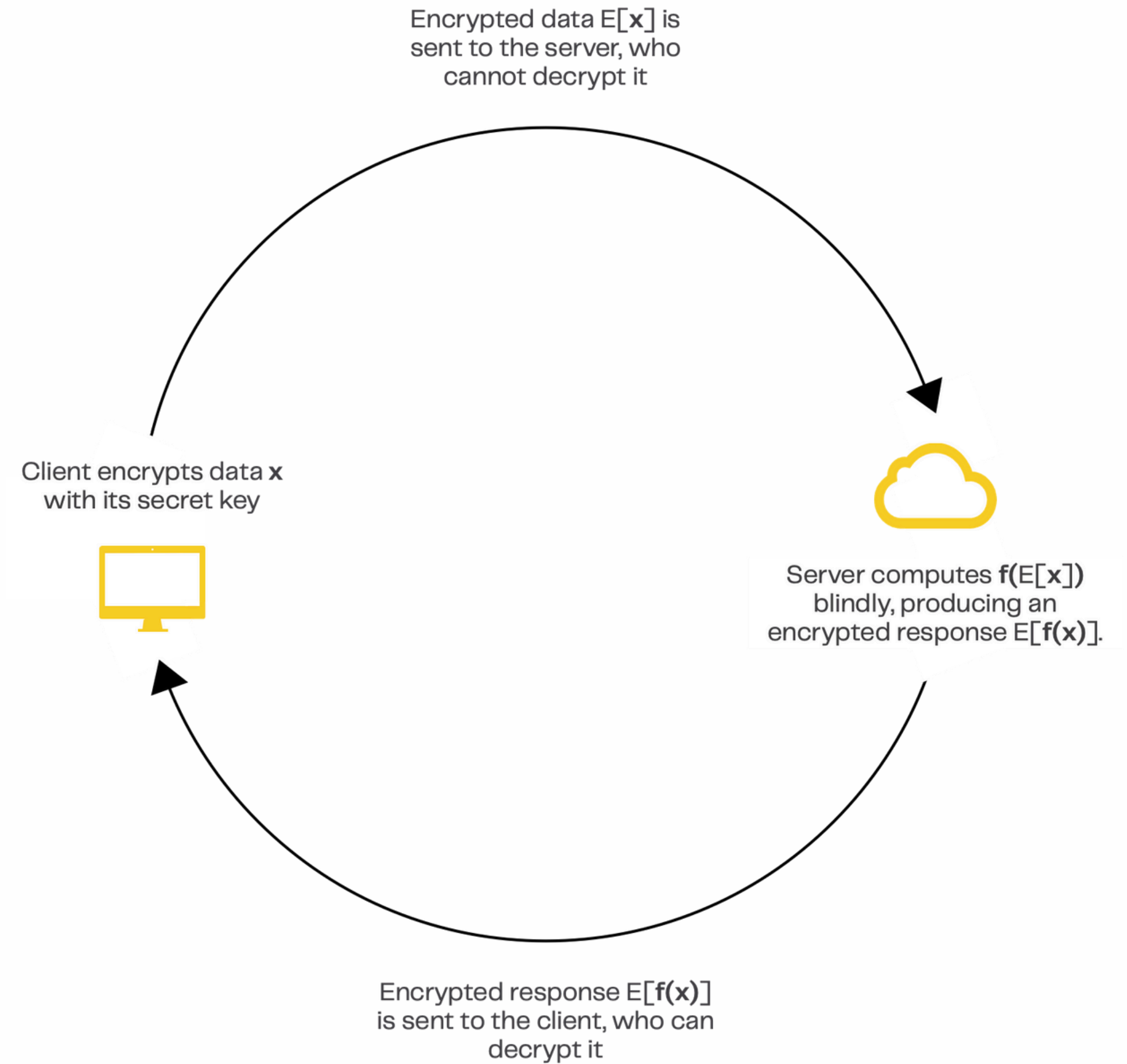
Risques

-  Vol
-  Surveillance
-  MEV

HTTPS: Chiffrement lors du transport

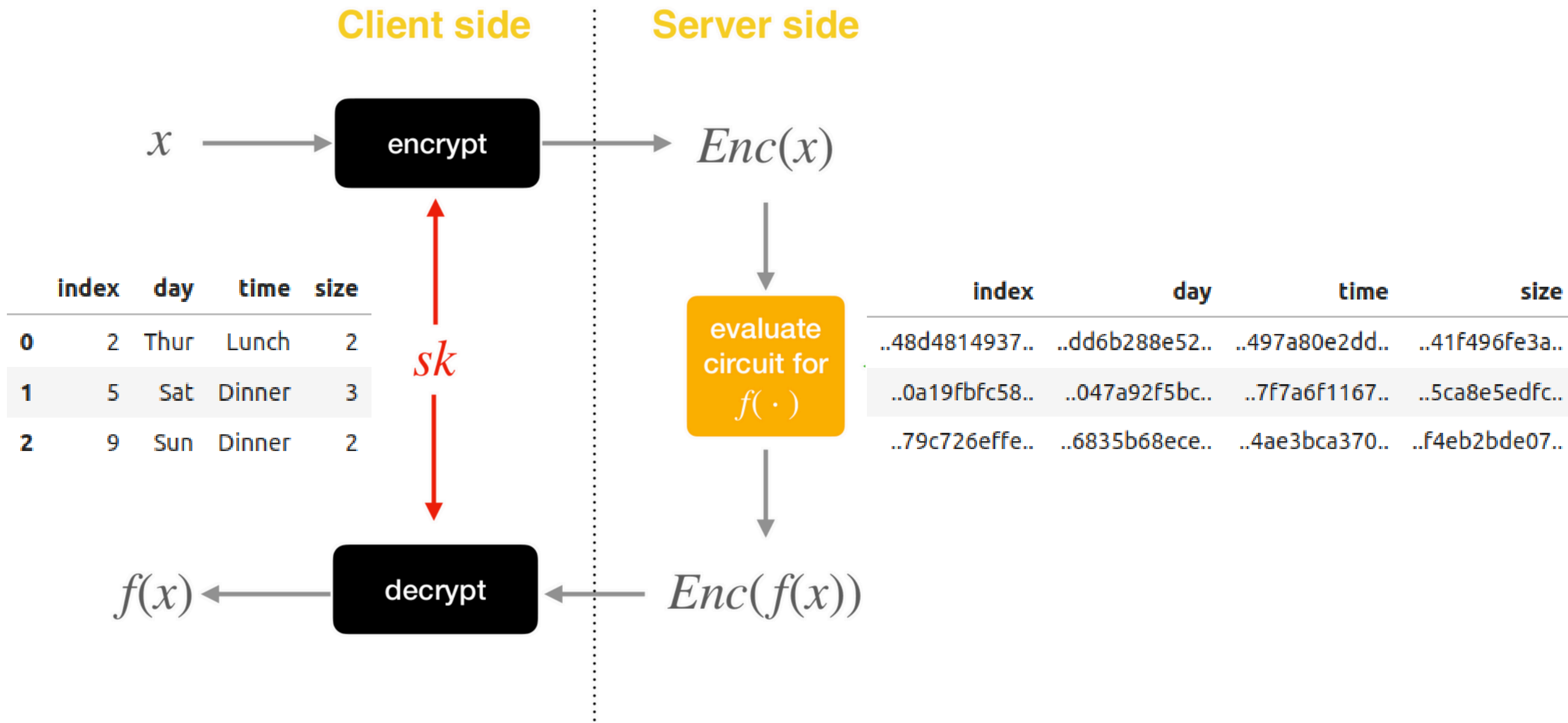


Avec le chiffrement homomorphe les données sont traitées à l'aveugle



FHE pour l'IA

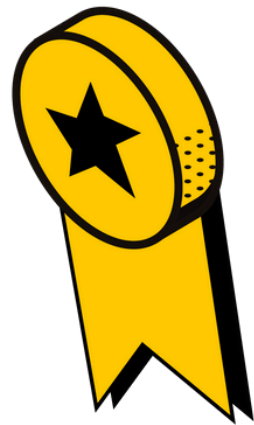
HTTPZ: Calcul sur des données chiffrées



Valeur ajoutée du FHE pour l'IA



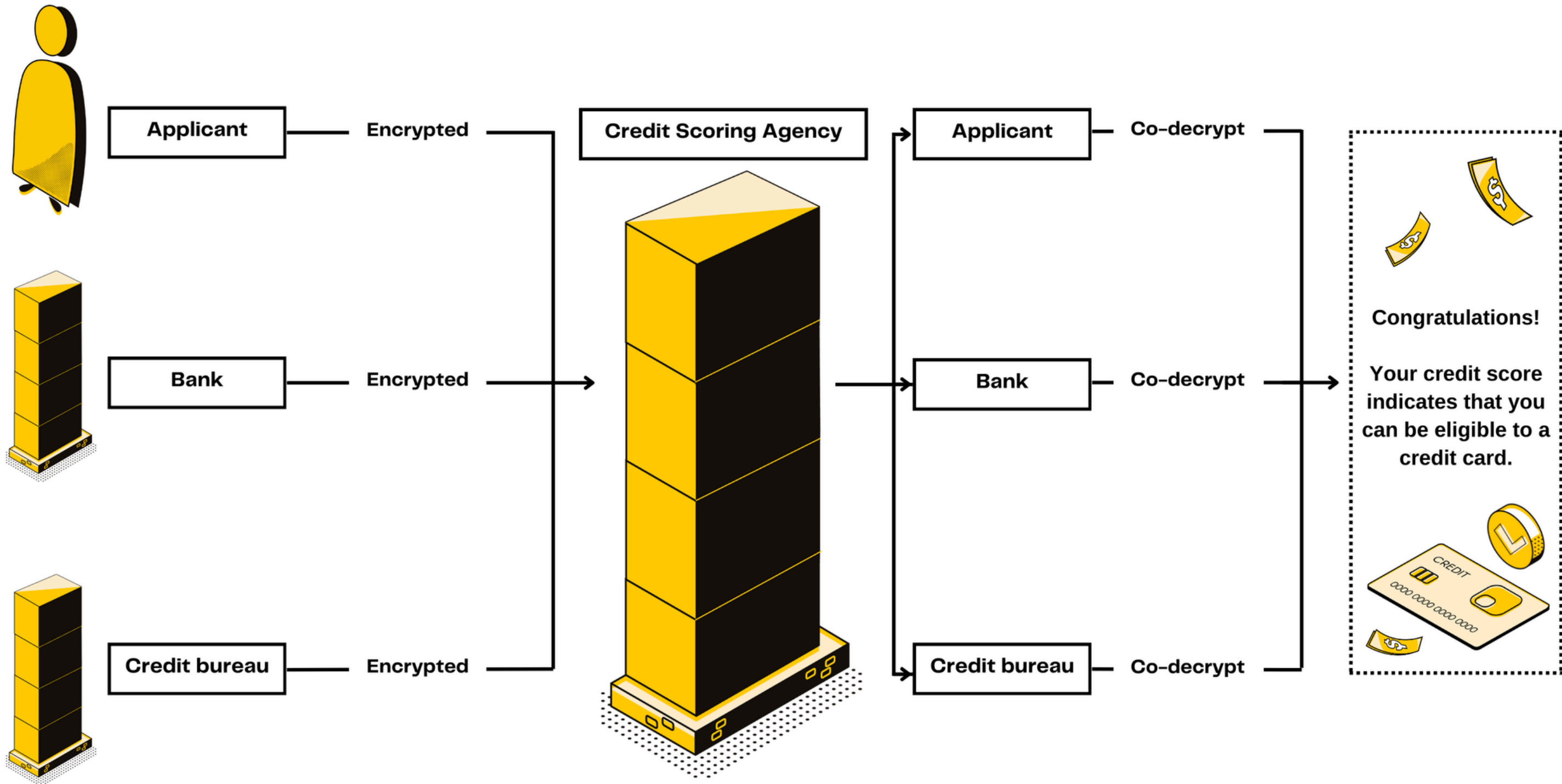
Sécuriser les données sensibles sans brider les fonctionnalités



Améliorer la qualité des prédictions par le biais de la collaboration confidentielle

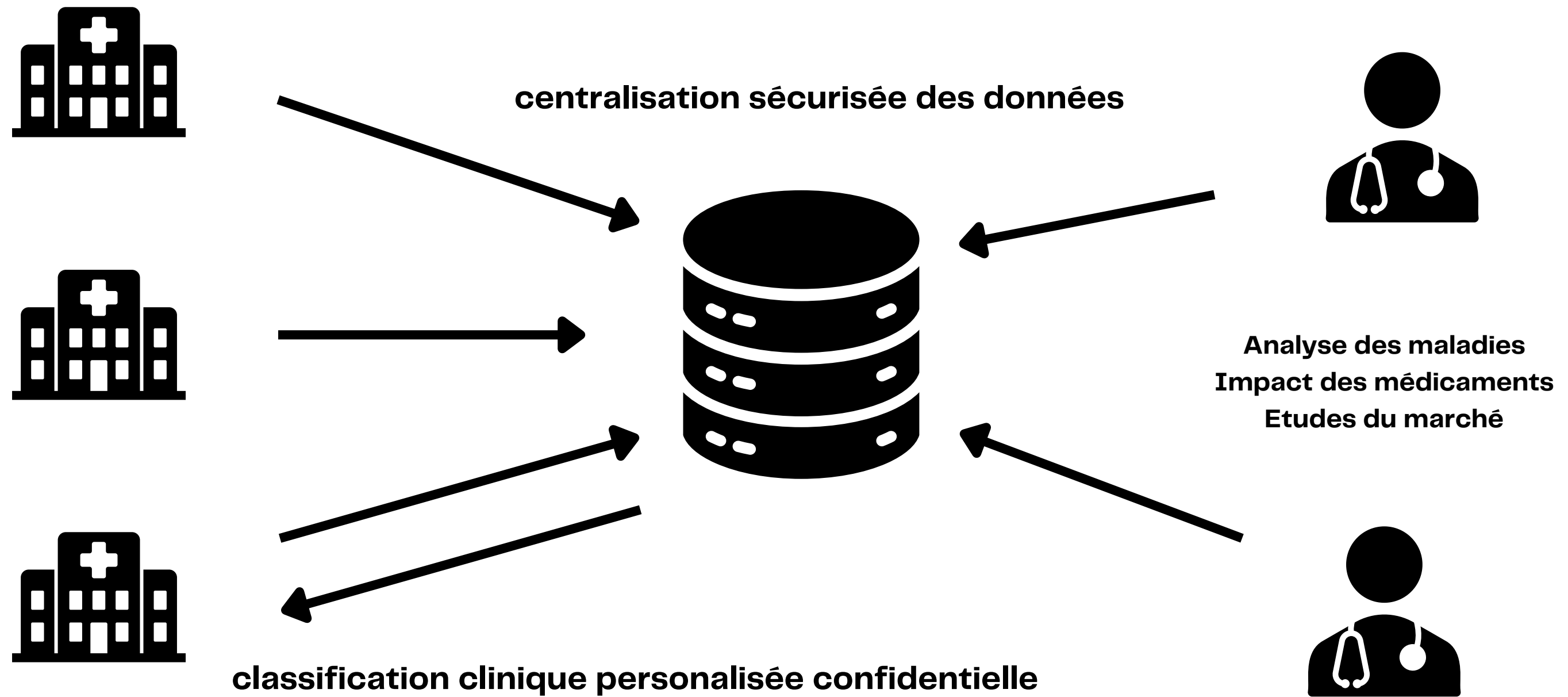
Applications finance

Prédiction améliorée grâce à l'analyse jointe d'informations confidentielles



Applications santé

Accès unifié, transparent et sécurisé, aux données de santé



FHE pour la Blockchain

Confidentialité des montants

Transactions Internal Txns **Erc20 Token Txns** Erc721 Token Txns Erc1155 Token Txns Analytics Comments

Latest 25 ERC-20 Token Transfer Events

View All

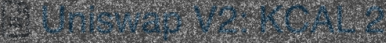
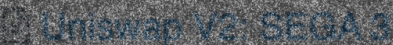
Txn Hash	Age	From	To	Value	Token
 0x61bac8ed64cf49ff537...	1 hr 8 mins ago	 Uniswap V2: KCAL 2	  vitalik.eth	2,500	 Step.app (KCAL)
 0xd9f47a344e278579cb...	1 hr 15 mins ago	Justin Sun	  vitalik.eth	25,143,213.150843308745475521	 Step.app (KCAL)
 0xdea02c32d141997aaa...	12 hrs 57 mins ago	 plamer.eth	  vitalik.eth	1	 AssangeDAO (JUSTIC...)
 0x74205c19a313ba8865...	1 day 11 hrs ago	 Uniswap V2: SEGA 3	  vitalik.eth	227,158,544.808096280091774569	 SEGA (SEGA)
 0xad5c19e1af6de6508e...	2 days 20 hrs ago	0xad29c28a868c945caf9...	  vitalik.eth	21,420	 ERC-20 (BASTAR...)
 0x1014024546d2e94f39...	3 days 4 mins ago	 Uniswap V2: ALIS 2	  vitalik.eth		 Acropolis DA... (ALIS)
 0xbffdb2fcd52e96f136c7...	3 days 24 mins ago	 vitalik.eth	  OlympusDAO: DAO Funds		 Acropolis DA... (ALIS)
 0x6ac57444413cd7bbef...	3 days 31 mins ago	 Uniswap V2: ALIS 2	  vitalik.eth		 Acropolis DA... (ALIS)
 0xb15136c85e15dd81b3...	3 days 1 hr ago	 OlympusDAO: DAO Funds	  vitalik.eth		 Acropolis DA... (ALIS)
 0xa9749c78f8ed9da996...	3 days 14 hrs ago	 Uniswap V2: Bvlgari	  vitalik.eth		 ERC-20 (Bvlgar...)

ZAMA

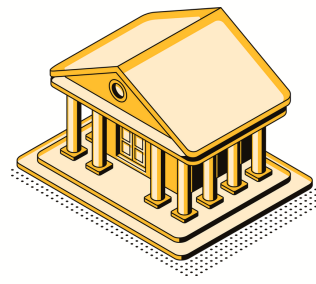
fhEVM

FHE smart contract protocol

Anonymat et confidentialité

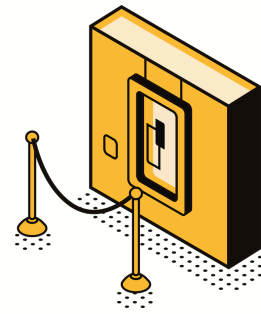
Transactions	Internal Txns	Erc20 Token Txns	Erc721 Token Txns	Erc1155 Token Txns	Analytics	Comments
Latest 25 ERC-20 Token Transfer Events						
View All						
Txn Hash	Age	From	To	Value	Token	
 0x61bac8ed64cf49ff537...	1 hr 8 mins ago			2,600		
 0xd9f47a344e278579cb...	1 hr 15 mins ago			25,143,213,150843308745475521		
 0xdea02c32d141997aaa...	12 hrs 57 mins ago			1		
 0x74205c19a313ba8865...	1 day 11 hrs ago			227,158,544,808096280091774569		
 0xad5c19e1af6de6508e...	2 days 20 hrs ago			21,420		
 0x1014024546d2e94f39...	3 days 4 mins ago	ZAMA				
 0xbffdb2fcd52e96f136c7...	3 days 24 mins ago	ZAMA				
 0x6ac57444413cd7bbef...	3 days 31 mins ago	ZAMA				
 0xb15136c85e15dd81b3...	3 days 1 hr ago	ZAMA				
 0xa9749c78f8ed9da996...	3 days 14 hrs ago	ZAMA				

Le FHE débloque des nouveaux cas d'usage



Tokenisation

Gestion et transactions des actifs tokenisés sans dévoiler les montants



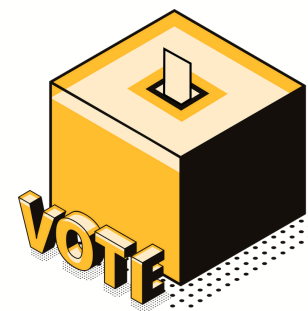
Enchères à l'aveugle

Faire une offre sans dévoiler son montant et cacher le gagnant de l'enchère



Electronic Cash

Transactions anonymes



Vote confidentiel

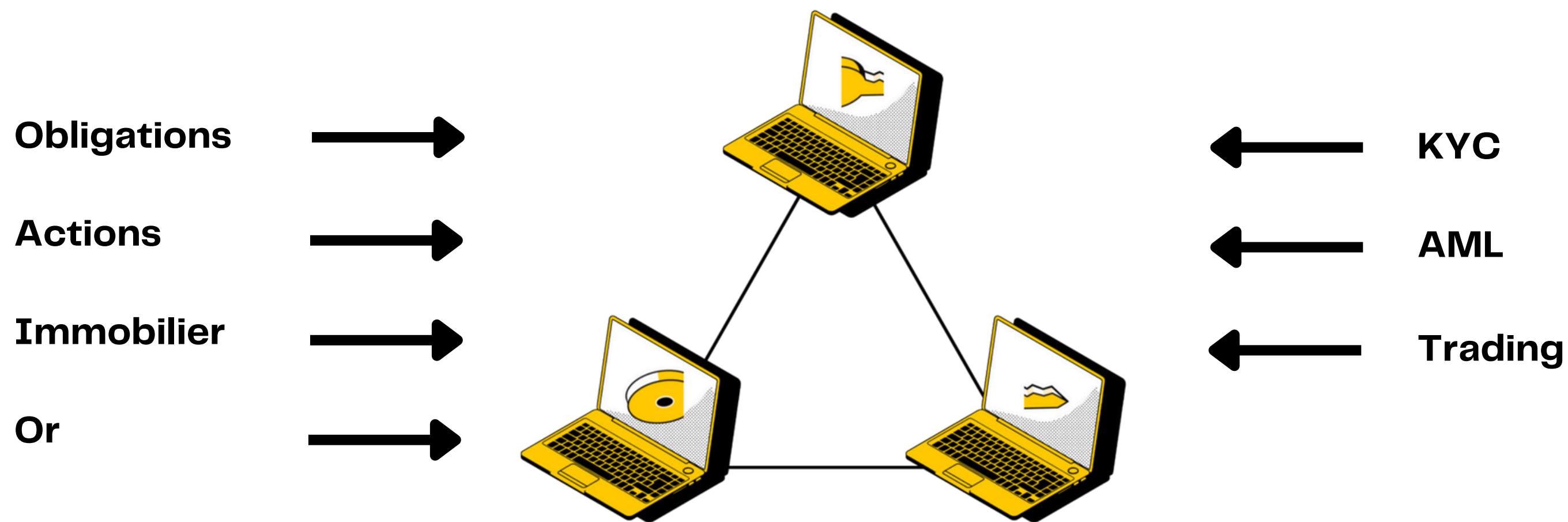
Empêcher la corruption des électeurs



Identité chiffrée

Vérifier l'identité des personnes et pour contrôler l'accès à des applications décentralisées

Tokenisation et FHE



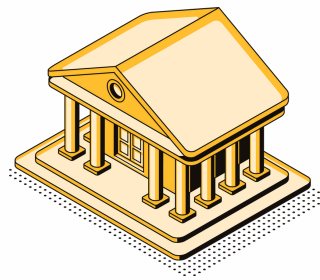
plateforme de tokenisation :

Publique: accès facilité, confidentialité des transactions;

Universelle: accès à tout type d'actif, AML et compliance facilités (auditable);

Les smart contracts implémentent les règles métier des transactions;

Monnaie numérique de banque centrale (CBDC)



Monnaie-banque-centrale:

Utilisée pour les règlements entre les banques.
Tokenisation étudiée par la Banque de France.

Interopérabilité avec stablecoins et autres
CBDC.

FHE: cacher les montants.



E-euro numérique:

Règlement gratuit.
Disponibilité 24/7.

Préserver l'anonymat des paiements en
espèces.

FHE: cacher les montants et adresses.

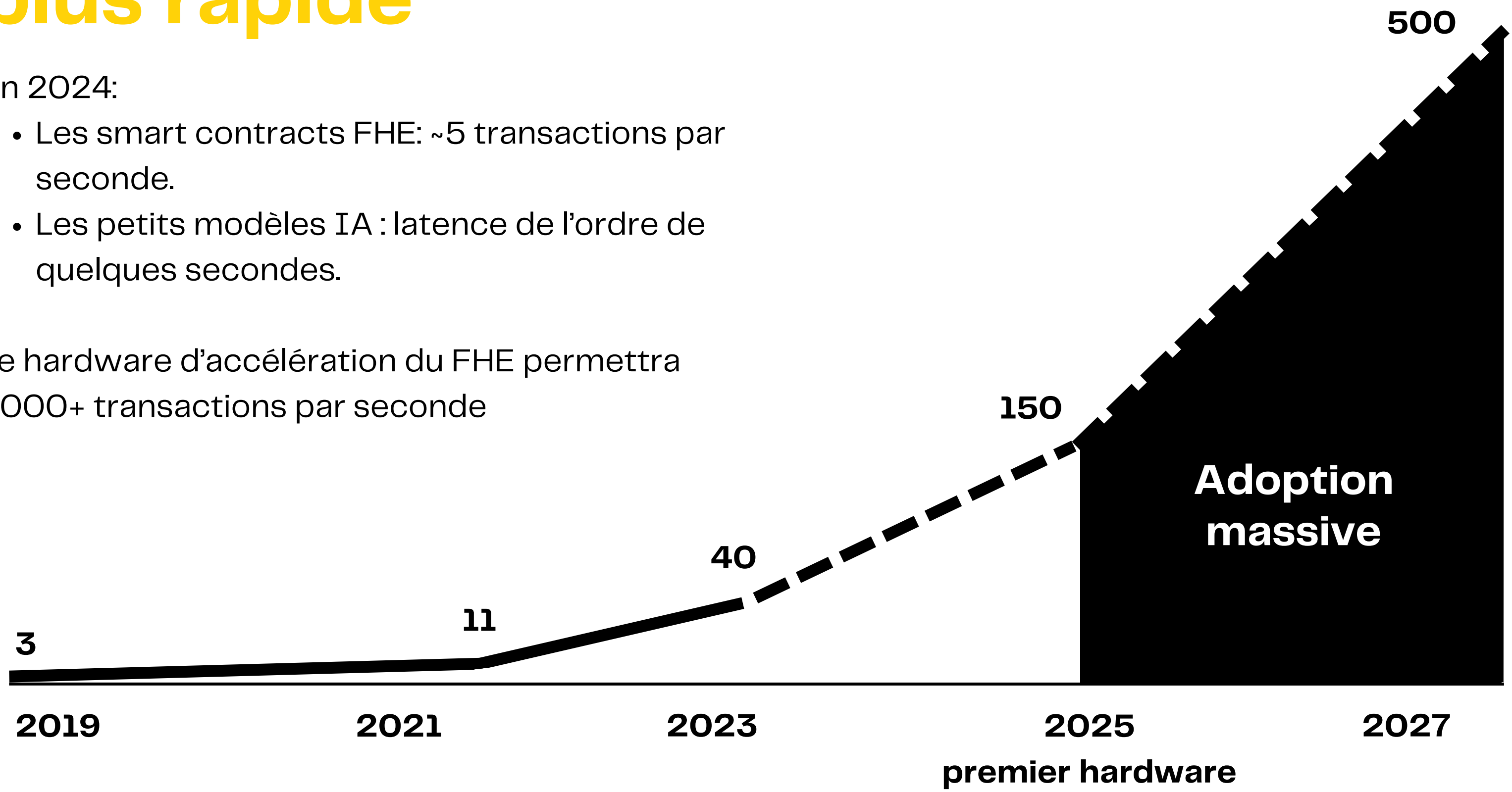
Le FHE est de plus en plus rapide

Zama FHE performance
(Million FHE gates / \$)

En 2024:

- Les smart contracts FHE: ~5 transactions par seconde.
- Les petits modèles IA : latence de l'ordre de quelques secondes.

Le hardware d'accélération du FHE permettra
1,000+ transactions par seconde



Contact et liens

andrei.stoian@zama.ai

zama.ai

[Github](#)

[Community links](#)

ZAMA