Blockchain Partner by KPMG

Cryptalk

L'institutionnalisation d'Ethereum

21 novembre 2022

Flavio Restelli
Nicolas Rongeard

KPMG FRANCE
Paris

+

Pascal Marguier

Fireblocks

Sommaire

01

“The Merge” : un changement de paradigme

Modification du consensus : pourquoi est-ce important ?

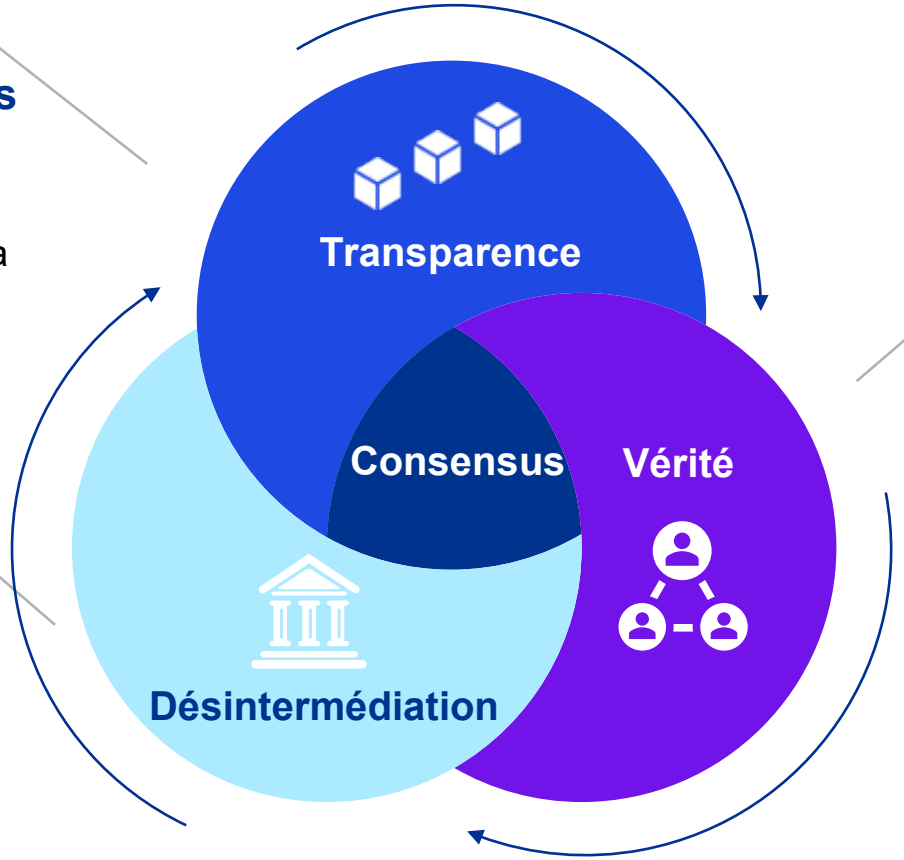
Pourquoi a-t-on besoin d'un consensus ?

Garantir l'intégrité des transactions

- Le registre est transparent et distribué
- L'intégrité des données fait référence à "la fiabilité et la crédibilité des données

Sans passer par un tiers de confiance

- Les nouvelles données doivent être acceptées à l'unanimité
- Sans intermédiaire central qui valide les transactions



S'accorder sur une seule version de la "vérité"

- Chaque pair doit utiliser le même registre
- Il faut une méthode pour désigner qui a le droit d'ajouter des informations (transactions)

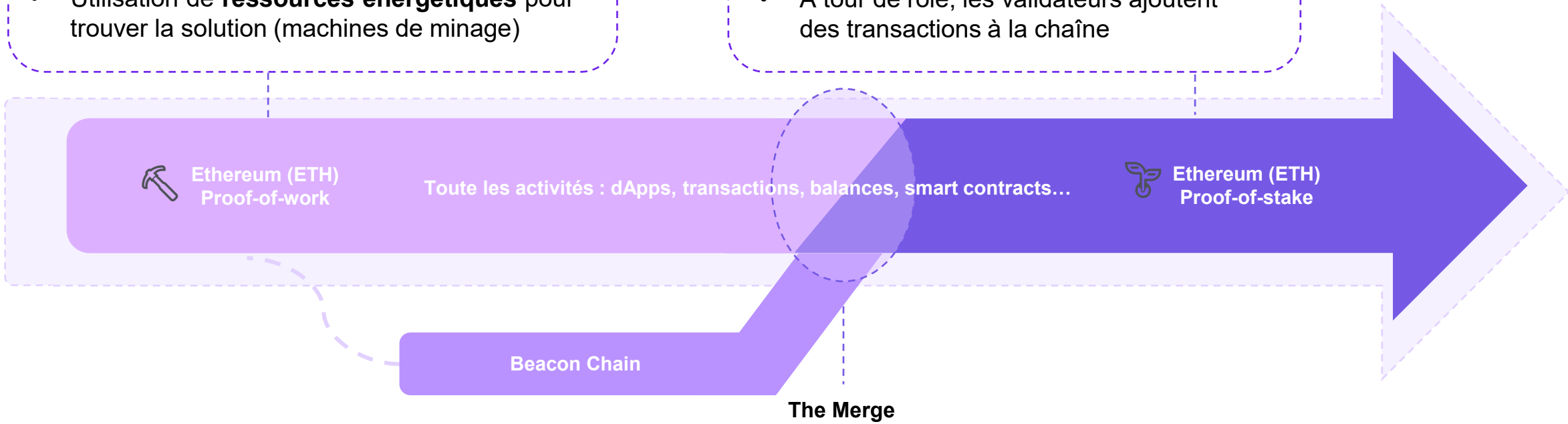
De la preuve de travail à la preuve d'enjeu

Proof of Work

- Pour gagner le droit à ajouter des transactions au registre (en échange d'une rémunération) : compétition mathématique
- Utilisation de **ressources énergétiques** pour trouver la solution (machines de minage)

Proof of Stake

- Sécurisation du réseau en **mettant sous séquestre des jetons** ETH par chaque participant (validateur)
- À tour de rôle, les validateurs ajoutent des transactions à la chaîne



Pourquoi « The Merge » ?

Fusion entre le vieux **mécanisme d'exécution** des transactions **+** la **nouvelle méthode de consensus** Proof-of-Stake

Ethereum : une chaîne ESG-friendly ?

Ethereum et le PoS : Une nouvelle narrative ESG

Une réduction drastique de la consommation énergétique du réseau d'environ 99%

- **Le passage d'Ethereum à la preuve d'enjeu** ne requiert plus l'utilisation de ressources énergétiques pour sécuriser le réseau.
- Toute tentative de **comportement malhonnête** de la part des validateurs est **automatiquement sanctionnée** (aucune récompense et jetons bloqués détruits).

Point d'attention sur le PoW

- Si les atouts du PoS sont à saluer, la **démystification des impacts environnementaux du PoW demeure primordiale**. En effet, les mineurs sont des consommateurs d'énergie très particuliers et peuvent s'approvisionner d'énergie gaspillée (ex. torchères) ainsi que d'extracapacité des centrales « vertes ».
- Cependant, à date il faut prendre en compte des **risques réputationnels** en cas d'utilisation d'une blockchain PoW. C'est pourquoi The Merge représentent une véritable opportunité pour les entreprises.

02

La conservation des cryptoactifs : condition n°1 pour l'adoption

Deux modes de conservation des cryptos se dégagent (B2B)

Custodial

Les cryptoactifs sont gérés par un intermédiaire centralisé, qui se charge de sécuriser les fonds pour le compte de l'entreprise (cf. système bancaire traditionnel)

Ces dépositaires :

- **Sont assurés** par des acteurs traditionnels reconnus
- Proposent des solutions de **trading,** avec des passerelles entre les monnaies fiats et les cryptoactifs
- Sont soumis à des exigences réglementaires (Ex: PSAN)

Conservation déléguée des cryptoactifs

BitGo · kraken · coinbase Prime

Non-custodial

Chaque entreprise est responsable de la sécurisation de ses cryptoactifs, qu'elle contrôle directement et utilise sans intermédiaires.

Les solutions non-custodial permettent de:

- **Garder le contrôle** (souveraineté) sur ses fonds
- Faciliter l'**accès** aux produits et services **Web3**
- **Documenter les processus**: accès, validation, recovery, reporting, etc.

Plusieurs solutions **technologiques** existent

Corporates Wallets

Fireblocks · Ledger Vault · METACO · TAURUS

La custody ouvre la voie à une multiplicité de services

Achat de cryptos / conversion crypto-fiat	**Cybersécurité / check smart contract**	**Conformité LCB / FT**	**Reporting / comptabilité**	**Pilotage de comptes via un dashboard (agrégation)**
Assurance	**Trading cryptos**	**Création, achat et vente NFTs**	**Tokenisation actifs**	**Staking**

Les solutions de custody peuvent offrir ces services **en propre ou via des partenaires**. Des exemples :

Chainalysis

Suivi des transactions on-chain et contrôles LCB / FT

LIDO

Staking décentralisé de cryptos sur blockchains proof-of-stake pour obtenir un rendement passif

Centralized Exchange (CEX) : les nouvelles banques ?

Description

1. Plateformes permettant l'**achat de cryptoactifs** avec des monnaies fiat, ainsi que le trading

2. Prestataires de services de **conservation des cryptoactifs** à destination des particuliers et des entreprises, selon le **modèle custodial**

3. Intermédiaire crypto par excellence, un CEX peut offrir un grand nombre d'**offres cryptos supplémentaires**

Exemples

BINANCE — **$14 milliards** de volume d'échange (24h)

coinbase — **$2 milliards** de volume d'échange (24h)

kraken — **$755 millions** de volume d'échange (24h)

Source : CoinMarketCap, 21 octobre 2022

Fireblocks en quelques chiffres

€8 milliards de valorisation
(Série E)

BNY MELLON · stripes · SEQUOIA · DRW · Ribbit Capital · Paradigm
SVB Silicon Valley Bank · CYBERSTART · coatue · 8VC EIGHT ROADS · swisscom Ventures

€3T+
Transférés sur le réseau

575+
Employés

HQ: New York
R&D: Tel Aviv
Sales: Global

1,700+
Clients

BNY MELLON · Revolut · eToro
BNP PARIBAS · worldpay · KOMAINU
ANZ · checkout.com · SDX SIX Digital Exchange

Notre activité

Plateforme SaaS institutionnelle permettant **l'autodétention** (self-custody), **le transfert** et **l'émission** d'actifs numériques

Wallet Self custody

(Hot, Warm & Cold)

1,500
Tokens

45+
Blockchains

€45B+
conservés

Transfer

40+
Exchanges Centralisés

Defi
Network
Fiat

Tokenization

Actifs financiers, stablecoins, NFTs..

SEGMENTS CLIENTS

- **Corporates**
- **Tradfi**
- **Echanges (CEX)**
- **Liquidity provider (LP)**
- **PSP**
- **Web3**

SÉCURITÉ ET CONFORMITÉ DE NIVEAU BANCAIRE

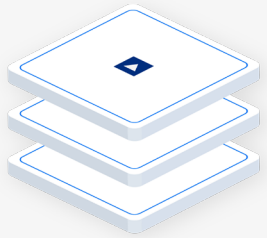
AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

ISO/IEC 27001:2013
ISO/IEC 27017:2015
ISO/IEC 27018:2019

Proposition de valeur Fireblocks

3 Piliers

Sécurité & Gouvernance



Paramétrage des validation

MPC Wallet

Intel SGX & Azure

Connectivité

Echanges (CEX), Network, **Defi**

Staking

Tokenization, Paiments

Conformité

Intégrations **LCB/FT**

Outils Audit / Reporting

Leviers

Activation marché **rapide**

Offre de service **flexible et agile**

Infrastructure **scalable et conforme**

03

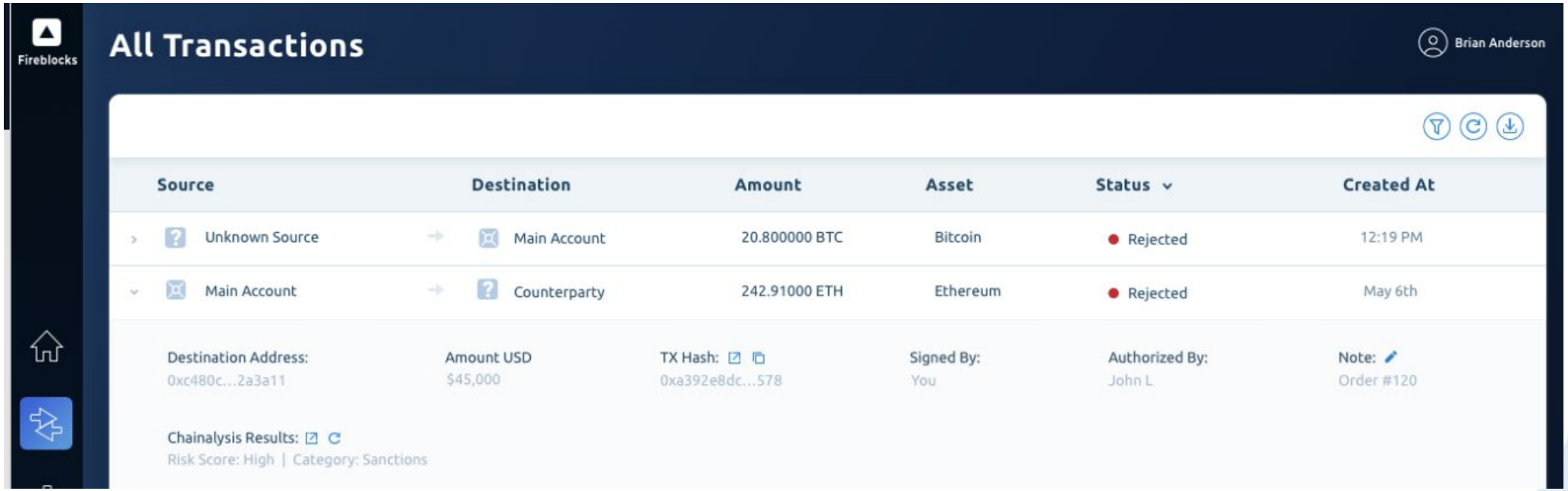
La conformité des opérations: condition n° 2 pour l'adoption

KYT – « Know your Transaction »

- **Screening des transactions**

Chainalysis

- Contrôle des **risques**
- **Reporting** pour l'Audit / régulateurs



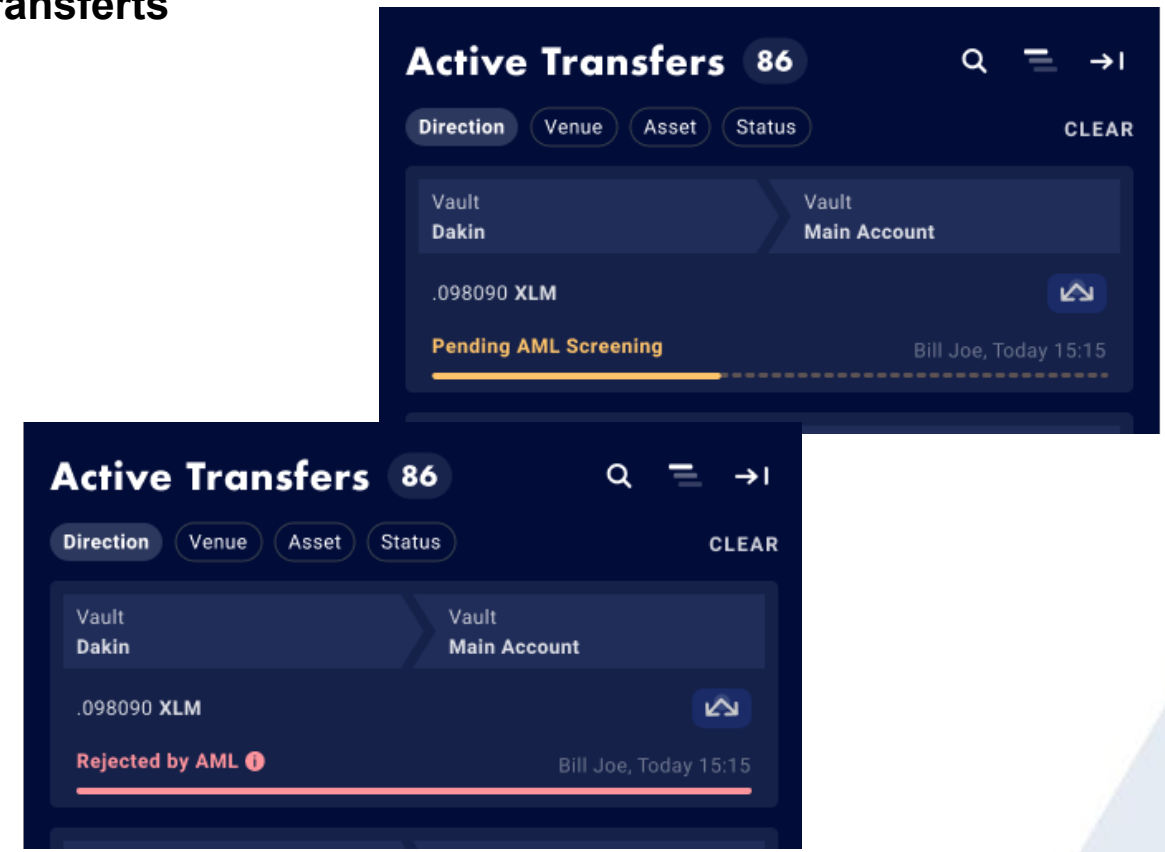
Passage à l’échelle - KYT

Contrôles de conformité dynamiques pour les transferts

- Automatiser les processus de LCB/FT
- Refus / Gèle des transactions

Eviter les procédés manuels

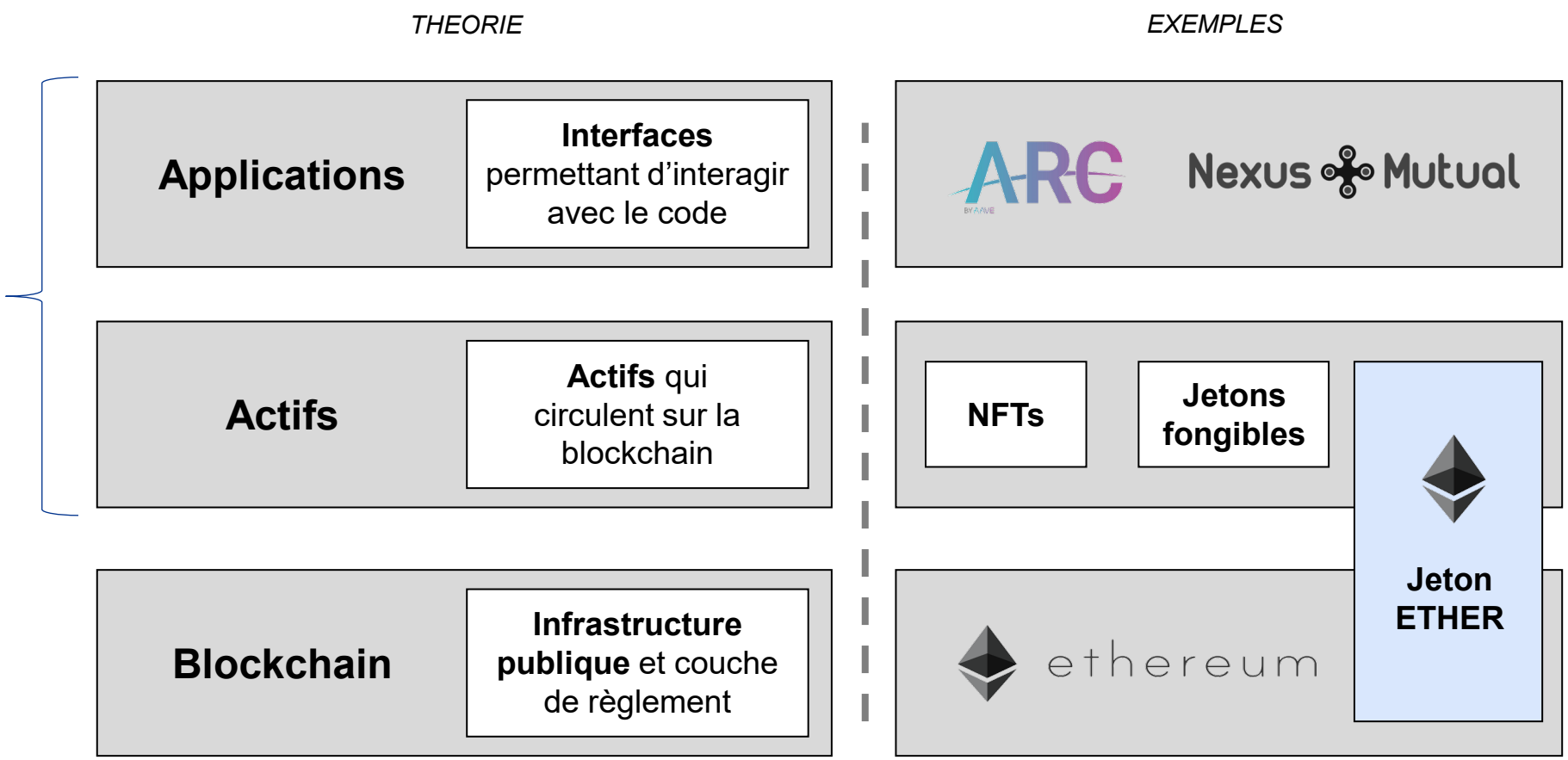
- Alertes sur les transferts
- Reporting



DeFi permissionnée : une nouvelle frontière pour les institutionnels

Les **contrôles KYC, LCB / FT etc.** peuvent être appliqués pour créer des cas d'utilisation conformes

L'infrastructure doit rester **agnostique et incensurable**



Aave Arc : des pools avec KYC directement dans la DeFi

Un marché de liquidité **sans intermédiaires**

L'offre classique du **protocole Aave:**

- Dépôts rémunérés et emprunts de cryptomonnaies
- Taux variables en fonction de l'offre et de la demande

AAVE

+

Une couche de contrôle

Whitelisting ou accès permissionné:

- Conformité FATF (KYC/KYB)
- Screening LCB via intégration du software Chainalysis
- Sécurisation non-custodial des actifs

Fireblocks

=

Une DeFi conforme

Des **pools privées** pour des institutionnels :

- **30 clients institutionnels** dès le lancement (janvier 2022)
- **$7.8 millions** de Valeur Totale Bloquée (TVL) à date

ARC

Objectifs

- **Faire bénéficier les institutionnels des avantages de la DeFi** et d'une infrastructure décentralisée et publique
- Répondre à une demande croissante : établir des **connexions entre finance traditionnelle et DeFi**
- Réagir aux besoins des acteurs institutionnels : continuer à respecter les **contraintes en termes de conformité**

Sources Aave Arc : Defillama