



À la croisée de l'informatique confidentielle et des technologies Trustless !

Qui sommes-nous ?



Partenaires & adoptants



Introduction: BigData, Confidentialité et Cybersécurité

2016

90% données générées les 2 années précédentes, 1% analysé.
McKinsey, 2016

2023

75% de la population mondiale sera couverte par des réglementations sur les données privées.
Gartner, 2023

2022

84% des entreprises accordent le plus d'importance à la gestion de la confidentialité lors de l'achat de logiciel.
Gartner, 2022

2025

60% des organisations vont traiter la cybersécurité comme risque N°1.
Gartner, 2023



Confiance



Honnêteté



Confidentialité



Sécurité

La confiance c'est quoi ?

"C'est un sentiment d'assurance..."

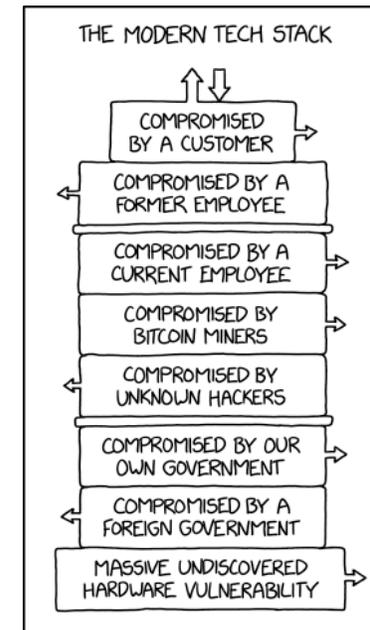


Confiance dans les intermédiaires

- Basé sur la réputation
- Coûteux
- Frein à l'innovation
- Souvent toujours très risqué
- Sujet à l'erreur



Confiance dans les systèmes d'informations



From <https://xkcd.com/2166/>



Objectif: Limiter la confiance au maximum

Principes de conception de Klave



Honnêteté et vérifiabilité

- Attestation
- Preuve Cryptographique



Limiter la confiance

- Approche Zéro confiance
- Limiter la confiance dans les tierces parties



Confidentialité et Sécurité

- Intégrité calculatoire
- Intégrité des données
- Cryptographie avancée



Développeurs au centre

- Workflow intégration
- Langages de haut niveau
- Cycle de vie de l'Application

L'informatique confidentielle

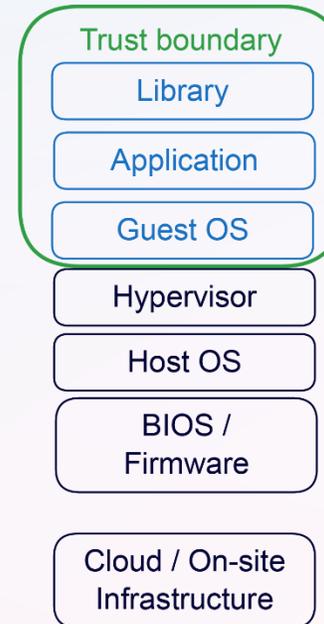
L'informatique confidentielle apporte des couches supplémentaires de sécurité pour protéger la logique business et préserver la confidentialité et l'intégrité des données pendant leur utilisation.

Traditional computing

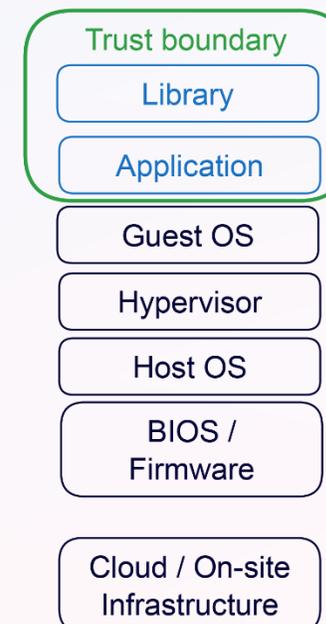


Confidential Computing

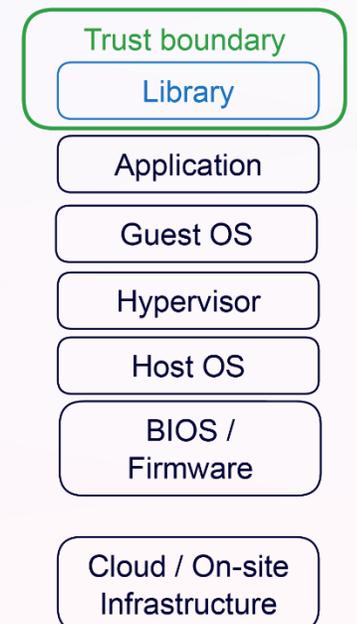
Virtual Machine isolation



Application isolation



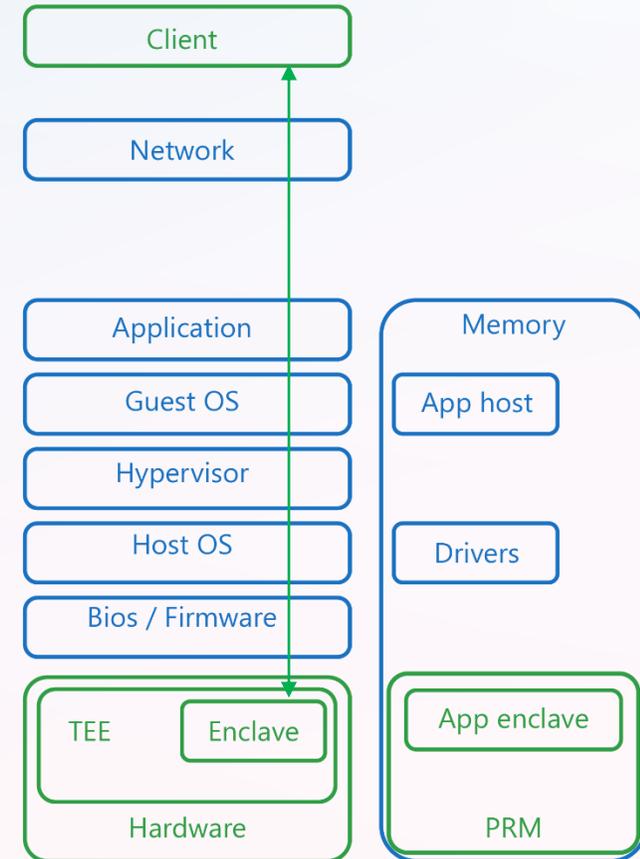
Library isolation



Environnement d'exécution de confiance & Enclave

L'informatique confidentielle est basée sur l'utilisation des environnements d'exécution de confiance qui apportent les garanties suivantes:

- Intégrité des données
- Confidentialité des données
- Intégrité du code
- Confidentialité du code
- Attestable
- Programmable
- Optimisation hardware pour la cryptographie



Management des enclaves: EncLOS

Enclave OS (EncLOS), est le système d'exploitation sécurisé que nous avons mis au point pour apporter toutes les fonctionnalités nécessaires aux enclaves.



Communications



Systèmes de fichiers



Traçage



Modèle de sécurité:

- Manipulation de hash
- Merkle proof
- Attestation locale & distante
- Signature digitale
- SMPC
- Secret sharing



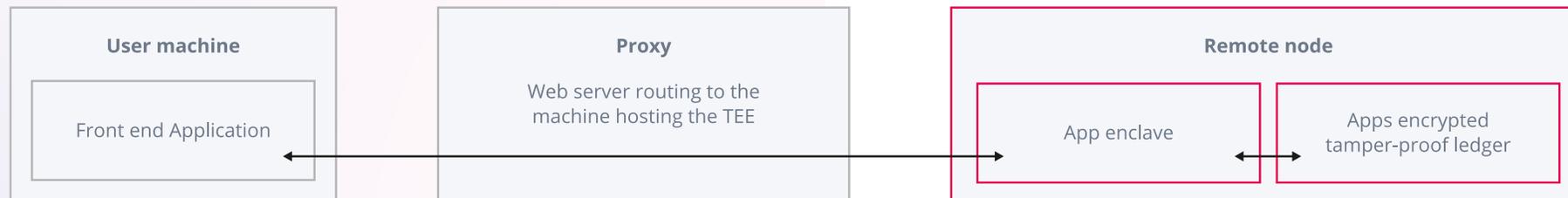
On premise encryption



Double encryption resists TLS termination and prevents deep packet inspection



Authenticated connection to the TEE, not just the physical machine



Architecture distribuée et DLT



Pour assurer une haute disponibilité et une continuité des opérations



DLT, base de données distribuées synchronise en quasi-temps réel.



Algorithme de consensus RAFT (state machine)



Logchain pour garder l'intégrité



Byzantine Fault Tolerance RAFT



Architecture sensible aux objectifs verts



Klave c'est quoi ?

Plateforme Trustless

- Intégrité des données & confidentialité
- Résistance à la fraude & intégrité de calcul
- Vérifiable & Honnête

Klave App

- Turing complete
- État persistant
- Confidentialité
- Intégrité
- Isolation
- Vérifiable

Développeur au centre

- SDK simple
- Langages haut niveau
- Intégration avec l'environnement

The screenshot shows the Klave web interface. At the top, there's a navigation bar with the Klave logo, a user greeting 'Welcome, florian@secretarium.org', and buttons for 'Deploy now' and 'Log out'. Below this, there's a section for 'APPLICATIONS (4)' with a search bar and a list of four applications: 'My Power App', 'Try Trustless', 'Crypto Cat', and 'Hello World', each with a 'Deployed' status. The 'My Power App' is selected, showing a detailed view with tabs for 'Activities', 'Deployments', 'Domains', and 'Settings'. The 'Deployments' tab is active, showing a table of recent deployments. The table has columns for 'Address', 'Version', 'Dates', and 'Action'. Two deployments are listed, both with a 'Release' button and a trash icon.

The screenshot shows a code editor with a file explorer on the left. The file explorer shows a project structure for 'MY-POWER-APP' with files like 'klave', '0-hello-world.d.ts', '0-hello-world.wasm', '0-hello-world.wat', 'apps/hello_world', 'TS_index.ts', 'tsconfig.json', 'TS_types.ts', '.gitignore', 'klave.json', 'package.json', and 'yarn.lock'. The main editor shows the content of 'TS_index.ts', which is a TypeScript file defining a 'fetchValue' function. The code imports 'Notifier', 'Ledger', and 'JSON' from '@klave/sdk'. It defines a 'myTableName' constant and a 'fetchValue' function that interacts with a 'Ledger' to retrieve data from a table. The function returns a 'FetchOutput' object with 'success' and 'value' properties.

 Ramener la responsabilité dans la logique business



Register to the beta now at klave.network/beta



Thank you!