Novel uses cases enabled by Fully Homomorphic Encryption in Blockchain

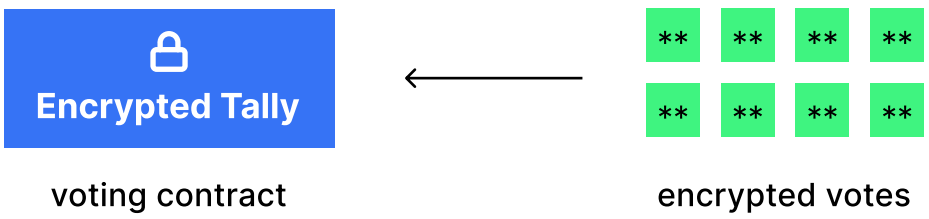
team@inco.network

Introduction:

- The transparent nature of public blockchains limits the feasibility of decentralized applications (DApps) that require confidentiality in order to make sense.
- Existing efforts have trade-offs: 1) Secure enclaves are vulnerable to side-channel attacks and depend on a centralized supply chain 2) Zero-knowledge (ZK) cryptography necessitates off-chain storage of sensitive data and computations in plaintext, adding complexity and the risk of data leakage from untrusted provers.
- The TFHE scheme, integrated into the Ethereum Virtual Machine (EVM) as a pre-compile, also known as fhEVM, broadens potential use cases across gaming, enterprise, and Decentralized Finance (DeFi).

Solving the coordination problem:

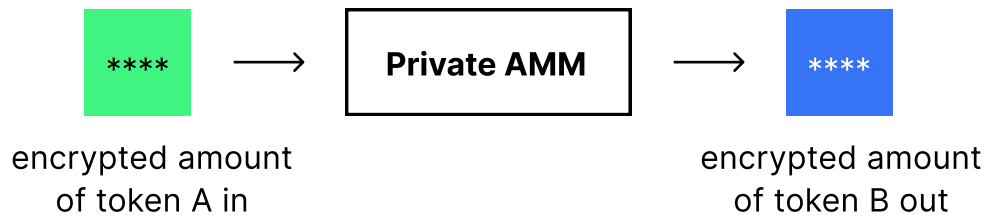
fhEVM introduces a “shared private state” that facilitates on-chain coordination and composability, enabling multi-party use cases.



Ex: Private Voting

MEV protection:

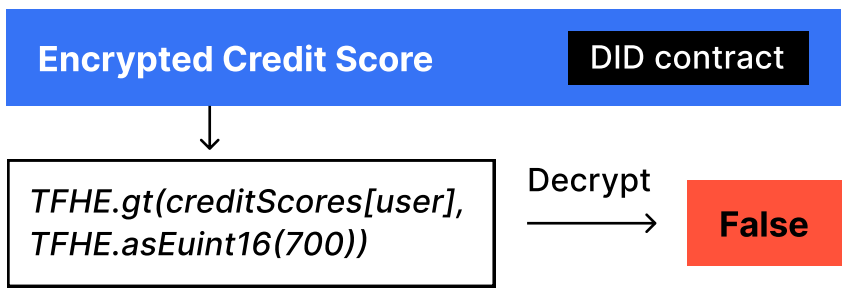
Using encrypted data as input can prevent MEV problems such as front-running given that the specific user intent will be masked.



Ex: Private AMM

Confidential state transition + comparisons:

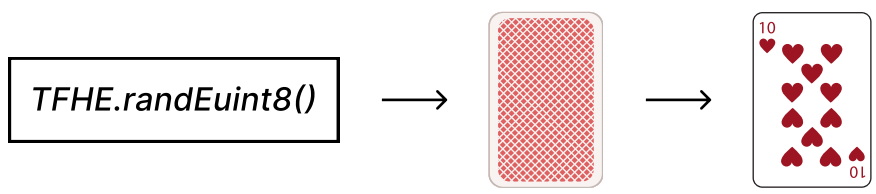
The ability to do computation and comparisons on top of encrypted data opens up for a broader range of use cases.



Ex: Is user credit score above 700?

Randomness & Confidentiality:

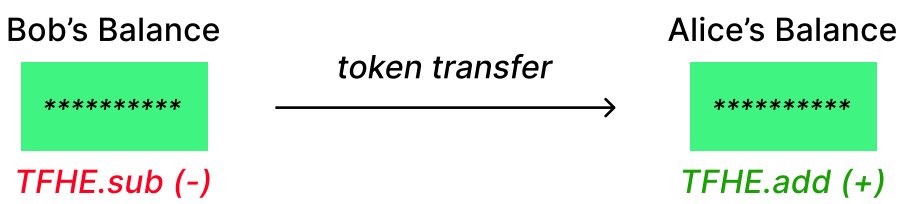
Combining randomness and confidentiality can unlock use cases that are currently not supported by existing plaintext VRF solutions.



Ex: Poker card game

Traceable confidentiality:

FHE offers traceable confidentiality because everything happens on-chain, which is more conducive to audit and compliance.



Ex: Confidential ERC-20

Conclusion:

Applying FHE to blockchain empowers developers to transition web2 applications to web3 in a trustless and painless manner compared to existing solutions, and push for the development of next frontier of decentralized applications (dApps) that weren’t possible before on existing public blockchains.

INCO

inco.org
docs.inco.org