Louis Tremblay Thibault

TUM Blockchain Salon
16 May 2024

Privacy-Preserving Smart Contracts using FHE

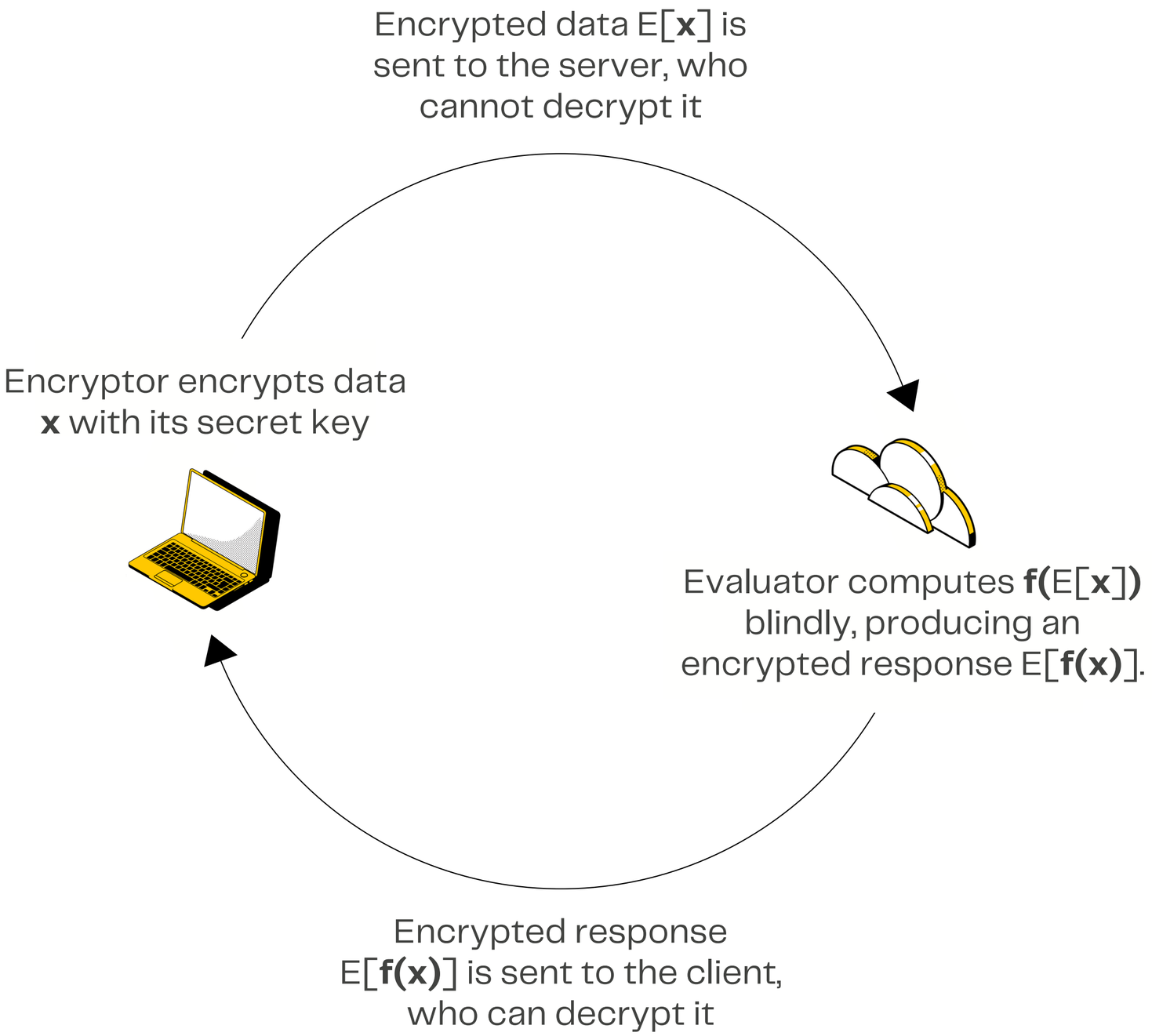
ZAMA

Zama is a **cryptography company** providing **open source homomorphic encryption solutions** for **blockchain and AI.**

Agenda

- Quick introduction to FHE
- What FHE means for Blockchain
- How the fhEVM works
- Challenges and research avenues

Fully Homomorphic Encryption (FHE) enables processing data blindly



FHE enables encrypted data processing

$$E[x] + E[y] = E[x + y]$$

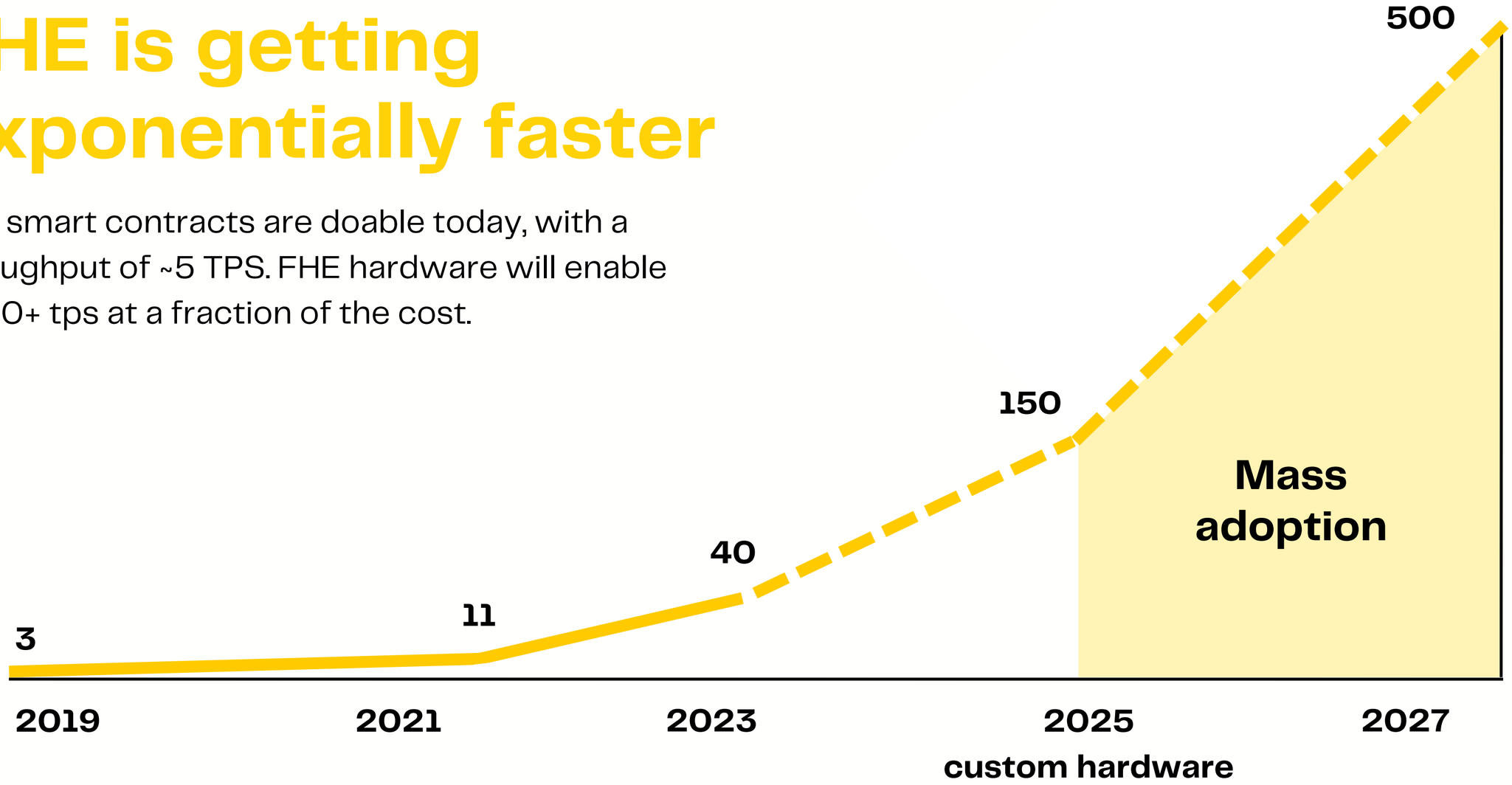
$$E[x] < E[y] = E[x < y]$$

More generally:

$$f(E[x], ..., E[y]) = E[f(x, ..., y)]$$

FHE is getting exponentially faster

FHE smart contracts are doable today, with a throughput of ~5 TPS. FHE hardware will enable 1,000+ tps at a fraction of the cost.



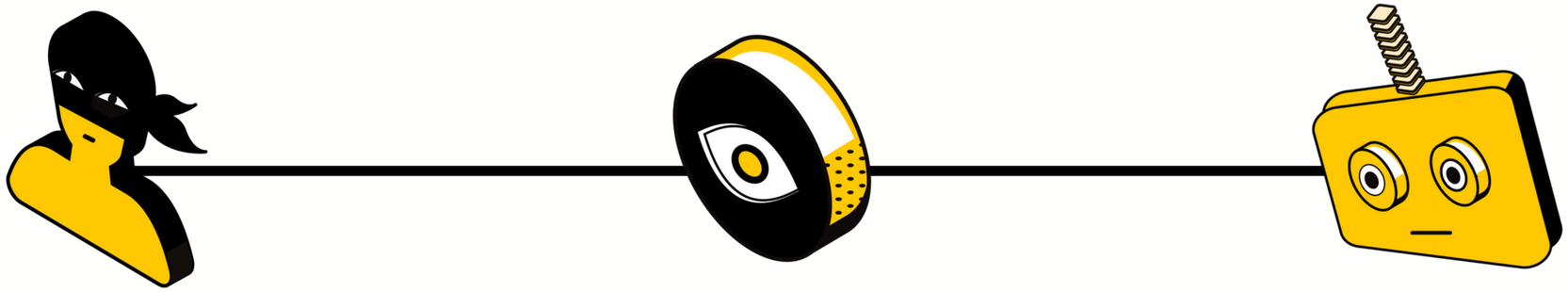
Onchain data is public by design, making it hard to build dapps that require confidentiality

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	IN	vitalik.eth	2,500	Step.app (KCAL)
0xd9f47a344e278579cb…	1 hr 15 mins ago	Justin Sun	IN	vitalik.eth	25,143,213.150843308745475521	Step.app (KCAL)
0xdea02c32d141997aaa…	12 hrs 57 mins ago	plamer.eth	IN	vitalik.eth	1	AssangeDAO (JUSTIC...)
0x74205c19a313ba8865…	1 day 11 hrs ago	Uniswap V2: SEGA 3	IN	vitalik.eth	227,158,544.808096280091774569	SEGA (SEGA)
0xad5c19e1af6de6508e…	2 days 20 hrs ago	0xad29c28a868c945caf9…	IN	vitalik.eth	21,420	ERC-20 (BASTAR...)
0x1014024546d2e94f39…	3 days 4 mins ago	Uniswap V2: ALIS 2	IN	vitalik.eth	153,473.76198500365822856	Acropolis DA... (ALIS)
0xbffdb2fcd52e96f136c7…	3 days 24 mins ago	vitalik.eth	OUT	OlympusDAO: DAO Funds	40,323.284453294043855726	Acropolis DA... (ALIS)
0x6ac57444413cd7bbef…	3 days 31 mins ago	Uniswap V2: ALIS 2	IN	vitalik.eth	40,323.284453294043855726	Acropolis DA... (ALIS)
0xb15136c85e15dd81b3…	3 days 1 hr ago	OlympusDAO: DAO Funds	IN	vitalik.eth	8,633.511805120159396357	Acropolis DA... (ALIS)
0xa9749c78f8ed9da996…	3 days 14 hrs ago	Uniswap V2: Bvlgari	IN	vitalik.eth	3,853,058,515,307.2989734036202684...	ERC-20 (Bvlgar...)
0x27fe35a36a42bbed75…	3 days 15 hrs ago	Uniswap V2: Bvlgari	IN	vitalik.eth	3,652,123,857,386.0501562459646840...	ERC-20 (Bvlgar...)

This leads to many privacy issues



Theft

Criminals know what you own, so they can easily target you and steal your crypto.

Surveillance

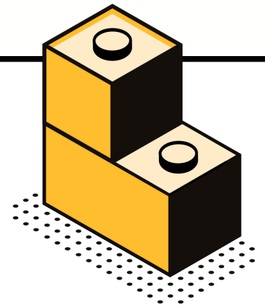
Governments can surveil you, even if you use multiple addresses.

MEV

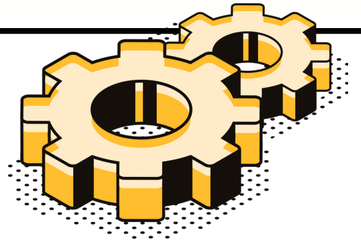
Bots can front-run you, creating a hidden tax on every transaction.

Zama's fhEVM enables confidential smart contracts using homomorphic encryption

E2E encryption of transactions and state

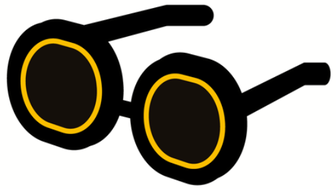


Composability and data availability onchain



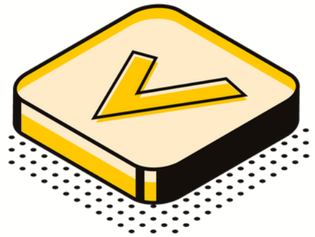
Doesn't break existing dapps and state

Without compromising transparency and usability



Computation

Users can still know what contracts are doing.



Access Control

Contracts are free to implement their own access control logic.

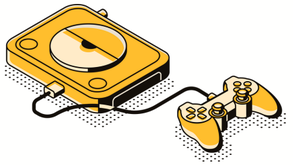
Composability

It is easy to mix data from multiple users and compose smart contracts.

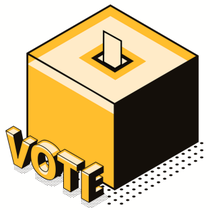
Zama's fhEVM unlocks new use cases

Tokenization
Manage and swap tokenized assets without other seeing it

Blind Auctions
Bid on items without revealing the amount or the winner

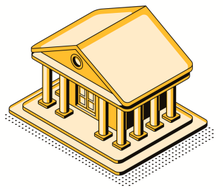


Onchain Games
Hide cards and moves until reveal (e.g. poker, blackjack, ..)



Confidential Voting
Prevents bribery and blackmailing by keeping votes private

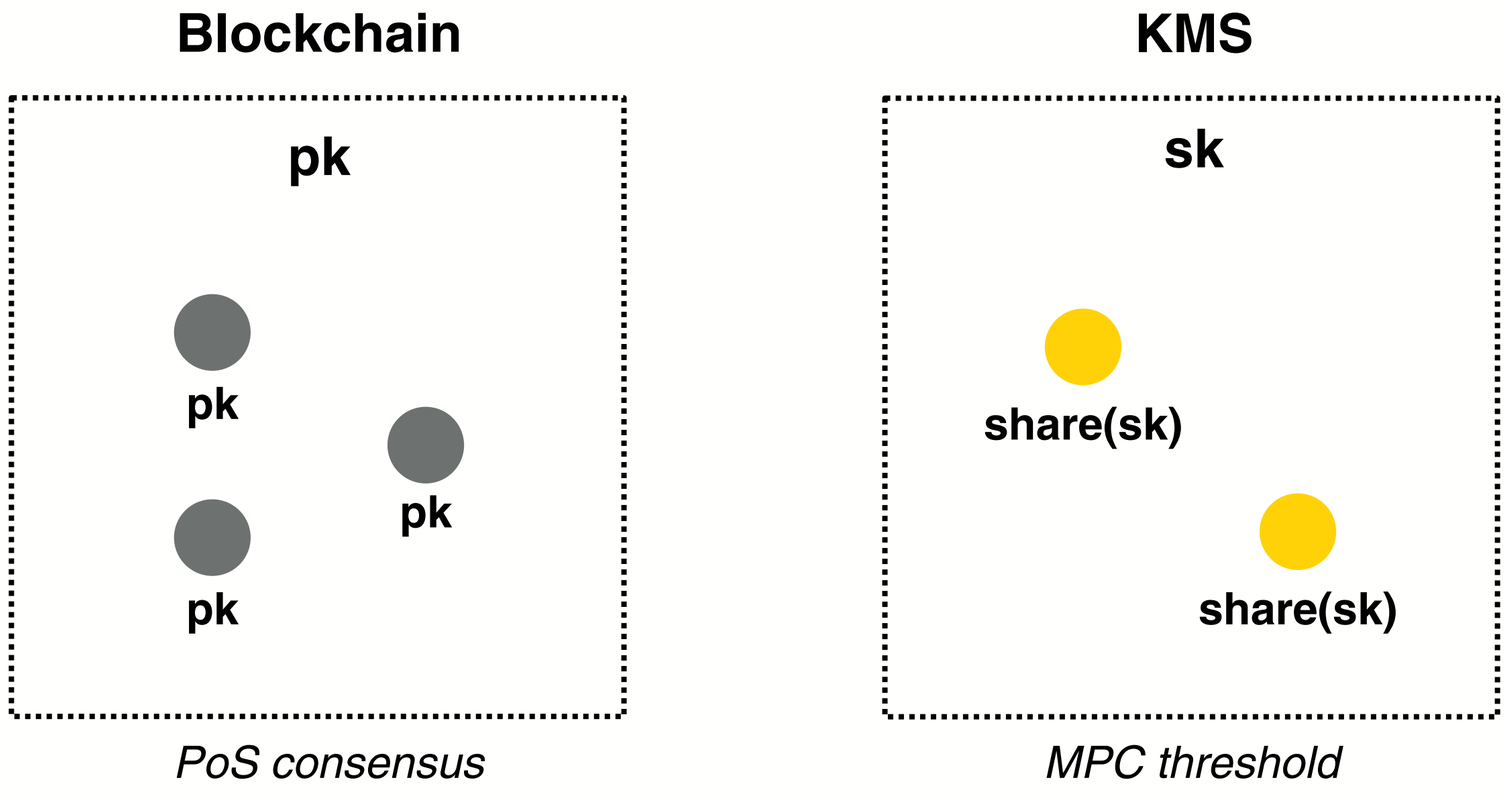
Encrypted DIDs
Store identities onchain and generate attestations without ZK



Private Transfers
Keep balances and amounts private, without using mixers

Zama's fhEVM: an overview

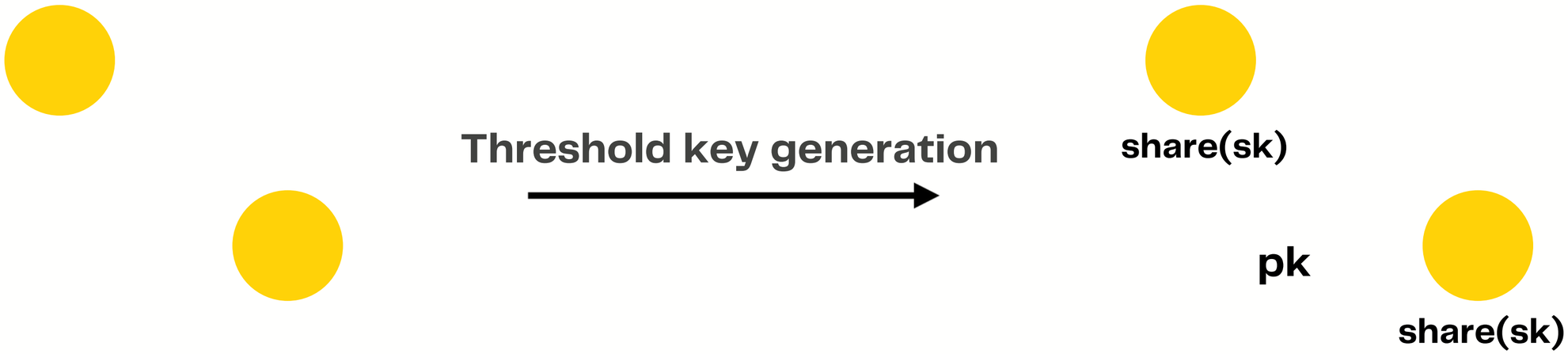
Everything is encrypted under a single global FHE public key



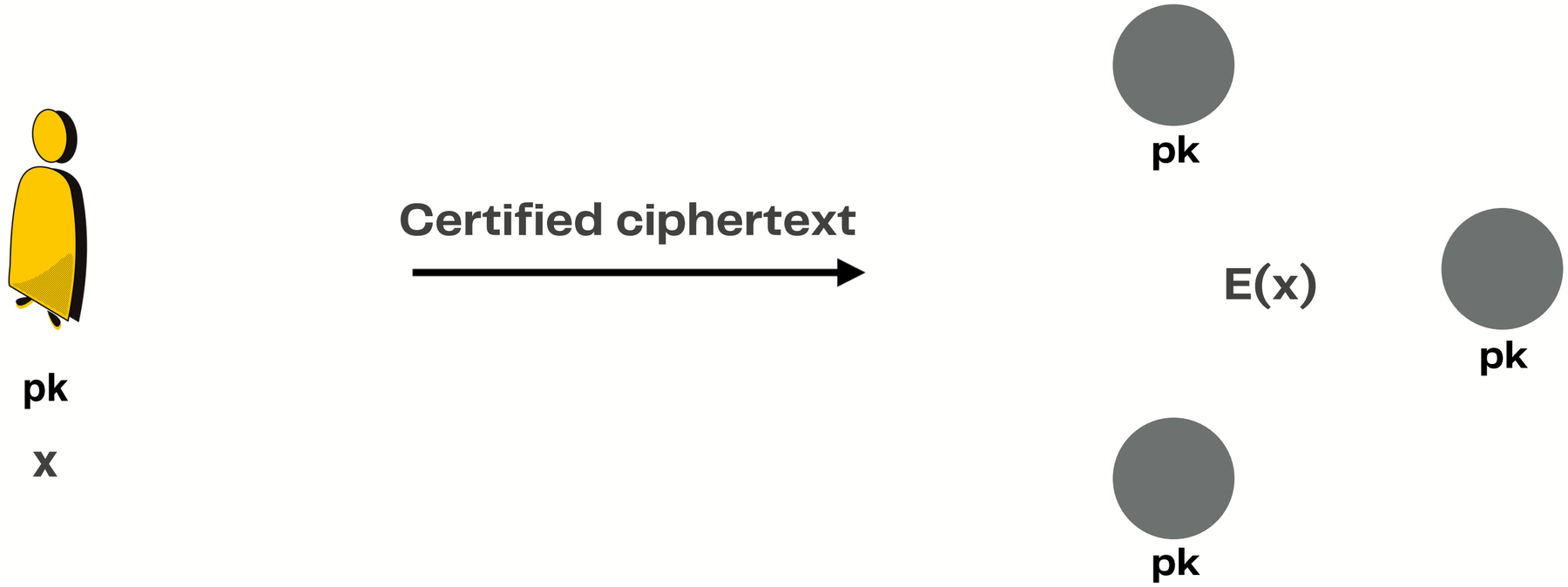
PoS consensus

MPC threshold

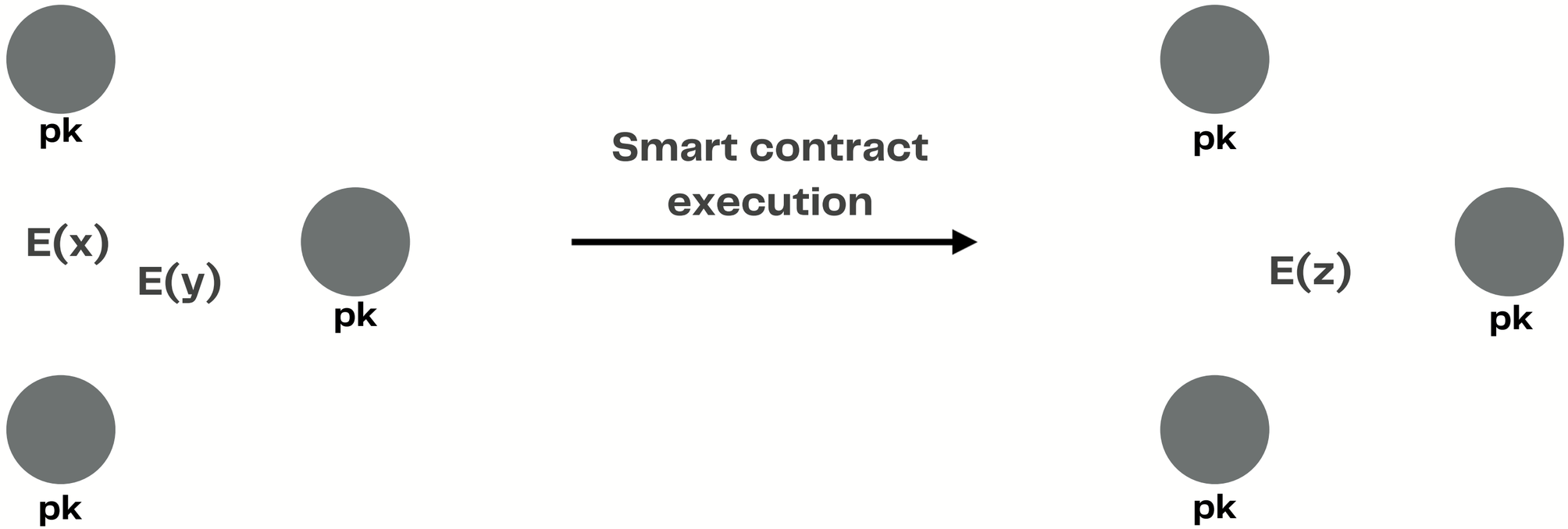
The global key is generated securely using a threshold protocol



The inputs are simply encrypted using the global public FHE key

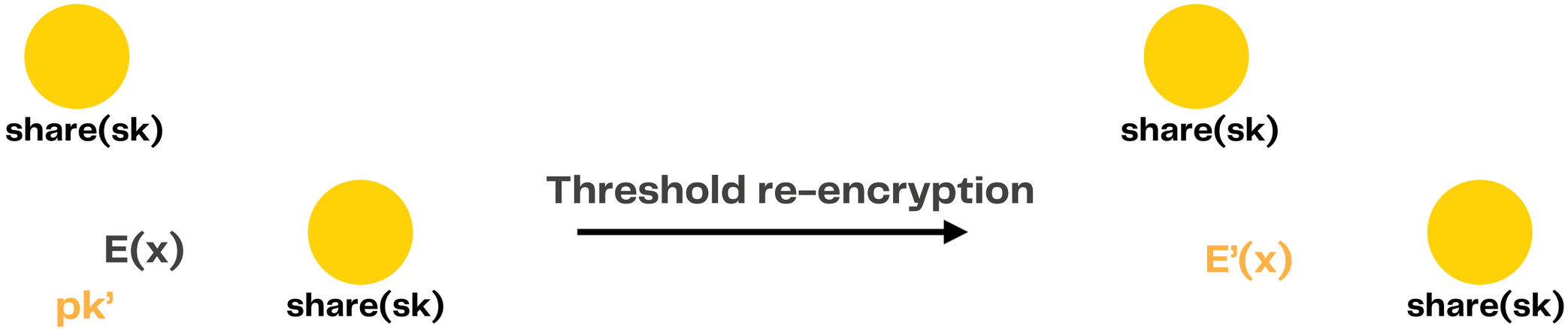


Computation is done locally by validators using homomorphic operations



Values can be decrypted by validators using a threshold protocol

Values can also be re-encrypted to user public key using a threshold protocol



Inside the fhEVM

Precompiled Smart Contract

- Calls out to Zama's FHE library (TFHE-rs)

Certified Ciphertexts

- Prevent misuse by keeping track of honestly obtained ciphertexts

github.com/zama-ai/fhevm

Developers can write confidential smart contracts without learning cryptography

```
contract EncryptedERC20 {

    // A mapping from address to an encrypted balance.
    mapping(address => euint64) internal balances;

    // Transfers an encrypted amount.
    function transfer(address from, address to, euint64 amount) internal {
        // Make sure the sender has enough tokens.
        ebool has_enough_funds = TFHE.le(amount, balances[from]);

        // Compute amount to actually transfer
        euint64 amount_to_transfer = amount * TFHE.asEuint64(has_enough_funds);

        // Add to the balance of `to` and subract from the balance of `from`.
        balances[to] = balances[to] + amount_to_transfer;
        balances[from] = balances[from] - amount_to_transfer;
    }

    // Returns the balance of the caller encrypted under the provided public key.
    function balanceOf(
        address wallet,
        bytes32 publicKey,
        bytes calldata signature
    ) public view virtual onlySignedPublicKey(publicKey, signature) returns (bytes memory) {
        if (wallet == msg.sender) {
            return TFHE.reencrypt(balances[wallet], publicKey, 0);
        }
    }
}
```

Solidity Integration

fhEVM contracts are simple solidity contracts that are built using traditional solidity toolchains.

Simple DevX

Developers can use the euint data types to mark which part of their contracts should be private.

Programmable Privacy

All the logic for access control of encrypted states is defined by developers in their smart contracts.

Challenges and research avenues

Technical challenges and research avenues

Scaling

- What would an optimistic or validity FHE rollup look like?
- What about hybrid rollups?

Incentives

- How to incentivize MPC parties not to collude?
- Can TEEs be used to prevent collusion?

MEV

- How does MEV look like on an encrypted blockchain?

arxiv.org/abs/2301.07041
ia.cr/2024/451

Zama's Bounty and Grant Program

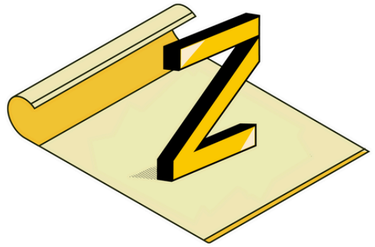
Build FHE applications to tackle real-world privacy challenges using Zama's suite of libraries

All info: https://github.com/zama-ai/bounty-and-grant-program

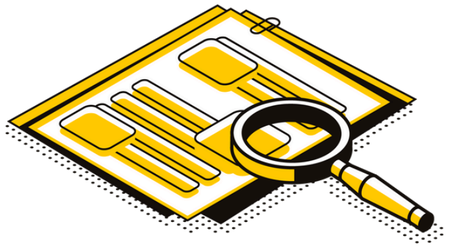
Obligatory self-promotion

Try the fhEVM yourself today

Github



White Paper



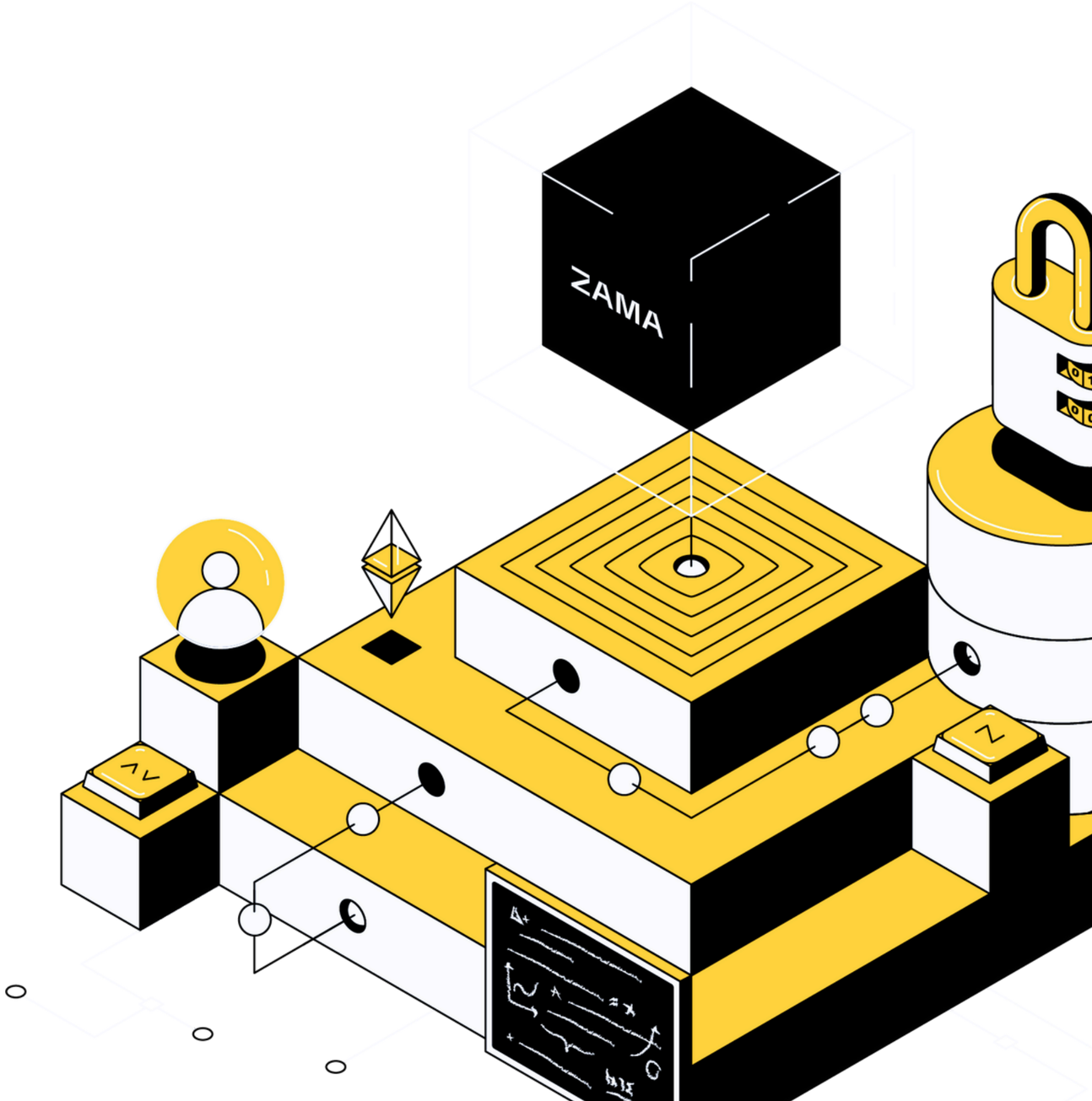
Documentation

Obligatory self-promotion

Zama is hiring

Join us in making protecting privacy easy.

–> jobs.zama.ai



Thank you.

ZAMA

Get in touch

@louis_tttt

zama.ai

github.com/zama-ai

@zama_fhe

ZAMA