LITEPAPER

OPENTRUST
LAB

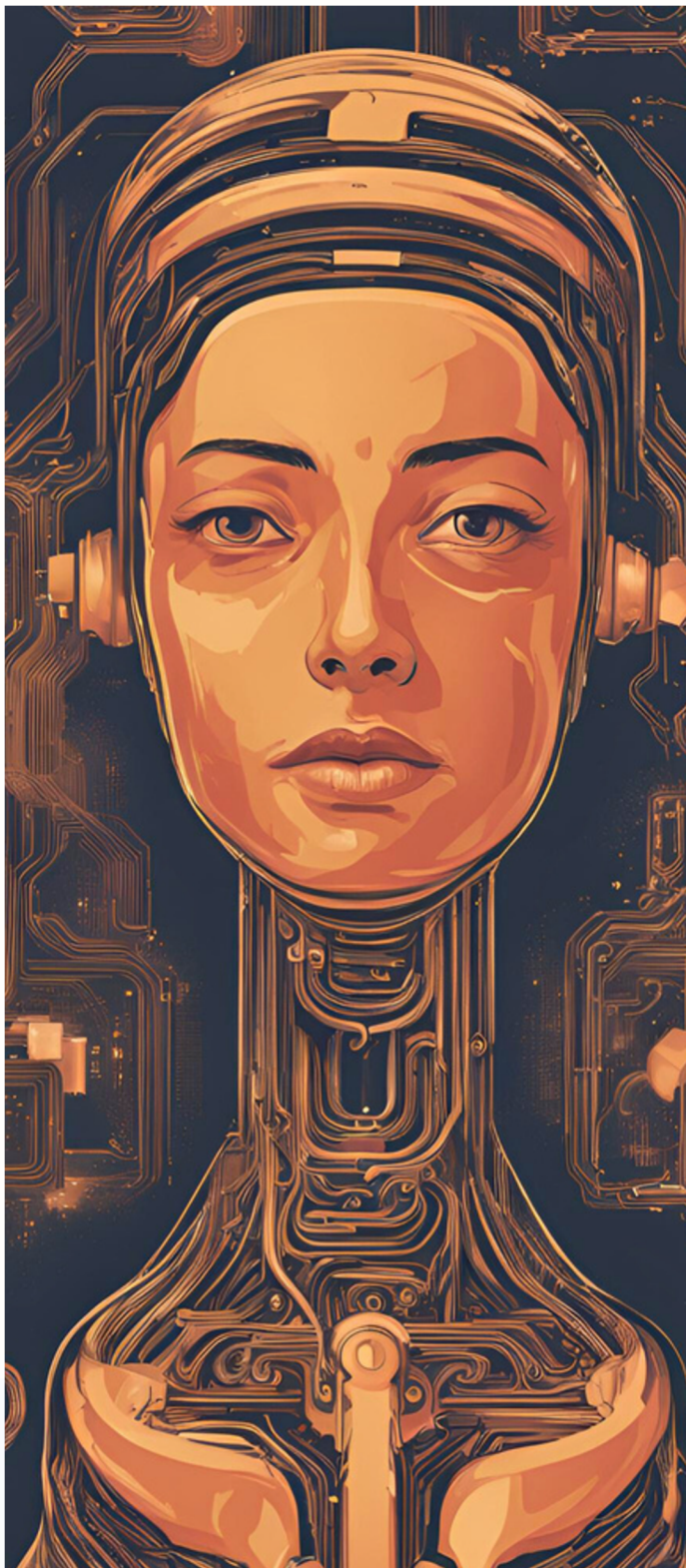
Building AI and Blockchain ecosystem
with practical FHE solutions

Oct 2024

Table of Contents

Introduction

Opentrust Lab is a research lab committed to pioneering the next generation of distributed cryptographic computing technologies. Our mission is to transform the AI and blockchain ecosystems by developing cutting-edge Fully Homomorphic Encryption (FHE) solutions. These innovations aim to deliver efficient, secure encryption, safeguarding data privacy and enabling the global adoption of intelligent applications. As the importance of data security and privacy grows, traditional encryption methods fall short of meeting both security and performance requirements. Opentrust Lab addresses these challenges by enabling computations on encrypted data without intermediate decryptions, allowing AI analytics to be conducted without exposing raw data. Moreover, it ensures that smart contracts are executed confidentially while still being verifiable by the public.



Introduction

In the AI sector

Opentrust Lab aims to build an encrypted ecosystem that not only protects the development process of AI models, but also enhances their computational efficiency. We introduce Shaftstop, a high-performance FHE architecture that enhances the speed of encrypted computations by innovatively introducing a set of lookup tables for ciphertext operations. Shaftstop achieves 1,000 times faster than mainstream TFHE encryption algorithms in logic gate operations, overcoming the performance limitations of current encrypted computation and making FHE solutions practical.

Based on Shaftstop, Opentrust Lab offers privacy-enhanced services for AI model to handle sensitive data. Our recent work has demonstrated the feasible implementation of privacy-enhanced models in Natural Language Processing, Computer Vision, and Knowledge Graphs. For instance, “FHEtorch” on our official website showcases how Opentrust enhances LLAMA3 inferences over encrypted data using Shaftstop. Additionally, Opentrust Lab will support the creation of high-quality data and model marketplaces, enabling developers to share and utilize data resources securely.

In the blockchain sector

Opentrust Lab provides the foundation for the development of encrypted smart contracts and the execution of encrypted data computations, driving the growth of various marketplaces. We are actively exploring and integrating FHE into various blockchain ecosystems, including Bitcoin, Ethereum, Solana, Dfinity, and so on.

In the future

Opentrust Lab will advance other encryption solution as Zero-Knowledge Proofs (ZK), Multi-Party Computation (MPC) and TEE(Trusted Execution Environment) with FHE. We will also combine practical quantum computing to optimize the speed and performance of FHE applications, committing to a future computing ecosystem that ensures data privacy while accelerating computational performance.

Problem

Current AI models face two major challenges:
Inference efficiency & Data privacy.

High computational demands limit deployment on low-power devices, restricting AI adoption. Meanwhile, on the privacy front, data breaches like the Facebook-Cambridge Analytica scandal, which exposed 87 million users' data for political manipulation, underscore the severe risks of centralized data storage. Such incidents erode user trust, incur heavy fines, and damage reputations, highlighting the urgent need for robust privacy protections. Additionally, AI models themselves are vulnerable to theft, risking unauthorized use and IP violations. Addressing these issues is critical to ensuring both data security and the integrity of AI models.

Problem

Existing solutions aimed at mitigating these concerns, such as Trusted Execution Environments (TEE) and Federated Learning, offer partial safeguards for user data privacy.

TEE (Trusted Execution Environment)

However, TEE encounters performance bottlenecks in model privacy protection due to limited memory capacity, frequent context switching, encryption/decryption overhead, and low I/O efficiency. These constraints hinder its ability to handle large-scale models, reducing its effectiveness in complex machine learning scenarios, despite its capability to ensure model integrity.

Zero-Knowledge Proofs (ZKPs)

Similarly, while Zero-Knowledge Proofs (ZKPs) are effective for safeguarding model privacy, their application in multi-party scenarios, such as private voting and decentralized games, remains significantly constrained. The core limitation lies in ZKP's inability to efficiently manage private shared states, which are essential in multi-party interactions. To circumvent this issue, developers often rely on off-chain storage for sensitive data, thereby introducing centralization and dependency risks. Additionally, designing ZK circuits for complex multi-party use cases is highly challenging, requiring specialized expertise in cryptographic languages and principles, which significantly raises development costs. Even when feasible, the on-chain verification of SNARK proofs remains resource-intensive, with each verification consuming approximately 200,000 gas on the Ethereum Virtual Machine (EVM). These factors collectively hinder scalability and limit the adoption of ZKPs in more advanced multi-party applications. Therefore, as AI continues to evolve and integrate into critical applications, overcoming these limitations is essential to build trust, protect intellectual property, and ensure the secure, efficient deployment of AI systems.

FHE:
The Solution to the Problem

Fully Homomorphic Encryption (FHE) offers a revolutionary approach to address the pressing challenges of data privacy and inference efficiency in AI applications. By enabling computations directly on encrypted data, FHE effectively protects user privacy and model integrity. This capability ensures that sensitive information remains confidential while allowing AI models to operate efficiently.

For example, on a data exchange platform, users' transaction data often needs to be processed, which typically involves the risk of data exposure. With Fully Homomorphic Encryption (FHE), user data is encrypted before being uploaded to the platform, allowing the platform to perform computations directly on encrypted data without needing to decrypt it. For example, a user can upload encrypted purchase records, and the platform can analyze them and generate personalized recommendations without accessing the plaintext information. This ensures that user privacy is protected while maintaining the accuracy and efficiency of the computations. Fig 1 provides an example on how a dataset looks like after it is encrypted by FHE.

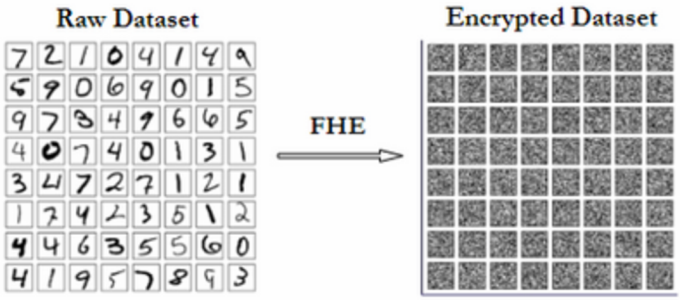


FIG 1: HOW A DATASET LOOKS LIKE AFTER FHE ENCRYPTION

FHE:
The Solution to the Problem

Opentrust Lab:
Practical Advancement with ShaftStop

Although FHE was proposed in 1978, its commercial applicability was severely limited by performance constraints. Our recent introduction of ShaftStop marks a significant advancement, making FHE practical for real-world applications. ShaftStop enhances traditional encryption systems by incorporating an evaluation function, structured as {KGen, Enc, Dec, Eval}. This framework allows for secure operations on ciphertext, facilitating complex computations without ever needing to decrypt the data or escrow keys. As a result, the risk of data leakage is minimized, addressing privacy concerns directly.

ShaftStop employs multivariate high-order polynomials with unknown functions for encryption. In the most challenging scenarios, this approach reduces to solving a multivariate quadratic (MQ) problem, which is computationally complex and enhances security through the use of a secret function key. This is one of the biggest innovations of ShaftStop. For example, a chaotic function can be used as the function key, ensuring that even minor changes in input produce significant differences in output.

The encryption process involves selecting random variables from the function key's domain, resulting in highly random ciphertexts, while the decryption process allows for straightforward recovery of plaintext by applying the appropriate key.

The other major innovation is to construct a set of lookup tables and archive the ciphertext computation by querying these tables. This is the origin of Shaftstop's high efficiency. We will provide more details on the construction of ShaftStop Ciphertext in the future whitepaper.

FHE:
The Solution to the Problem

Usecase 1:
Homomorphic Operations for AI Applications

ShaftStop supports very fast and high accuracy ciphertext computation for floating-point data . This capability is particularly crucial in the context of AI, where large datasets need to be processed securely and efficiently. By allowing operations on encrypted data, ShaftStop eliminates the need to expose sensitive information during computation.

Fig 2 illustrates a workflow where ShaftStop encrypts AI models and datasets, performing computations in ciphertext form to ensure that both the models and data remain encrypted throughout the process. This approach eliminates the need for decryption, key management, or the presence of plaintext at any stage, thereby mitigating the risk of data breaches.

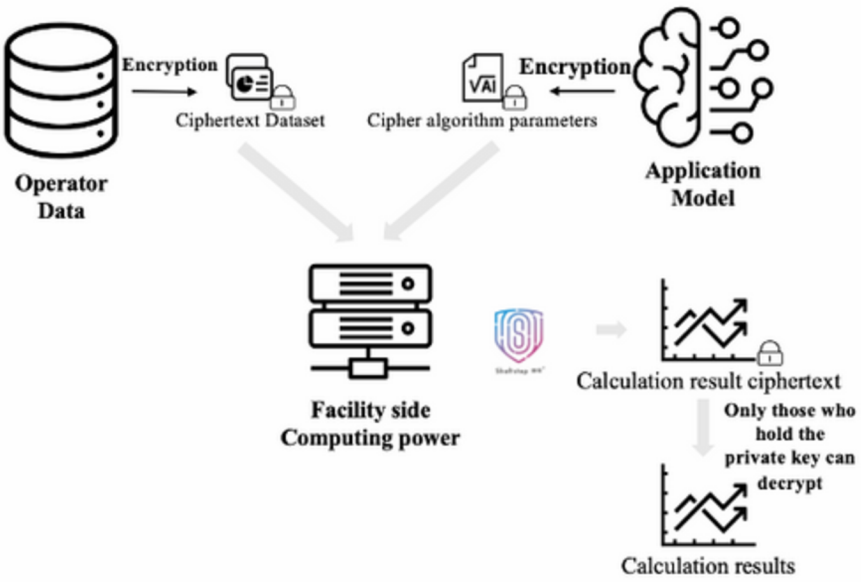


Fig 2: A Simple Workflow for Encrypting AI Models and Datasets

Usecase 2:
Blockchain Enhancement

ShaftStop significantly enhances the security of blockchain technology by encrypting sensitive data while maintaining transparency. Transaction details, such as amounts, remain confidential, even as other aspects of the transaction are publicly visible. This feature mitigates the risks associated with data leaks, a concern that has gained prominence in light of recent incidents involving unauthorized access to user information. By securing transaction data, ShaftStop helps to foster trust in blockchain systems. Fig 3 shows an example on how an encrypted WASM (in a new binary format) supports FHE ciphertext computing.

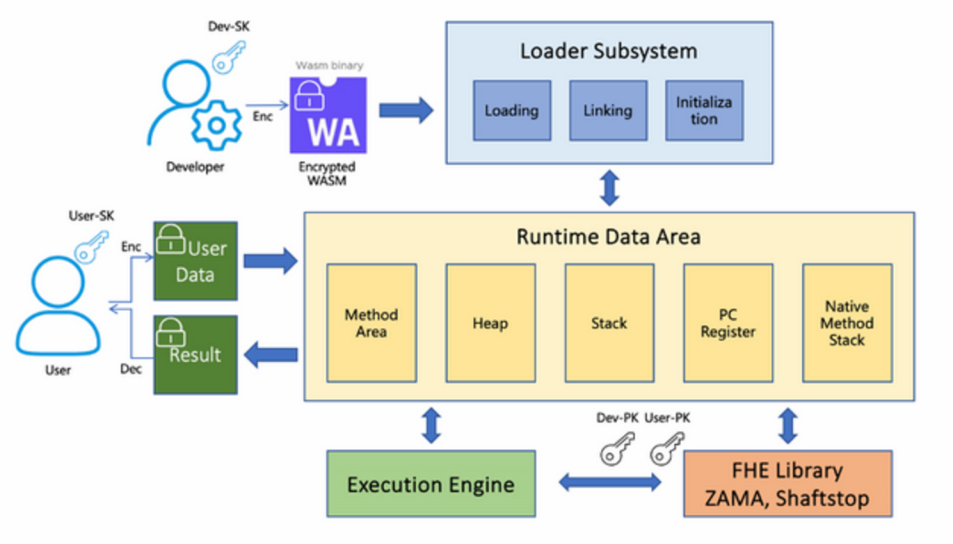


FIG 3: FHE-WASM ARCHITECTURE

Usecase 3:
Private Data Banks

As AI increasingly requires large datasets for training and inference, ShaftStop provides a viable solution for training AI models on encrypted data. This approach ensures that sensitive information—such as medical or biometric data—remains secure throughout the entire processing lifecycle. Additionally, ShaftStop facilitates the establishment of private data banks, where individuals and organizations can securely store encrypted data. These banks enable the performance of complex computations and analyses without ever accessing plaintext data, reinforcing both privacy and security.

FHE: The Solution to the Problem

Differentiation with Zama

We follow a different technical route from ZAMA. We don't need to decompose integers and original plaintext into binary bit for encoding and encryption. At the same time, we apply a lookup table mechanism to match the ciphertext and encryption methods. Therefore, the computing speed will increase dramatically while ensuring security.

Our team has been researching this method since 2014. After more than ten years of algorithm design and expert demonstration, it has obtained positive review and evaluation of authoritative institutions. Our security and decryption difficulty are based on Multivariate Quadratic Problem (MQ Problem is often studied as a source of hardness assumptions for cryptographic schemes. The complexity of this problem lies in the large number of variables and the quadratic nature of the polynomials, making it hard to find efficient algorithms to solve it). This approach has been thoroughly tested and refined over the years, ensuring a high level of security and making decryption an extremely challenging task. With a decade of dedicated research and the input of numerous experts, our solution has proven to be reliable and robust.

Market Figures

The data trading and AI public cloud services are experiencing strong expansion, with market sizes steadily each year, as shown in Fig 4.

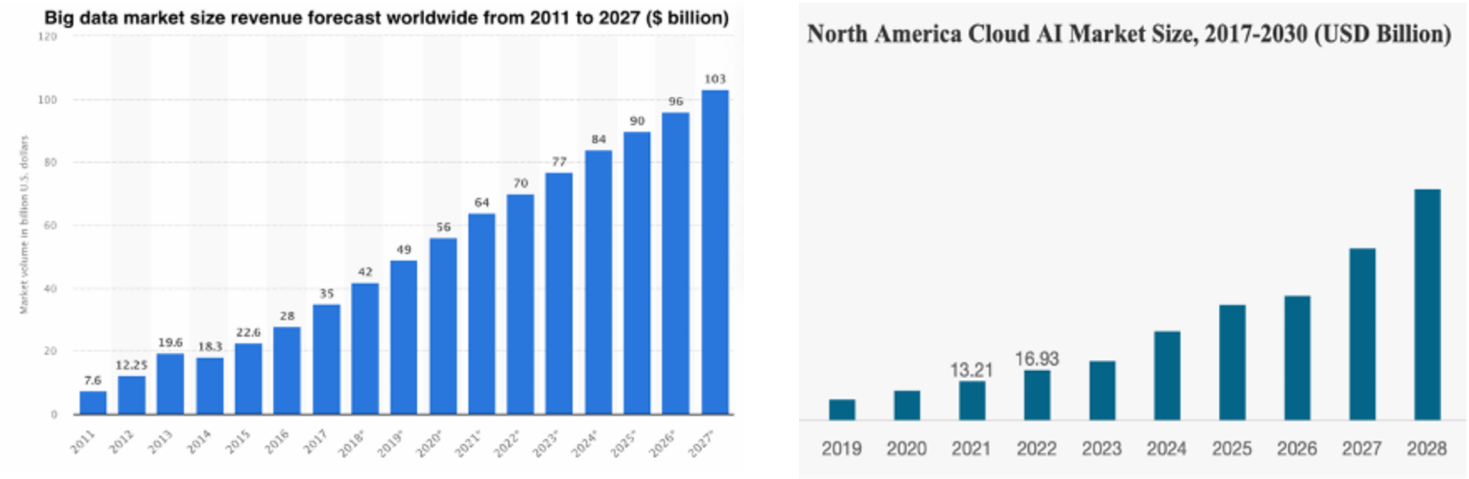


Fig 4. Big data market size revenue worldwide and North America Cloud AI market size

According to forecasts from Statista and Fortune Business Insights, the global big data market is expected to reach approximately $103 billion by 2027, while the North American AI cloud market is projected to grow to $40 billion by 2030, highlighting significant opportunities for innovation and investment.

Additionally, it is estimated that the global software and hardware encryption market will reach 666.51 billion dollars by 2028, further underscoring the value of FHE technology in protecting sensitive information. (Zion Market Research) (Research and Markets)

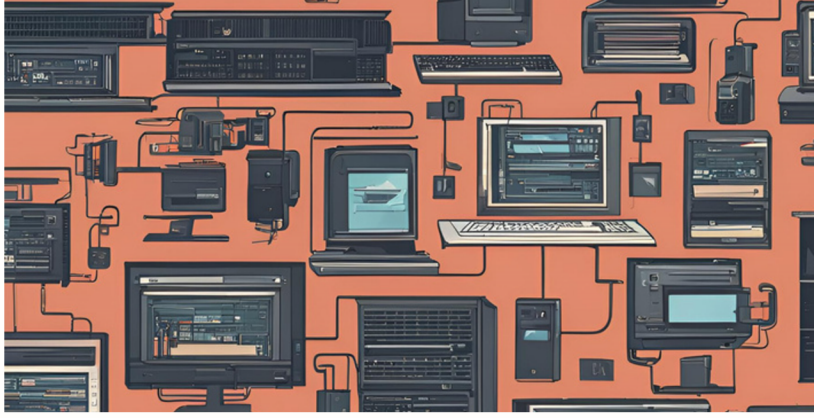
With encrypted self-service processing and encrypted model inference, we provide essential security and privacy protections for these rapidly growing markets. Our approach not only enhances computational efficiency but also ensures strong privacy safeguards, positioning us as a crucial solution for organizations seeking to leverage data while maintaining compliance with privacy regulations. Our technology also exhibits vast potential in emerging fields such as AI and blockchain.

Team History and Background

The team has over 10 years of experience in cryptography and related fields and has established relationships with both academic and industry leaders, such as Zama.

Core team members and advisors include professors and PhDs from Stanford, UC Berkeley, Yale, Bristol, etc.,

Future Plans



In our future development strategy, we aim to methodically expand both our technological capabilities and ecosystem by integrating Fully Homomorphic Encryption (FHE), Artificial Intelligence (AI), blockchain, and privacy computing. Our initial focus will be on enhancing FHE support in AI models, particularly in areas like knowledge graphs, speech recognition, and computer vision, ensuring sensitive data remains secure while improving AI accuracy and efficiency.

To accelerate performance, we will leverage hardware acceleration such as GPUs and FPGAs in the short term, while exploring quantum computing for further optimization. This will allow us to process complex, privacy-preserving AI tasks more efficiently in the long term.

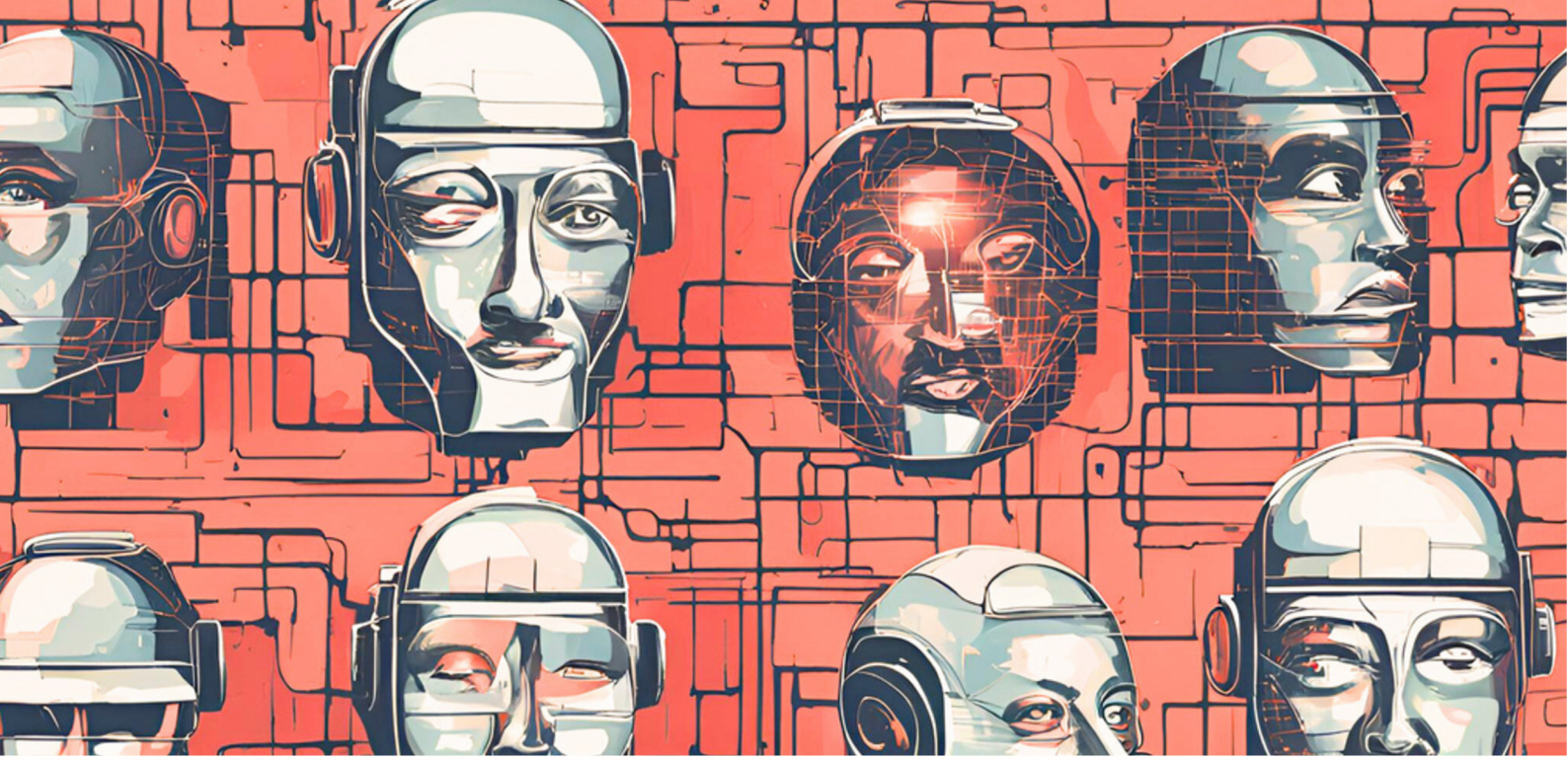
Simultaneously, we will prioritize the integration of FHE with blockchain, utilizing FHE-based WebAssembly (WASM) to develop privacy-focused blockchain solutions. This includes creating a data marketplace where encrypted data can be securely exchanged, unlocking new opportunities in industries like healthcare, finance, and IoT.

We will also address privacy challenges in decentralized finance (DeFi) and decentralized physical infrastructure networks (DePIN) by collaborating with over 20 DApp clients. By combining FHE with technologies like Zero-Knowledge Proofs (ZK) and Multi-Party Computation (MPC), we will build a comprehensive privacy computing ecosystem, supporting scalable and secure decentralized applications.

From the user perspective, we will provide customized services for enterprises, and there will be a dedicated team to evaluate and help customers meet their needs.

Looking forward, we will continue to prioritize innovation while fostering collaboration with academic and industry partners to drive knowledge exchange, research, and the development of privacy standards, solidifying our leadership in privacy-preserving technologies and decentralized ecosystems.

If you are interested in any of the above aspects, we are more than happy to collaborate.



Conclusion

In conclusion, Opentrust Lab is at the forefront of revolutionizing data security and privacy through its innovative Fully Homomorphic Encryption (FHE) technology, Shaftstop. This solution addresses critical challenges in the AI and blockchain landscapes by enabling secure computations on encrypted data, ensuring user privacy while enhancing computational efficiency. As the data trading industry and AI public cloud services continue to grow, the importance of robust privacy measures becomes increasingly vital. Shaftstop not only mitigates risks associated with data breaches but also supports the creation of private data banks, facilitating secure AI model training. With the global FHE market projected to reach $666.51 billion by 2028, Shaftstop positions itself as a key player in promoting trust and enabling the responsible use of advanced technologies across various sectors.

Opentrust Lab invites investors, developers, and users to join us in revolutionizing data security with Shaftstop. Be part of the future of privacy protection in AI and blockchain. Contact Opentrust Lab today to help drive the next wave of secure, innovative technology!

Contact Us

Email	opentrustlab@gmail.com
Twitter(x)	@OpentrustLab
YouTube	@OpentrustLab
Github	Opentrust-Lab

Reference List

1. Research and Markets, Global Hardware Encryption Market Report and Forecast 2023-2028, *Research and Markets,* <https://www.researchandmarkets.com/reports/5901126/global-hardware-encryption-market-report>.
2. Zion Market Research 2021, ZM Global encryption software market to witness impressive growth, revenue to surge to USD 29.1 billion by 2028, *Zion Market Research*, <https://www.zionmarketresearch.com/news/global-encryption-software-market.>.