CORNAMI®
Intelligent Computing

Enhanced Trust and Security in Smart Contracts with Fully Homomorphic Encryption

Table of Contents

ABSTRACT ***1***

CHALLENGES ***2***

Data Privacy **2**

Low Scalability **3**

SOLUTIONS ***4***

Incorporation of Advanced Technologies (FHE) **4**

Scalable Performance **4**

Enhanced Security Measures **5**

Key Advantages of FHE-enabled Smart Contracts **6**

BENEFITS ***7***

Accuracy **7**

Speed and Transparency **7**

Data Privacy **8**

Cost Savings **8**

The Impact of Scalable Computing on Privacy-Enhancing Technologies ***9***

Conclusion ***10***

SOURCES: ***10***

ABSTRACT

In the dynamic arena of digital transactions, the concept of Smart Contracts marks a pivotal innovation, re-engineering the core mechanics of contractual engagement. These protocols, operating autonomously, execute the specifics of an agreement embedded within their code. This digital automation dispenses with traditional intermediaries, optimizing the transaction process for heightened efficiency, reduced costs, and bolstered trust.

Crucial to Smart Contracts is blockchain technology, offering a decentralized ledger that immutably logs contract stipulations, nullifying the risks of alteration and the ambiguities often associated with conventional contracts. Such a system is propelling various sectors, including finance and healthcare, towards an automated and lucid economy.

Yet, the progression of Smart Contracts is tethered to data privacy challenges, like those faced in the healthcare sector's management of sensitive information. Here, Fully Homomorphic Encryption (FHE) could play a game-changing role. By permitting computations on encrypted data without decryption, FHE could reinforce Smart Contracts against the invasive threats to privacy, all while enabling the essential analytics and data exchange needed to push the digital transaction space forward.

The practical adoption of FHE within Smart Contracts has been hindered by its demand for intensive computation—until the advent of Cornami's FracTLcore™ computing fabric technology. Cornami's scalable and configurable computing architecture is specifically designed to meet the rigorous demands of FHE, and transcends traditional computational constraints, presenting a massively scalable and on-the-fly configurable computing architecture. This innovation signals the transition of a theoretically robust security measure into a commercially viable reality for Smart Contracts, potentially catalyzing a new era of secure and efficient data sharing.

The paper acknowledges the practical challenges that have historically impeded the adoption of FHE, such as its intensive computational demands. It suggests that these obstacles might be overcome through innovative computing architectures, specifically Cornami's FracTLcore® Compute Fabric. This technology promises the necessary computational power to render FHE a feasible option for organizations dealing with and executing smart contracts.

This whitepaper aims to dissect the intersection of Smart Contracts' role in data exchange, the imperatives for stringent cybersecurity, and the advanced computing solutions poised to redefine data transaction security. It intends to outline a prospective trajectory, illuminating a path to harness the power of data amidst the complexities of privacy and security in an increasingly data-centric landscape.

CHALLENGES

Data Privacy

The integration of Smart Contracts into the digital landscape offers a paradigm shift in executing and enforcing agreements, but it also brings forth considerable challenges concerning data privacy. Traditional contracts, typically documented on paper, inherently safeguard sensitive information within the confines of the involved parties. This is not the case with Smart Contracts, whose terms are coded and stored on a blockchain, visible to any participant in the network.

This level of transparency, a cornerstone for the trustworthiness and auditability of blockchain transactions, stands in stark contrast with the privacy requirements of contractual agreements. Sensitive data, once recorded on the blockchain, is immutable and can be accessed by any party, potentially compromising the confidentiality that is often crucial in business dealings.

In response to this dichotomy, researchers and technologists have been exploring cryptographic solutions to reconcile the need for both privacy and transparency. The development of zero-knowledge proofs (ZKPs), as discussed by Kosba et al. in "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," provides a means to verify the correctness of transactions without revealing underlying details, offering a layer of privacy previously unattainable in public blockchains [1].

Further, the decentralization of privacy, as detailed by Zyskind, Nathan, and Pentland, allows for the protection of personal data through blockchain technology, creating a secure environment where information can be verified without being exposed ("Decentralizing Privacy: Using Blockchain to Protect Personal Data") [2].

However, the intersection of blockchain technology with existing legal frameworks introduces additional complexities. Finck's exploration of "Blockchain Regulation and Governance in Europe" highlights the tension

between blockchain's immutable nature and regulatory requirements, such as the GDPR's right to erasure, indicating a need for ongoing dialogue and development in this area [3].

As the application of Smart Contracts becomes increasingly mainstream, addressing the challenge of data privacy will necessitate a multifaceted approach that includes advancements in cryptographic techniques, legal adaptations, and continued research into privacy-preserving technologies.

Low Scalability

Smart Contracts, while effective for handling straightforward agreements, face a substantial scalability challenge as their complexity grows. This issue is particularly pronounced within blockchain networks, the foundational infrastructure for Smart Contracts. These networks grapple with limited transaction throughput, increased latency, and the expanding size of the blockchain itself. As operations become more intricate, these challenges are further compounded.

Technologies like sidechains and state channels have emerged as potential solutions to improve blockchain scalability. Sidechains are separate blockchains that run parallel to the main blockchain, designed to increase transaction throughput and scalability for specific applications [4]. State channels take a different approach by enabling a series of transactions to occur off-chain, with only the final state being recorded on the main blockchain, thus reducing network congestion and improving transaction speeds [4].

Moreover, Scalable Distributed Ledgers, which distribute the workload across multiple nodes, have been identified as a key solution for overcoming these scalability challenges. By doing so, they can handle a high volume of transactions while maintaining network capacity and speed [4].

The scalability trilemma remains a fundamental challenge, referring to the difficulty in achieving a balance between decentralization, security, and scalability simultaneously. It's a delicate balance where enhancing one aspect may compromise another [4]. The next generation of Smart Contracts, referred to as Smart Contracts 2.0, aims to address these scalability challenges by utilizing advanced technologies such as sidechains and off-chain computation to increase scalability and improve transaction speeds [4].

The scalability of Smart Contracts is a multifaceted issue that requires the continuous development of blockchain technology and the implementation of innovative solutions. Chainlink provides an overview of various approaches to blockchain scalability, discussing the trade-offs and advantages of each method, which could be instrumental in enhancing the scalability of Smart Contracts [5].
The scalability dilemma extends beyond mere technical barriers; it directly impacts the widespread adoption and practical implementation of Smart Contracts in large-scale business operations. Without a scalable solution to handle the burgeoning complexity, the potential of Smart Contracts to revolutionize various industries remains unrealized.

Fortunately, emerging advancements in scalable computing architectures offer promising avenues to address these monumental workloads. Cornami's FracTLcore™ computing fabric stands out among these innovations,. With its ability to handle extensive computational demands efficiently, FracTLcore™ technology presents a viable solution to the scalability woes plaguing Smart Contracts. By leveraging such cutting-edge technologies, businesses can unlock the full potential of Smart Contracts, enabling seamless integration into their operations and fostering innovation on a much broader scale.

SOLUTIONS

Incorporation of Advanced Technologies (FHE)

Fully Homomorphic Encryption (FHE) represents a breakthrough in data privacy for blockchain-based Smart Contracts. With FHE, data remains encrypted throughout its entire lifecycle, including during processing. This means that sensitive information is not exposed at any point, providing robust privacy guarantees for Smart Contracts deployed on public, permissionless blockchains. FHE's capability to perform computations on encrypted data enables Smart Contracts to automate contractual events and actions securely, without ever decrypting the underlying information. This leads to increased transaction efficiency, accuracy, and security while preventing fraud and unauthorized data exposure [6], [7].

FHE allows for the confidentiality of contractual terms, events, and actions, ensuring that their definitions and histories remain encrypted and secure from breaches. Furthermore, the ability to compute on encrypted data means that Smart Contracts can fully automate the recognition of contractual events and subsequent actions, all while maintaining the confidentiality of the data involved [8].

Current advancements in FHE are making smart contracts not only more private but also increasingly performant. With the development of FHE-specific ASICs and improvements in the underlying cryptographic algorithms, the potential throughput for Smart Contracts using FHE is expected to grow significantly, reaching thousands of transactions per second and reducing costs [6].

The integration of Fully Homomorphic Encryption (FHE) into blockchain technology, as demonstrated by projects like Zama's fhEVM and Fhenix's layer-2 network, represents a notable advancement in ensuring the privacy and security of smart contracts. However, the computational demands of FHE, especially when combined with other privacy-preserving techniques like Multi-party Computation (MPC) and Zero-Knowledge Proofs (ZK), necessitate significant hardware acceleration to achieve practical feasibility. [7], [8].

Traditional computing systems often struggle to efficiently handle the complex calculations required for FHE operations alongside MPC and ZK protocols. This is where Cornami's Scalable Computing Fabric technology comes into play. Cornami's architecture is specifically designed to tackle the computational challenges posed by advanced cryptographic techniques such as FHE, MPC, and ZK.

By leveraging FHE alongside Multi-party Computation (MPC) and Zero-Knowledge Proofs (ZK), FHEVM offers an unprecedented level of privacy and security, enabling applications that handle sensitive data to benefit from blockchain technology's transparency and immutability without compromising confidentiality [8].

Cornami's Scalable Computing Fabric technology offers massive hardware acceleration capabilities, enabling the rapid processing of encrypted data while maintaining high levels of privacy and security. By leveraging Cornami's solution, blockchain developers can harness the power of FHE, MPC, and ZK without being hindered by computational bottlenecks. This allows for the seamless integration of advanced cryptographic techniques into blockchain applications, empowering developers to create privacy-preserving smart contracts with ease and efficiency.

Scalable Performance

The concept of scalable performance within the realm of Fully Homomorphic Encryption (FHE) is a groundbreaking innovation that significantly enhances the practicality and applicability of Smart Contracts. Cornami's approach to FHE performance and latency is particularly interesting as it introduces a scalable infrastructure that can be tailored to meet specific service level agreements (SLAs) for various use cases.

At the core of this scalability is the unique correlation between performance, latency, and the number of Cornami servers utilized. This means that the infrastructure can be dynamically adjusted to handle varying computational loads by simply altering the number of servers in operation. By implementing Cornami's FHE hardware acceleration, the execution of Smart Contracts becomes highly adaptable, with the flexibility to increase computing resources to reduce response times or scale down during periods of lower demand.

Cornami's technology promises to address one of the primary challenges faced by Smart Contracts – the ability to achieve predictable and responsive performance levels that align with the stringent requirements of business operations. As the execution platform for FHE-enabled Smart Contracts, Cornami enables users to precisely define their SLA response times according to the deployed server capacity.

This scalability is essential for the widespread adoption of Smart Contracts in sectors where response time is critical. For instance, in financial services, where millisecond delays can equate to significant monetary losses, or in supply chain management, where real-time tracking and updates are paramount, Cornami's scalable performance could ensure that Smart Contracts deliver reliable and timely outcomes.

Furthermore, this scalable approach could catalyze the development of more complex and feature-rich Smart Contracts, as developers would no longer be constrained by the performance limitations of traditional blockchain platforms. With Cornami's FHE hardware acceleration, the potential for innovation in Smart Contract design and implementation is vast, opening new avenues for automation and computation in secure, decentralized environments.

Enhanced Security Measures

Enhanced security in Smart Contracts, particularly in the context of Fully Homomorphic Encryption (FHE), has taken a significant leap forward thanks to the incorporation of lattice-based cryptographic systems recognized as Post Quantum Cryptography (PQC). These cryptographic systems are known to be resilient against both traditional and quantum computing attacks, providing a robust layer of security for Smart Contracts on blockchain platforms.

FHE utilizes complex mathematical structures called lattices, where the difficulty of solving certain problems in high-dimensional lattice space forms the basis of the encryption's security. This complexity is believed to be secure against quantum computer attacks, making it a viable candidate for securing data in a future where quantum computing is prevalent [9].

Smart Contracts encrypted with FHE benefit from this advanced encryption by ensuring that their blockchain entries remain confidential throughout their entire lifecycle. They remain encrypted during computation, and only when necessary, encrypted data can be securely decrypted in a trusted environment, away from the public blockchain. This ensures that plaintext data and decryption keys are not exposed, significantly reducing the risk of data breaches or unauthorized access [6].

The security provided by FHE is not just theoretical but is backed by ongoing research and development. For example, the TFHE scheme is built upon lattice-based cryptography and is designed for efficient bootstrapping and precise computations. This scheme is integral for operations that require a high level of security and privacy, such as confidential voting, blind auctions, and other applications where data confidentiality is paramount [6].

Moreover, the homomorphic aspect of FHE allows computations to be performed on encrypted data without ever decrypting it, which is crucial for maintaining the integrity and confidentiality of the data. This aspect is especially important when dealing with sensitive information where data exposure can have significant consequences [10].

As we advance, FHE is expected to become exponentially faster, with the development of hardware accelerators that could potentially increase the throughput of Smart Contracts using FHE to thousands of transactions per second. These advancements in FHE are paving the way for broader adoption in various industries, ensuring enhanced security measures for Smart Contracts that meet the stringent requirements of modern-day digital transactions [6].

The continuous improvements in the field of FHE are creating a robust foundation for the secure implementation of Smart Contracts, contributing significantly to the trustworthiness and reliability of blockchain technology in handling sensitive and private data.
Increasing Efficiency While Reducing Risk
The utilization of Fully Homomorphic Encryption (FHE) in Smart Contracts ushers in a new era where trust between contractual parties is transformed. With FHE, the reliance on trust is diminished because the encrypted nature of Smart Contracts ensures that confidentiality is maintained, allowing businesses to automate their operations securely. This introduces a significant leap in efficiency and risk reduction.

Key Advantages of FHE-enabled Smart Contracts

- **Protected Contractual Details:** All components of a contract, including its terms, historical events, and associated actions, remain encrypted and safeguarded against unauthorized access or breaches. This encryption persists across the contract's lifecycle on the blockchain, ensuring the data's integrity and confidentiality.

- **Automation and Efficiency:** The automation of contract terms expedites processing times, thus increasing the overall operational efficiency. Smart Contracts, by virtue of being encoded in software, remove the delays inherent in manual processing, leading to a more fluid and error-free execution of contractual obligations.

- **Minimized Risks:** The risks associated with misinterpretation, tampering, and fraudulent activities are significantly reduced due to the immutable and encrypted nature of Smart Contracts. This is because the potential for human error or intentional manipulation is greatly lessened when processes are automated and secured through encryption.

- **Auditability:** Despite the encrypted state of the contract's contents, the blockchain's nature allows for an auditable trail of all transactions and contract events. This transparency, paired with the security of

encryption, provides a reliable means to verify the contract's execution while maintaining the necessary privacy.

FHE-enabled Smart Contracts represent a critical development in the realm of digital agreements, offering a sophisticated mechanism to maintain privacy while still leveraging the inherent benefits of blockchain technology. As FHE technology matures, we anticipate even greater efficiencies and reduced risks, solidifying the role of Smart Contracts as a cornerstone of modern business operations [6], [11].

BENEFITS

Accuracy

Smart contracts provide a mechanism to enhance the accuracy of transactions and agreements by automating the execution of contractual terms. This automation minimizes human error, which is common in traditional manual transaction processes. The use of blockchain technology ensures that once a smart contract is deployed, it is immutable and transparent, making it resistant to unauthorized alterations or tampering. Such a system creates an auditable trail that allows all parties involved to verify the accuracy of the contract execution without the need for intermediaries like lawyers or notaries, which traditionally could introduce delays and potential for errors [12], [13].

The automation of smart contracts is not just about reducing the likelihood of errors but also about enhancing the efficiency and integrity of contractual obligations. For example, smart contracts can include mechanisms for conditional execution, where actions are automatically performed only when certain predefined conditions are met. This could be combined with escrow mechanisms, where funds or assets are held securely until all parties meet the conditions of the agreement, thereby reducing the risk of disputes or errors in fulfillment [13].

In essence, smart contracts shift the responsibility for executing and verifying agreements from humans to code, which can execute flawlessly if it is written correctly. This shift significantly reduces the chances of miscommunication and errors that can arise from manual processes. However, it also means that the accuracy of a smart contract is heavily dependent on the precision of its code. The development of smart contracts requires a high level of attention to detail to ensure that the code accurately reflects the terms of the agreement and includes measures to handle any potential exceptions or errors that could occur during its execution [12].

Speed and Transparency

The integration of Fully Homomorphic Encryption (FHE) alongside hardware acceleration into Smart Contract technology marks a pivotal advancement in achieving both speed and transparency in blockchain transactions. Current Smart Contract technologies already facilitate simultaneous or near-instantaneous transactions across various parties, boosting efficiency and maintaining full security and transparency in transaction execution. FHE brings an additional layer of confidentiality to this framework. With FHE, blockchain entries, although public, are encrypted, allowing only authorized participants to access the full details of transactions. This encrypted state ensures that the terms, events, and actions, as well as their histories within a contractual relationship, remain confidential and protected against unauthorized disclosure [6], [14].

The transparent nature of blockchain technology provides an immutable and auditable trail of all transactions, ensuring that every action is verifiable and reliable. FHE enhances this by ensuring that while transparency is maintained for the integrity of the system, the contents of transactions remain private. This duality is crucial for applications requiring both public verifiability and privacy, such as in voting systems or sealed-bid auctions [6].

FHE is not only about maintaining privacy; it's also about preserving the speed of blockchain transactions. While traditional rollups used for scalability, such as ZK Rollups, can be computationally intensive, FHE rollups offer a promising alternative that could potentially streamline the process, making it more efficient without sacrificing security [14].

Moreover, the computational power of FHE is increasing, with new hardware accelerators on the horizon expected to exponentially boost transaction processing speeds, aiming for thousands of transactions per second. These developments signify that FHE-enabled Smart Contracts are not just theoretical constructs but are rapidly becoming a practical reality [6].

FHE-enabled Smart Contracts represent a significant stride towards optimizing the blockchain for high-speed, confidential, and transparent transaction execution, promising a future where such contracts can be widely utilized across various industries for secure and efficient digital transactions.

Data Privacy

Fully Homomorphic Encryption (FHE) has emerged as a transformative solution for data privacy in Smart Contracts. Unlike traditional Smart Contract platforms that may post entries in plaintext or utilize non-FHE encryption methods, FHE preserves the confidentiality of data even when it's processed. This is crucial because blockchain platforms are inherently public and often rely on cloud platforms that are not fully trusted. With FHE, all computations can occur on encrypted data, which means the contractual terms, events, and actions remain private, and protected from potential exposure or breaches [15], [16].

FHE's ability to process data while remaining encrypted provides end-to-end security for remote computing services. This ensures that sensitive information is never revealed to any third party, not even those processing the data. Furthermore, FHE is resistant to decryption attempts, including those from future quantum computers, making it a robust option for securing Smart Contracts against advanced cyber threats [15].

However, while FHE offers compelling data privacy benefits, it is not without its challenges. The computational intensity required for FHE has historically been a barrier to its practical application. It can require a significantly larger amount of computing power compared to operations on plaintext data. Despite this, ongoing research and development are continuously improving FHE's efficiency, bringing it closer to practical, scalable use for ensuring privacy in blockchain applications [16], [17] .

The integration of FHE into Smart Contracts thus offers a promising path toward reconciling the need for transparency and verifiability in blockchain transactions with the imperative for data privacy. As FHE technology continues to evolve, it has the potential to enable a wide range of privacy-sensitive applications on blockchain platforms, expanding their use into areas where confidentiality is paramount.

Cost Savings

Smart contracts are fundamentally reshaping the way businesses approach transactions, offering significant cost savings compared to traditional contracts. By automating contractual obligations, smart contracts eliminate the need for intermediaries such as lawyers, brokers, or notaries, which in turn reduces the associated costs like legal fees and administrative expenses. This automation ensures that the terms of the contract are executed swiftly and without the errors that can come from manual processing, contributing to overall cost efficiency.

The transparency and accuracy inherent in smart contracts, supported by blockchain technology, also play a crucial role in cost reduction. Since every transaction and action executed through a smart contract is recorded on the blockchain, it creates an immutable and auditable trail. This reduces the need for additional verification processes and the potential costs associated with disputes or litigation.

Additionally, smart contracts enable global accessibility and cross-border transactions without the complications of international legal systems or exchange rates, which can further save costs in terms of time and financial resources. The decentralized nature of blockchain means that smart contracts can be used internationally with ease, opening markets and reducing barriers to entry, which traditional contracts may not easily overcome.

The use of smart contracts is not just a theoretical advantage but is already being applied in various industries, from real estate to financial services, healthcare, and supply chain management, demonstrating tangible cost savings and increased efficiency in operations. As the technology continues to develop and more use cases emerge, the economic benefits of smart contracts are likely to expand even further, solidifying their position as a cost-effective alternative to traditional contracts [12], [18], [19], [20].

The Impact of Scalable Computing on Privacy-Enhancing Technologies

The evolution of privacy technologies, particularly in the realm of smart contracts, is crucial for ensuring the confidentiality and integrity of sensitive data. Cornami's groundbreaking innovation, the FracTLcore® Compute Fabric, stands at the forefront of this progress by addressing the substantial computational requirements of smart contract operations. This scalable computing solution not only facilitates real-time processing of encrypted data but also upholds the highest standards of security.

Cornami's computing architecture is meticulously designed to be scalable and versatile, catering to the diverse computational demands of various privacy-enhancing technologies. It enables the seamless execution of intricate algorithms associated with smart contracts and facilitates their integration with complementary technologies such as Zero Knowledge Proofs (ZKP) and Privacy-Preserving Machine Learning (PPML). This harmonious integration results in robust, multifaceted solutions that handle sensitive data with unparalleled efficiency.

By streamlining the computational workflow, Cornami's FracTLcore® Compute Fabric makes it feasible to perform complex calculations on encrypted data swiftly and securely, a capability of paramount importance for organizations dealing with smart contracts. Consequently, the smart contract ecosystem stands to gain from the dual benefits of high-performance computing and stringent data privacy.

With Cornami's technology, organizations can tap into new possibilities for securely managing and analyzing vast datasets. This not only fosters trust among stakeholders but also enhances the capabilities of data-driven decision-making processes. Cornami's FracTLcore® Compute Fabric represents a significant advancement in

the practical implementation of compute-intensive privacy technologies, laying the groundwork for more sophisticated and secure smart contract systems.

Conclusion

We've explored the crucial role of Fully Homomorphic Encryption (FHE) within the smart contracts sector, particularly in safeguarding proprietary information and sensitive data. FHE implementation empowers organizations to securely analyze and exchange encrypted data without the necessity of decryption. This methodology shields critical information against cyber threats while ensuring compliance with regulatory frameworks, such as those governing personal data protection.

In the realm of smart contracts, security considerations are paramount, given the personal nature of the involved data. FHE technology facilitates secure analysis of contract outcomes and enables seamless information exchange between parties, fostering collaborative endeavors while preserving data confidentiality.

The incorporation of FHE into smart contract data frameworks yields manifold advantages. Improved security and privacy not only align with legal requirements but also foster collaborative research efforts and enhance management of contract-based transactions. Although computational demands pose a challenge, advancements in specialized hardware accelerators and algorithm optimization are rendering FHE more accessible and practical for smart contract applications.

The potential impact of FHE on smart contracts, particularly when complemented by scalable solutions such as those offered by Cornami, is substantial. Cornami's scalable computing architecture is adept at addressing FHE's computational complexities, facilitating swift processing of encrypted data and broader technology adoption.

By harnessing the capabilities of FHE alongside Cornami's technological innovations, the smart contracts sector stands on the cusp of a transformative era. In this era, data privacy, security, and collaborative contract innovation converge, propelling the industry toward a secure, efficient, and cooperative future.

SOURCES:

[1] Kosba, A., et al. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts." In 2016 IEEE Symposium on Security and Privacy (SP). https://ieeexplore.ieee.org/document/7546538

[2] Zyskind, G., Nathan, O., and Pentland, A. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." In 2015 IEEE Security and Privacy Workshops. https://www.scirp.org/reference/ReferencesPapers?ReferenceID=2409397

[3] Finck, M. "Blockchain Regulation and Governance in Europe." Cambridge University Press, 2018. https://assets.cambridge.org/97811084/74757/frontmatter/9781108474757_frontmatter.pdf

[4] Adams, J. (2023) "What Are the Blockchain Scalability Issues and How Can They Be Solved?" https://www.doubloin.com/learn/blockchain-scalability-issues

[5] Chainlink (2023) " Blockchain Scalability: Execution, Storage, and Consensus https://chain.link/education-hub/blockchain-scalability

[6] Hindi, R. (2023) “Private Smart Contracts Using Homomorphic Encryption” https://www.zama.ai/post/private-smart-contracts-using-homomorphic-encryption

[7] Say, N. (2024) “Fhenix: The Fully Homomorphic Encryption (FHE) Powered L2 for Encrypted Web3”
https://blockonomi.com/fhenix/

[8] Dahl, M. Danjou, C. Demmler, D. Frederiksen, F. Ivanov, P. Smart, N. Thibault, L. (2023) “fhEVM: Confidential EVM Smart Contracts using Fully Homomorphic Encryption∗”
https://github.com/zama-ai/fhevm/blob/main/fhevm-whitepaper.pdf

[9] Smart, N. (2022) “Fully Homomorphic Encryption and Post-Quantum Cryptography”
https://www.zama.ai/post/fully-homomorphic-encryption-and-post-quantum-cryptography

[10] Creeger, M. (2022) "The Rise of Fully Homomorphic Encryption."
https://queue.acm.org/detail.cfm?id=3561800

[11] Liu, B. (2023) “Fully homomorphic encryption rollups are one step closer to reality”
https://blockworks.co/news/fhenix-whitepaper-fhe-rollups

[12] Irei, A. (2023) “Smart contract benefits and best practices for security”
https://www.techtarget.com/searchsecurity/tip/Smart-contract-benefits-and-best-practices-for-security

[13] financegov (2023) “How do Smart Contracts ensure accuracy and reduce errors?”
https://finance.gov.capital/how-do-smart-contracts-ensure-accuracy-and-reduce-errors/

[14] Fhenix (2023) “FHE-Rollups: Scaling Confidential Smart Contracts on Ethereum and Beyond – whitepaper”
https://www.fhenix.io/fhe-rollups-scaling-confidential-smart-contracts-on-ethereum-and-beyond-whitepaper/

[15] Pallier, P. (2023) “5 ways in which FHE can solve blockchain’s privacy problems”
https://www.helpnetsecurity.com/2023/09/04/fully-homomorphic-encryption-fhe/

[16] Partida, D. (2021) “What Is Fully Homomorphic Encryption (FHE)?”
https://www.cioinsight.com/news-trends/fully-homomorphic-encryption/

[17] Tech Beacon Security Researcher, N4nk3r ph3193 (2021) “The state of FHE: Don't believe the hype—but it is hopeful”
https://techbeacon.com/security/state-fhe-dont-believe-hype-it-hopeful
[18] Howell, J. (2023) “10 Advantages of Using Smart Contracts”
https://101blockchains.com/advantages-of-smart-contracts/

[19] CFI (Corporate Finance Institute) “Smart Contracts: Computer protocols that digitally facilitate the verification, control, or execution of an agreement”
https://corporatefinanceinstitute.com/resources/valuation/smart-contracts/

[20] Monah, L. (2023) “What Are Smart Contracts – A Beginner’s Guide”
https://robots.net/fintech/what-are-smart-contracts-a-beginners-guide/