Privacy: A Critical Layer in Modern Blockchain Systems

INCOSANK RESEARCH CIRCLE

x: @eddy_phos, @kamarXBT, @SirNicco, @bigBash25

November 28, 2025

Abstract

Blockchain technology has evolved from a transparent ledger system into a global platform for decentralized finance, digital identity, enterprise coordination, and large scale data exchange. While transparency was originally considered a strength, it has become a significant structural limitation as adoption expands into regulated industries, high value financial markets and privacy sensitive applications. The open visibility of transactions, addresses, account histories, and smart contract interactions has created a new surface for surveillance, competitive intelligence extraction, user profiling, and institutional risk.

This research paper examines the shift toward privacy as a critical capability for next generation blockchain networks. It highlights how emerging regulatory frameworks, enterprise requirements, user protection concerns and advanced threats in decentralized finance have accelerated demand for confidentiality layers. It further outlines the technologies that are shaping the privacy landscape and provides a structured view of why privacy is becoming the most important pillar for mainstream blockchain adoption.

Keywords: Blockchain Privacy, Zero-Knowledge Proofs, Transparency Paradox, Fully homomorphic encryption, Privacy-Preserving Technologies, Trusted execution environment.

1. Introduction

Blockchain began as a transparent digital ledger designed to remove intermediaries and enable open verification of financial activity. The introduction of Bitcoin demonstrated that a decentralized network can coordinate global value without requiring any central authority [1]. Ethereum expanded the concept by enabling programmable transactions that support decentralized applications and complex business logic [2]. Subsequent generations of blockchain technology improved throughput, modularity, energy efficiency and interoperability, but retained transparency as a core architectural feature [3].

As the ecosystem matured, new participants entered the space including institutional investors, public companies, financial institutions, creators, governments and consumer focused companies [4]. These participants bring expectations regarding information security, data protection and compliance. Their involvement exposes the fundamental tension between transparency and privacy, creating the need for new architectural approaches [5].

1.1 The Transparency Paradox

Transparency helps networks achieve trustless verification, but it also exposes every transaction, balance, contract interaction and account history to anyone with internet access [6]. This universal visibility has allowed chain analysis companies and advanced machine learning systems to map user relationships, identify behavioral patterns, correlate wallet ownership and trace funds across decentralized ecosystems [7].

The paradox is that the more successful blockchain becomes, the more dangerous transparency becomes. What was originally a feature for open communities has become a challenge to enterprise adoption, consumer protection, competitive security, regulatory compliance and national level data governance [8].

1.2 Problem Statement

Blockchains reveal too much information to too many parties. Every action recorded on a public ledger becomes permanent, trackable and linkable [9]. This creates exposure to surveillance, financial exploitation, reputation harm, regulatory breaches, market manipulation and loss of competitive advantage. Without strong privacy guarantees, many high value use cases remain inaccessible, including private commerce, institutional trading, confidential identity systems, enterprise coordination and sensitive data markets [10].

1.3 Objectives of the Study

This research paper aims to achieve four primary objectives. First, to explain the historical evolution of blockchain transparency and the reasons it has become a structural weakness [1,2]. Second, to identify the major drivers behind the global demand for blockchain privacy [5,6]. Third, to describe the technical landscape of modern privacy solutions and how they are applied in practice [4,7]. Fourth, to demonstrate why privacy is emerging as a foundational requirement for the next era of blockchain systems [3,8].

1.4 Importance of Blockchain Privacy Today

Privacy is becoming a competitive requirement for companies that interact with digital assets, decentralized finance platforms, smart contract applications and tokenized real world assets [5,9]. It is no longer a secondary feature but a foundational capability that influences adoption, regulatory alignment, customer trust and institutional participation.

Privacy enables regulatory compliant data management by ensuring that sensitive information is selectively disclosed only to authorized parties. This is especially important in jurisdictions with strict data protection laws that mandate confidentiality of personal and financial information [5]. Organizations that cannot guarantee privacy expose themselves to legal liability, reputational damage and operational risk.

Privacy also protects user and customer information. Transparent ledgers allow anyone to observe transaction histories, spending patterns, wealth levels, commercial relationships and network activity. For both individuals and enterprises, this level of exposure creates avenues for exploitation ranging from targeted financial attacks to competitive intelligence gathering [9]. By embedding privacy directly into blockchain infrastructure, companies can shield both internal operations and customer interactions from global visibility.

Furthermore, privacy enables sensitive operations to be executed securely without compromising strategic, contractual or proprietary information. Business workflows involving pricing models, supply chain processes, identity attributes, credentials, customer data or treasury movements cannot be performed safely on transparent networks. Privacy preserving execution allows enterprises to move critical functions on chain without exposing themselves to risk [9].

Overall, privacy transforms blockchain systems from open data environments into secure computation platforms suitable for mainstream adoption. It aligns decentralized technologies with the real world requirements of businesses, regulators and users, enabling blockchain to evolve beyond experimentation and into critical market infrastructure.

2. The Evolution of Blockchain and Rise of Privacy Concerns

2.1 First-Generation Blockchains: Bitcoin and Full Transparency

Bitcoin introduced the idea of global value transfer without central control. Its architecture prioritizes transparency, where every transaction is visible to everyone [1]. This model supports integrity and open verification, but it also exposes all

activity to analysis. Over time researchers demonstrated that seemingly anonymous addresses could be linked to real world identities through transaction patterns, clustering methods and external data correlations [2,6].

2.2 Second-Generation Blockchains: Ethereum and Programmability

Ethereum expanded the capabilities of blockchain by enabling programmable smart contracts [2]. This unleashed a wave of innovation across decentralized finance, gaming, digital identity and tokenization. However the transparent architecture of Ethereum made every contract call, parameter value, balance change and interaction visible to public observers [3]. As a result, advanced forms of market surveillance, competitive intelligence extraction and automated exploitation became common across decentralized ecosystems [7].

2.3 Third-Generation Blockchains: Scalability and Interoperability

The next evolution in blockchain design focused on scaling transactions, separating execution from data availability and improving cross chain communication [3]. While these innovations increased throughput and flexibility, they did not fundamentally address privacy challenges. In fact, greater data availability increased the visibility of sensitive information across multiple layers [8].

2.4 How Transparency Became a Structural Weakness

The open nature of blockchain data allowed powerful analytics companies and artificial intelligence systems to create complete maps of user behavior [6,7]. What was once perceived as harmless transactional metadata evolved into a rich dataset capable of revealing intimate details about individuals and organizations. Over time, transparency transformed from a mechanism for trustless verification into an unintended source of surveillance and competitive exploitation.

Every action recorded on a transparent ledger contributes to an expanding behavioral footprint.

2.5 Data Leakage Through Wallets and On-Chain Activity

Wallet addresses are persistent identifiers that reveal long term user behavior. Once a single address is linked to a person or organization, every past and future action can be monitored [6]. This includes donations, purchases, savings, financial relationships, contract interactions and even the timing of investment decisions [9].

2.6 Emergence of Privacy-Preserving Technologies

In response to these risks, new classes of privacy solutions have emerged [4]. Zero knowledge proofs allow users to prove correctness without revealing underlying data. Trusted execution environments protect computations within secure hardware. Fully homomorphic encryption allows encrypted data to be processed without decryption. Multi party computation distributes trust across multiple participants. Confidential smart contracts enable logic execution without exposing inputs, outputs or state [7].

2.7 Summary of Evolutionary Trends

The blockchain ecosystem has moved from transparency as a fundamental design choice to privacy as a required capability for serious adoption. Early systems prioritized open verification. Modern systems prioritize selective disclosure, user protection and compliance [3,8]. Future systems will integrate privacy as a default capability rather than an optional add on [5,10].

3. Drivers Behind the Need for Privacy

3.1 Regulatory Pressure

Governments across the world are enforcing data protection laws that require confidentiality of personal and sensitive information [5]. Regulations such as the General Data Protection Regulation in Europe impose strict penalties for improper exposure of user data. Public blockchains that reveal identifiable information create risks for both operators and companies that rely on them. Privacy preserving infrastructure is essential for compliance with global data protection standards [5,6].

3.2 Enterprise Adoption Requirements

Enterprises need confidentiality across a wide range of activities, including internal operations, supply-chain coordination, partner negotiations, pricing strategies, treasury management, and automated business workflows [7]. No organization can safely conduct these processes on a fully transparent public ledger. Without strong privacy guarantees, enterprise use of blockchain technology will remain confined to non-sensitive or experimental functions [4,9].

3.3 User Data Exposure and Surveillance

Every blockchain transaction reveals behavioral and financial metadata about users, including spending patterns, counter-parties, and long-term activity trails [6]. Advanced chain-analysis techniques combine on-chain data with off-chain identifiers to produce detailed behavioral profiles [7]. This level of surveillance threatens

consumer safety, erodes autonomy, and contradicts modern expectations of digital privacy [9].

3.4 DeFi Related Risks

Decentralized finance (DeFi) exposes users to a range of advanced adversarial behaviors enabled by full transaction transparency. In public mempools, every pending transaction including its sender address, asset type, size, intent, and slippage settings is visible to observers before confirmation. This visibility creates a rich environment for malicious actors and automated bots to extract value at the expense of regular users [11,12].

Transaction ordering attacks occur when validators or bots manipulate the position of transactions in a block to gain profit. By simply reordering transactions, an attacker can influence market conditions, liquidations, or protocol outcomes to their advantage. Studies have shown that transaction reordering is one of the most exploited weaknesses in transparent blockchain environments [13].

Front running takes place when adversaries detect a profitable user transaction in the mempool and submit their own transaction with higher fees to be executed first. This allows attackers to profit from predictable price movements, often leaving the user with a worse execution price or a failed transaction. Multiple empirical analyses have documented widespread front running in decentralized exchanges, especially those built on automated market makers [14].

Sandwich attacks combine front running and back running. Attackers place one transaction before and one after the victims trade to artificially move the price, capture the spread, and extract value directly from the user. This attack is now one of the most common forms of value extraction in automated market maker systems, where trade visibility directly reveals price impact and slippage tolerance [15].

Maximal Extractable Value (MEV) describes the total value validators or third party actors can extract by reordering, inserting, or censoring transactions within a block [16]. MEV has evolved into a structural phenomenon within DeFi, with entire ecosystems of searchers, relays, and block builders competitively exploiting profitable opportunities. Research shows that MEV contributes to instability, user harm, and systemic inefficiencies across decentralized markets [17].

Because all of these attacks rely on prior visibility of transaction intent, DeFi users are uniquely vulnerable. Every trade, loan, liquidation, or collateral adjustment becomes a public signal that adversaries can detect, simulate, and exploit in

milliseconds. This places users at a consistent informational disadvantage and undermines the fairness, transparency, and reliability of decentralized markets [18].

Privacy layers fundamentally change this dynamic by removing transaction intent from the public mempool. When orders, positions, and parameters are hidden until finalization, adversaries lose the informational asymmetry required to manipulate execution. As a result, users gain significantly improved protection, more predictable outcomes, and a market structure that better reflects genuine supply and demand rather than adversarial exploitation. Privacy is therefore a prerequisite for building safe, equitable, and economically sustainable DeFi systems [19].

4. Privacy Technologies in Blockchain

The risks associated with transparent blockchain systems especially in decentralized finance and sensitive enterprise applications highlight the critical need for privacy preserving mechanisms. To address these vulnerabilities, researchers and developers have designed a range of technologies that allow data and transactions to remain confidential while still enabling secure verification and computation. Privacy technologies in blockchain ensure that sensitive information including user identities, transaction parameters and contract states can be protected from external observers, malicious actors and even partially trusted participants. These solutions do not compromise the core benefits of decentralization and immutability; rather, they complement them by adding confidentiality as a fundamental layer of security. This section explores the major privacy enhancing technologies currently employed in blockchain systems including zero knowledge proofs, fully homomorphic encryption, trusted execution environments, secure multiparty computation and confidential smart contracts. For each technology we examine its underlying principles, security guarantees and practical applications in the blockchain ecosystem [20] [21] [22] [23].

4.1 Zero Knowledge Proof

Zero knowledge proofs (ZKPs) are cryptographic protocols that allow a prover to convince a verifier that a statement is true without revealing any of the underlying information. In essence, the verifier learns only that the statement holds, and nothing else about the data or computation involved [20].

ZKPs rely on two key security properties. **Completeness** ensures that if the statement is true and the prover is honest, the verifier will always be convinced of its validity. **Soundness** guarantees that if the statement is false, no dishonest prover can convince the verifier except with negligible probability [20].

ZKPs can be either interactive, requiring multiple rounds of communication, or non-interactive, where a single proof is generated and independently verified by others. In blockchain applications, non-interactive proofs are preferred because they allow a single proof to be broadcast across the network without repeated back-and-forth communication, reducing network overhead while maintaining strong security guarantees [21].

In practice, zero knowledge proofs are widely used to preserve privacy in blockchain systems. They enable confidential transactions where the validity of transfers can be verified without exposing sender or receiver addresses, transaction amounts, or other sensitive details. Many privacy-focused blockchains and layer two solutions for public blockchains rely on ZKPs to achieve both confidentiality and correctness while maintaining decentralization and verifiability [22], [23].

By providing a mechanism to prove truth without revealing information, zero knowledge proofs form a foundational building block for blockchain privacy, ensuring that sensitive data can remain confidential even in fully transparent environments.

4.2 Fully Homomorphic Encryption

Fully Homomorphic Encryption is a cryptographic technique that enables arbitrary computations to be performed directly on encrypted data while preserving the confidentiality of the underlying information. Under FHE, data encrypted by a user remains encrypted throughout computation, and only the data owner can decrypt the final output. This property ensures that neither validators nor external observers ever gain access to sensitive information during processing [24].

In the context of blockchain systems, FHE represents a major advancement in privacy preserving computation. It allows decentralized applications and smart contracts to operate on private inputs such as balances, identity attributes, business logic, or proprietary data without exposing these values on the public ledger. This guarantees that confidentiality is maintained while still enabling correct and verifiable execution of program logic [25]. Privacy preservation no longer requires trust in intermediaries or restrictive off chain computation. Instead, privacy is guaranteed through strong cryptographic foundations.

Recent innovations have significantly increased the practicality of FHE for blockchain use. Breakthroughs in bootstrapping optimizations, lattice based schemes, and modern implementation frameworks have reduced computational overhead and improved performance, making FHE increasingly viable for real world applications.

Research from Inco highlights that new generation FHE architectures are specifically optimized for decentralized environments, enabling encrypted smart contract execution and privacy preserving on chain analytics with far lower latency than earlier generations of FHE systems [26].

These improvements are enabling new categories of blockchain applications. Financial systems can support confidential lending, private asset management, and encrypted order books. Enterprises can run collaborative analytics on encrypted datasets without exposing business sensitive information. Governments and institutions can deploy private voting, secure record management, and encrypted identity verification where data remains protected even during computation. Because all operations occur over encrypted values, trust shifts from institutional assurances to mathematically provable security guarantees [27].

While FHE still introduces performance overhead compared to plain text computation, ongoing research continues to close this gap. As a result, FHE is becoming increasingly suited for privacy critical applications where correctness, auditability, and confidentiality must coexist. These include confidential DeFi protocols, secure multi organization analytics, regulatory compliant data handling, and advanced privacy preserving autonomous agents [28].

Overall, Fully Homomorphic Encryption stands as one of the most transformative privacy technologies available to blockchain ecosystems. Its ability to compute on encrypted data without exposure provides a robust foundation for secure, private, and verifiable decentralized systems, and its rapid technical advancement positions it as a cornerstone for the next generation of privacy first blockchain infrastructure.

4.3 Trusted Execution Environments

Trusted Execution Environments represent a hardware based approach to achieving confidentiality in blockchain systems. A TEE is a secure and isolated region within a processor that protects sensitive computations from the rest of the operating system. Data are supplied to the enclave in encrypted form, decrypted and processed securely inside the trusted environment, and then re-encrypted before being returned to external components. This architecture ensures that even if the surrounding software stack is compromised, the data and computation occurring within the enclave remain protected from unauthorized access [29].

In blockchain settings, TEEs have become an important tool for enabling confidential computation without revealing private inputs to the network. They allow smart contracts, decentralized applications, or off chain logic to operate on sensitive

information while maintaining execution integrity. By combining blockchain properties such as immutability and consensus verification with TEE based confidentiality, developers can build privacy preserving systems that do not require exposing user data or proprietary logic to validators or external observers [30].

One of the most attractive characteristics of TEEs is their computational efficiency. Unlike fully homomorphic encryption, which performs cryptographic computation entirely on encrypted data, TEE processing occurs on plaintext within a secure enclave. This allows near native execution speeds with significantly reduced overhead. For many real world applications, TEEs therefore provide a practical balance between privacy, performance, and deployment feasibility. According to recent analysis, TEEs remain the preferred option when applications require high throughput, low latency, and real time responsiveness, and when trust in hardware vendors is operationally acceptable [31][32].

Overall, Trusted Execution Environments offer a powerful and practical foundation for privacy preserving blockchain systems. They enable confidential smart contract execution, secure off chain computation, private data processing, and protected workflow automation. When properly implemented and combined with robust attestation, side channel mitigation, and hardware verification, TEEs provide a compelling mechanism for enhancing privacy while preserving the decentralized trust model of blockchain networks.

4,4 Secure Multi Party Computation

Secure multi-party computation (MPC) is a powerful cryptographic framework that allows multiple parties to jointly compute a function over their private inputs without ever revealing those inputs to one another [33]. Each participant contributes encrypted or secret shared data, and the protocol ensures that the only information disclosed at the end of the computation is the final output. This property makes secure multiparty computation one of the strongest guarantees for collaborative privacy protection, particularly in environments where participants must cooperate without compromising confidentiality.

In blockchain ecosystems secure multi-party computation enables decentralized networks to perform complex joint operations while preserving the privacy of individual contributors. It has been deployed in scenarios such as private transaction validation, private auctions, collaborative analytics, and cross-organization data sharing [34].

A key strength of secure multiparty computation is its ability to operate in trust-minimized environments. Because the protocol ensures that no single party has access to the complete data, participants can safely collaborate even when the level of mutual trust is limited. This makes secure multiparty computation particularly suitable for multi-stakeholder blockchain applications such as consortium networks, decentralized governance, multi-party data pooling, and cooperative machine learning.

While secure multiparty computation traditionally introduced communication and computational overhead due to the need for coordination among participants, recent advancements have significantly improved efficiency. Optimizations such as preprocessing protocols, lightweight secret sharing schemes, and improved circuit constructions have reduced latency and enabled more scalable deployments [35].

Within the broader privacy landscape secure multiparty computation stands out as a highly promising approach for enabling confidential collaboration on decentralized networks. Its ability to provide strong, mathematically grounded privacy guarantees while supporting collective decision-making positions it as a critical technology for the next generation of secure and trustworthy blockchain applications.

5. Case Studies of Privacy-Preserving Protocols

Blockchain privacy solutions have evolved from theoretical concepts into fully implemented systems with substantial adoption in decentralized finance and enterprise applications. As the total value locked in DeFi platforms continues to grow, privacy-focused blockchains and infrastructure projects have gained prominence across the cryptocurrency ecosystem. These case studies highlight diverse approaches to achieving transaction confidentiality, emphasizing privacy guarantees, scalability, regulatory compliance, and usability. The following examples, Monero’s ring signatures and stealth addresses, Zcash’s zk-SNARK shielded transactions, Tornado Cash’s mixing protocols, and Inco Network’s confidentiality layer, demonstrate the breadth of technical strategies employed to preserve privacy while maintaining verifiability.

5.1 Monero – Ring Signatures and Stealth Addresses

Monero, launched in 2014, is a privacy-focused cryptocurrency designed to overcome the traceability limitations of transparent blockchains. Built on the CryptoNote protocol, it employs ring signatures, stealth addresses, and Ring Confidential Transactions (RingCT) to ensure transaction confidentiality while

maintaining verifiability. Ring signatures mix a sender's signature with multiple potential signers, obscuring the true origin of a transaction, while stealth addresses generate unique one-time recipient addresses for each transfer, preventing external observers from linking multiple payments to the same destination. RingCT conceals transaction amounts while allowing cryptographic verification of inputs and outputs through range proofs, ensuring the integrity and balance of the ledger [36][37][38].

Monero's privacy-preserving architecture has enabled a wide range of applications, including secure peer-to-peer payments, anonymous charitable donations, and decentralized infrastructure for IoT and digital asset management. Its technology supports atomic swaps, enabling private cross-chain asset exchanges, and can be integrated into decentralized finance platforms to facilitate confidential lending, payments, and trading. The combination of these features allows users and enterprises to maintain privacy without sacrificing trustless verification or security.

As of early 2025, Monero had a market capitalization approaching $7.5 billion, with increasing adoption fueled by growing concerns over digital privacy, identity protection, and regulatory surveillance mechanisms such as central bank digital currencies. Despite facing regulatory challenges and delistings from certain exchanges, Monero continues to advance through protocol upgrades such as Triptych, which expands anonymity sets and improves network scalability without significantly increasing transaction size. These continuous improvements, along with support for evolving use cases, reinforce Monero's position as a foundational privacy-first cryptocurrency and a reference standard for secure, untraceable digital transactions [39][40].

5.2 Zcash – zk-SNARK Shielded Payments

Zcash, introduced in 2016, is a pioneering cryptocurrency that provides optional privacy for blockchain transactions through zero-knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs). Unlike Monero, which enforces privacy by default, Zcash allows users to choose between transparent transactions similar to Bitcoin and shielded transactions that hide transactional metadata, supporting selective privacy while accommodating regulatory and operational requirements.

The protocol's zero-knowledge proof system enables users to prove the validity of a transaction without revealing sender and recipient identities or transaction amounts. Transparent addresses, referred to as t-addresses, function like conventional blockchain accounts with full public visibility. Shielded addresses, or unified addresses, hold funds within a cryptographically verified shielded pool, ensuring the confidentiality of transaction metadata. This dual-address structure allows users to

perform fully private transactions between shielded accounts or hybrid transfers that involve both transparent and shielded addresses. While the shielded pool significantly enhances privacy, metadata leakage can occur during movements between transparent and shielded accounts if privacy practices are not carefully maintained.

Zcash's technical evolution includes major upgrades such as Sapling and Orchard. Sapling introduced more efficient zk-SNARK constructions, optimized proof generation, and reduced transaction verification times. Orchard further improved protocol efficiency, strengthened security assumptions, and removed the need for trusted setup ceremonies using Halo 2 zero-knowledge proofs, mitigating trust dependencies during deployment. These innovations have made Zcash more practical for real-world applications, including private payments, confidential donations, and enterprise financial operations where selective privacy is essential.

Zcash's privacy technology has found adoption in both retail and institutional contexts, with a shielded pool currently holding over 4.5 million ZEC, representing roughly 25–30% of circulating supply. As of November 2025, ZEC trades above $600 with a market capitalization near $9–10 billion, placing it among the top 20 cryptocurrencies. Increased adoption of shielded transactions and default wallet integrations highlight Zcash's transition from optional privacy to mainstream usage. The network's technical robustness, combined with optional privacy and compliance flexibility, positions Zcash as a leading example of zero-knowledge cryptography applied at scale in blockchain systems [41][42][43][44].

5.3 Tornado Cash – Mixing Protocol

Tornado Cash, launched on Ethereum in 2019, is a decentralized protocol that anonymizes token transfers by breaking the link between deposit and withdrawal addresses. Users deposit funds into smart contract pools, receiving cryptographic commitments. Withdrawals require zero-knowledge proofs to verify entitlement without revealing the corresponding deposit, ensuring unlinkability [45].

The protocol uses zk-SNARK constructions and Merkle trees to maintain anonymity. Each deposit generates a hashed secret recorded in the tree, while withdrawals reveal a nullifier and a proof that the user deposited funds without exposing which transaction belongs to them. This approach allows trustless privacy without intermediaries [45][46].

Tornado Cash supports multiple fixed-amount pools to increase anonymity set size. Privacy is enhanced when pools are large and deposits and withdrawals are

temporally distributed. Proper use, such as delaying withdrawals and employing relayers, is essential to maintain privacy [46][47].

Despite its cryptographic design, Tornado Cash has faced regulatory scrutiny. In 2022, the U.S. Treasury sanctioned the protocol for alleged illicit use, highlighting the legal risks of decentralized privacy tools [48]. Nevertheless, it has processed billions of dollars in deposits and remains an important example of privacy-preserving infrastructure for Ethereum and DeFi applications [49][50].

5.4 Inco Network – Confidentiality Layer

Inco Network delivers a full-featured confidentiality layer for existing blockchains, providing a comprehensive privacy solution that enables secure smart contracts, confidential data storage, and private computation without altering the underlying blockchain infrastructure. Rather than launching a separate chain, Inco integrates with existing networks, analogous to how SSL/TLS adds encryption to the Internet, allowing encrypted states, verifiable computations, and controlled data disclosure [51][52]. This modular design positions Inco as a versatile privacy infrastructure capable of supporting both public and enterprise blockchain applications.

Inco offers two complementary modes of operation, Inco Lightning and Inco Atlas, designed to balance privacy, performance, and trust assumptions. Inco Lightning leverages Trusted Execution Environments to deliver verifiable confidential computation at near-native speeds, making it suitable for latency-sensitive applications such as real-time games, high-frequency DeFi operations, private payments, and other scenarios where performance is critical and trust in enclave security is acceptable [52][51]. Inco Atlas employs advanced cryptographic techniques, including Fully Homomorphic Encryption and Multi-Party Computation, to provide maximal privacy guarantees even in adversarial environments. Inco Atlas is ideal for high-security applications such as confidential asset management, private voting, payroll, or sensitive enterprise operations where no single party including infrastructure operators can access plain text data [53][54].

The dual-mode architecture enables developers and organizations to select the appropriate level of confidentiality based on specific security, performance, and trust requirements, offering a flexible yet robust privacy solution across a wide range of use cases.

A key innovation of Inco’s technology is the Confidential ERC-20 Framework, developed in collaboration with Circle Research, which adapts the standard ERC-20 token specification to support on-chain confidentiality. This framework conceals user

balances and transaction amounts while preserving the programmability, interoperability, and composability of ERC-20 assets [55]. Confidential ERC-20 tokens facilitate privacy in stablecoins, utility tokens, and other digital assets, enabling confidential payroll, private remittances, B2B payments, and enterprise transactions without exposing financial data publicly. Programmable access and optional disclosure features ensure compliance requirements are met while maintaining default user privacy [55][52].

By combining modular integration, dual confidentiality modes, and confidential token standards, Inco Network establishes a comprehensive privacy layer for blockchain applications, representing a leading solution in the evolving privacy-focused ecosystem.

6. Why Privacy Is Now a Critical Layer

Privacy has transitioned from an optional feature to a foundational component of blockchain architecture, enabling scalability, regulatory compliance, and user trust amid the rapid expansion of the cryptocurrency ecosystem. As global adoption grows, transparency—once a defining strength—exposes systemic risks including large-scale hacks, front-running by maximal extractable value (MEV) actors, and regulatory challenges. Privacy-by-design is increasingly mandated by frameworks such as the European Data Protection Board 2025 guidelines, and enterprise surveys indicate that most organizations prioritize zero-knowledge proofs and fully homomorphic encryption to meet privacy requirements [56][57]. Privacy layers mitigate MEV, enable trustless identity systems, and unlock economic potential in tokenized assets, with projections estimating a $7 trillion market for secure, compliant blockchain ecosystems [58].

Blockchain transparency, while improving accountability, limits adoption by exposing sensitive financial and operational data. Analyses by the World Bank show that full visibility of on-chain activity can erode trust in financial flows, prompting enterprises to avoid blockchain adoption [59]. Public ledgers allow third parties, including government agencies, to reconstruct user identities and target high-value accounts, deterring significant capital inflows. Regulatory inconsistencies across jurisdictions further exacerbate challenges, as frameworks such as the EU’s MiCA and the US GENIUS Act impose compliance obligations difficult to reconcile with fully transparent blockchains. Privacy layers are therefore essential for user protection, enterprise integration, and mainstream adoption.

Privacy is also a fundamental user right, providing autonomy against pervasive surveillance. Privacy-first blockchain architectures support national security, enable anti-money laundering and know-your-customer compliance, and preserve individual sovereignty. As Vitalik Buterin emphasized, “whoever has the information has the power,” highlighting the protective role of privacy in preventing information asymmetry and exploitation [56]. EDPB guidance reinforces this by emphasizing consent, erasure rights, and controlled data processing, making privacy a key enabler of trust and innovation [57].

From a security perspective, privacy is non-negotiable. Transparent blockchains, despite their accountability benefits, leave high-value transactions vulnerable to tracking, front-running, and other exploitation. Sensitive operations such as military procurement or healthcare data management are particularly exposed, underscoring the need for privacy-preserving architectures. Confidential blockchain designs safeguard critical activities while enabling verifiable, compliant interactions, mitigating risks from malicious actors and sophisticated analytics [58].

Enterprises adopt privacy layers to secure operational data, intellectual property, and customer information. Legal frameworks such as GDPR and CCPA require organizations to protect personal information and maintain user control over data. Blockchain privacy ensures compliance, preserves competitive advantage, and facilitates adoption across sectors by enabling secure financial transactions, confidential reporting, and operational autonomy [59].

Privacy is integral to trustless identity systems, allowing users to prove credentials without revealing sensitive information. Advanced cryptographic techniques including zero-knowledge proofs, fully homomorphic encryption, trusted execution environments, and multi-party computation enable decentralized identity verification while maintaining data integrity and authenticity [56][57].

Privacy also strengthens blockchain-based reputation systems by enabling verifiable feedback without fear of exposure. Anonymous participation encourages honest reporting, fosters trust, and ensures accurate representation of user behavior, supporting accountability in distributed ecosystems [58].

Moreover, privacy is essential for mitigating the impact of MEV exploitation. MEV actors exploit transaction ordering and mempool visibility to extract value, often causing losses in the billions and deterring institutional participation. Privacy layers obscure sensitive transaction data, reduce MEV risk, enhance fairness, and incentivize capital inflows, supporting broader ecosystem growth [59].

Economically, privacy layers catalyze blockchain adoption, innovation, and market expansion. They enable new use cases, support secure decentralized application development, and facilitate confidential management of tokenized assets. By integrating privacy into core architecture, blockchain platforms can achieve scalability, security, and regulatory alignment, paving the way for mainstream adoption and long-term sustainable growth [56][57][58][59].

7. Future Outlook

The momentum behind decentralized finance (DeFi) demonstrates the economic opportunity that privacy-enabled infrastructure can unlock. As of mid-2025, the combined total value locked (TVL) in DeFi protocols stands at approximately USD 123.6 billion [60]. This highlights the existing scale of blockchain finance, and integrating robust privacy layers could accelerate growth by unlocking markets constrained by confidentiality, compliance, and institutional risk aversion.

Privacy-preserving smart contracts and confidential tokens, such as Confidential ERC-20 assets, have the potential to attract new capital from individuals, enterprises, and institutions that previously avoided public chains due to exposure and regulatory risk [61]. With the continued tokenization of real-world assets (RWAs) and financial instruments, the tokenization infrastructure market is projected to grow at a compound annual growth rate (CAGR) of 28–32% between 2025 and 2030 [62]. If this trend holds, assets under management on-chain, including RWAs and DeFi, could reach multiple trillions of dollars within this decade.

Confidential tokens and privacy-first DeFi also enable new revenue streams beyond traditional public DeFi models, including private stablecoin yield products, compliant institutional asset management, privacy-preserving payroll and remittances, and enterprise treasury solutions [63]. These offerings target users with higher compliance and confidentiality requirements, potentially commanding premium fees and attracting institutional liquidity. Consequently, privacy-enabled services could generate tens of billions of dollars annually in revenue in the coming years.

As privacy layers become standard via modular blockchain architectures that separate execution, data, and privacy, adoption is likely to broaden from retail users to enterprise finance, institutional asset management, RWA tokenization, and cross-border finance [64]. This expansion could dramatically increase TVL over time, moving from hundreds of billions toward trillions of dollars. Tokenization of global real estate, fixed income, equities, and commodities under privacy-preserving frameworks could approach the scale of traditional global capital markets.

Privacy-enabled DeFi also reduces barriers for institutional participation, encouraging larger capital inflows, longer-term investments, and demand for compliance-ready infrastructure [65]. As a result, blockchain could evolve from a nascent alternative finance channel to core infrastructure for global finance, digital securities, cross-border payments, and asset management.

Embedding privacy as a foundational blockchain layer through confidential tokens, private smart contracts, privacy-preserving identity, and compliance tools can unlock a future of finance that blends decentralization, confidentiality, regulatory alignment, and institutional-grade liquidity. The potential market size is vast, revenue opportunities are diverse, and the chance to reshape global finance is significant [60] [65].

8. Conclusion

This research establishes that privacy is no longer an optional feature but a critical pillar of modern blockchain systems, underpinning security, regulatory compliance, and user trust. Advanced privacy-preserving technologies including zero-knowledge proofs, fully homomorphic encryption, trusted execution environments, and confidential tokens address the inherent risks of transparency, mitigate MEV exploits, and enable trustless identity and reputation systems.

We recommend that developers, enterprises, and policymakers embrace privacy-first blockchain architectures, integrating modular confidentiality layers and confidential token standards to drive innovation, scalability, and secure adoption.

The future impact of privacy layers is substantial. They will catalyze widespread institutional and retail adoption, unlock unprecedented financial and enterprise applications, expand total value locked in decentralized finance, and lay the foundation for the next generation of compliant, secure, and efficient global financial systems. By embedding privacy at the core, blockchain platforms can achieve sustainable growth, foster confidence across stakeholders, and realize the full transformative potential of decentralized finance.

References

1. Nakamoto S. Bitcoin A Peer to Peer Electronic Cash System. 2008.
2. Buterin V. Ethereum Whitepaper A Next Generation Smart Contract Platform. 2014.
3. Zheng Z, Xie S, Dai H, Chen X, Wang H. Blockchain Challenges and Opportunities A Survey. International Journal of Web and Grid Services. 2017.
4. Ben Sasson E, Chiesa A, Tromer E, Virza M. Succinct Non Interactive Zero Knowledge Arguments for NP. USENIX. 2013.
5. European Union. General Data Protection Regulation GDPR. 2018.
6. Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker G. A Fistful of Bitcoins Characterizing Payments Among Men with No Names. ACM IMC. 2013.
7. Chainalysis. Crypto Crime Report. Multiple editions.
8. Finck M. Blockchain and the General Data Protection Regulation. European Parliament Research Service. 2019.
9. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and Cryptocurrency Technologies. Princeton University Press. 2016.
10. Hyperledger Foundation. Enterprise Blockchain Requirements Overview. 2020.
11. Qin, K., Zhou, L., Kumar, A., & Gervais, A. (2021). *Attacking the DeFi ecosystem with flash loans for fun and profit*. IEEE Symposium on Security and Privacy.
12. Eskandari, S., Salehi, M., Gu, M., & Clark, J. (2020). *SoK: Transparent dishonesty front running attacks in blockchain*. ArXiv:1902.05164.
13. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Front running, transaction reordering, and consensus instability in decentralized exchanges. IEEE Symposium on Security and Privacy.
14. Torres, C. F., Steichen, M., & State, R. (2021). *Frontrunning in decentralized exchanges: A survey*. ACM Ledger Journal.

15. Qin, K., Zhou, L., & Gervais, A. (2021). *The dynamics of sandwich attacks in automated market maker protocols*. Crypto Valley Conference.

16. Ferreira, L., Fritsch, M., Kell, T., & Juels, A. (2023). *Maximal Extractable Value: Economic impacts and mitigation techniques*. ChainSecurity Research.

17. Flashbots Research. (2022). *The MEV Supply Chain: A deep dive into the economic structure of MEV*. Flashbots Publications.

18. Fraxman, M., & Bonneau, J. (2022). *DeFi transparency harms: Modeling user disadvantage under open mempools*. Financial Cryptography and Data Security.

19. Kiffer, L., Teixeira, R., & Juels, A. (2023). *Privacy for DeFi: Why hiding transaction intent is essential for fair markets*. Cornell University.

20. R. Lavin, X. Liu, H. Mohanty, L. Norman and G. Zaarour, "A Survey on the Applications of Zero Knowledge Proofs," *arXiv*, Aug. 2024. (arxiv.org)

21. E. Bünz, D. Bootle, and A. Boneh, "Zero Knowledge Proofs and Their Role in Scaling and Privacy for Blockchain," *Communications of the ACM*, 2023. (cacm.acm.org)

22. I. Muntean et al., "Blockchain and Homomorphic Encryption for Data Security and Statistical Privacy," *Electronics*, vol. 13, no. 15, 2024. (mdpi.com)

23. A. Solomon, R. Weber and G. Almashaqbeh, "smartFHE: Privacy Preserving Smart Contracts from Fully Homomorphic Encryption," *IACR ePrint Archive*, 2021. (eprint.iacr.org)

24. C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, Communications of the ACM, 2010.

25. Z. Brakerski and V. Vaikuntanathan, Efficient Fully Homomorphic Encryption from Standard Lattices, SIAM Journal on Computing, 2014.

26. Inco Research, A Complete Guide to Fully Homomorphic Encryption, Inco Blog, 2024.

27. S. Halevi and V. Shoup, Algorithms in Lattice Based Cryptography and FHE Performance Improvements, Journal of Cryptographic Engineering, 2021.

28. IEEE Digital Privacy Initiative, Homomorphic Encryption and Secure Computation, IEEE Digital Privacy Publications, 2023.

29. Intel Corporation, Intel Software Guard Extensions Architectural Overview, Intel Technical Report, 2020.

30. V. Costan and S. Devadas, Intel SGX Explained, MIT CSAIL Technical Report, 2016.

31. IEEE Secure Computing Forum, Hardware Enclaves and Confidential Computing in Distributed Systems, IEEE Publications, 2023.

32. Inco Research, Comparison of Trusted Execution Environments and Fully Homomorphic Encryption for Confidential Computation, Inco Blog, 2024.

33. Y. Lindell, “Secure Multiparty Computation (MPC),” Unbound Tech / Bar-Ilan University, 2020.

34. J. Ren, W. He, M. Kos, N. Johnson, A. Miller et al., “Using Secure Multiparty Computation to Protect Privacy on a Permissioned Blockchain,” Sensors, vol. 21, no. 4, 2021.

35. D. Escudero, “An Introduction to Secret-Sharing-Based Secure Multiparty Computation,” Cryptology ePrint Archive, Paper 2022/062, 2022.

36. Rivest, R. L., Shamir, A., & Tauman, Y. (2001). How to leak a secret. In *Advances in Cryptology—ASIACRYPT 2001* (pp. 552–565). Springer. https://doi.org/10.1007/3-540-45682-1_32

37. Noether, S. (2015). Ring signature confidential transactions for Monero. *IACR Cryptology ePrint Archive*. https://eprint.iacr.org/2015/1098.pdf

38. Schnorr, C. P. (1989). Efficient identification and signatures for smart cards. U.S. Patent.

39. Monero Market Data, CoinMarketCap. Retrieved 2025.

40. Monero Project Updates and Triptych Protocol Upgrade, Monero Research Lab. 2024.

41. BlockNews, “Zcash Shielded Supply Explodes Past 4.4 Million — 27% of All ZEC Now Completely Untraceable,” Oct. 13, 2025.

42. “Shielded Zcash Supply Reaches 5M All-Time High Despite Market Crash,” Coinspeaker / Yahoo Finance, Nov. 4, 2025.

43. “Zcash Breaks Into Top-20 Crypto List, Hits USD 600 for First Time Since 2018,” CoinDesk, Nov. 7, 2025.

44. Electric Coin Company, “NU5 Activates on Mainnet, Eliminating Trusted Setup and Launching a New Era for Zcash,” May 31, 2022.
45. Tornado Cash documentation, How does Tornado Cash work. (docs.tornado.cash)
46. Arkham, Tornado Cash: what is it and how does it work? 2025. (info.arkm.com)
47. Tornado Cash official site, Tornado Cash private transactions on Ethereum. (tornadoapp.cash)
48. Wikipedia contributors, Tornado Cash — History and legal status, 2025. (en.wikipedia.org)\
49. Decrypt, Ethereum mixer Tornado Cash processed almost $2 billion in deposits during the first half of 2024. (decrypt.co)
50. R. Cristodaro, B. Kramer, C. J. Tessone, Clustering deposit and withdrawal activity in Tornado Cash: A cross-chain analysis, 2025. (arxiv.org)
51. Inco Raises 5M in Strategic Round Led by a16z CSX to Accelerate Web3 Confidentiality, Inco press release, April 24 2025.
52. Inco Docs, “Introduction” and “Overview” — Inco Lightning and Atlas architecture documentation. https://docs.inco.org/introduction
53. Inco Website, “The Confidentiality Layer of Web3” overview page. https://www.inco.org/
54. Inco, “Inco Use Cases,” Inco Blog https://www.inco.org/blog/inco-use-cases
55. Circle Partners with Inco Network to Launch a More Private Version of ERC-20 Token Standard, CryptoNews, October 2024.
56. European Data Protection Board (EDPB), “Guidelines 02/2025 on processing of personal data through blockchain technologies”, April 2025.
57. General Data Protection Regulation (GDPR) + commentary and analysis on blockchain vs data-protection conflict; e.g. the literature review “A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems” by Belen-Saglam et al., 2022.
58. World Bank (and related analyses), illustrating how full visibility of on-chain data can erode trust and hinder institutional adoption; also general analyses of transparency vs privacy in blockchain contexts. For example, the article

"Beyond the blockchain hype: addressing legal and regulatory challenges" (2024) discusses privacy challenges of public blockchains.

59. Recent commentary from Forbes arguing that "privacy and regulation are key to blockchain's future" and describing the "transparency trap" for public blockchains.

60. CoinLaw, "Decentralized Finance Market Statistics 2025," CoinLaw.io. [Online]. Available: https://coinlaw.io/decentralized-finance-market-statistics/?utm_source=chatgpt.com

61. Inco Network, "Confidential ERC-20 Tokens and Privacy-Preserving DeFi," Inco.org. [Online]. Available: https://www.inco.org/blog/inco-use-cases

62. Macholevante, "Tokenization Infrastructure for DeFi 2025: Market Surge Forecast," Macholevante.com, 2025. [Online]. Available: https://macholevante.com/news-en/198302/tokenization-infrastructure-for-defi-2025-market-surge-30-cagr-forecast-through-2030/?utm_source=chatgpt.com

63. Dapp Expert, "Privacy-First DeFi Revenue Opportunities and Confidential Tokens," 2025. [Online]. Available: https://dappexpert.com/inco-network-privacy-revenue-opportunities

64. Inco Network, "The Confidentiality Layer of Web3," Inco.org. [Online]. Available: https://www.inco.org/

65. Deloitte, "Enterprise Adoption of Privacy-Preserving Blockchain Infrastructure," 2025. [Online]. Available: https://www2.deloitte.com/global/en/pages/financial-services/articles/privacy-blockchain-enterprise.html.