ZorroCash Project Whitepaper

1. Executive Summary

ZorroCash (ZORR) is a dual-layer cryptocurrency ecosystem designed to combine the accessibility of public blockchain infrastructure with the confidentiality of privacy-focused distributed ledger technology. The project operates simultaneously within two interconnected environments: as a BEP-20 token on Binance Smart Chain (BSC) and as a native blockchain derived from the Monero protocol.

ZorroCash (ZORR) is a dual-layer cryptocurrency ecosystem designed to combine the accessibility of public blockchain infrastructure with the confidentiality of privacy-focused distributed ledger technology. The project operates simultaneously within two interconnected environments: as a BEP-20 token on Binance Smart Chain (BSC) and as a native blockchain derived from the Monero protocol.

On Binance Smart Chain, ZorroCash benefits from the speed, low transaction costs, and interoperability of the broader decentralized finance ecosystem. However, as with most public smart contract platforms, transactions on BSC are fully transparent. To address this limitation, ZorroCash introduces a fully confidential native blockchain where transactions are not publicly traceable.

A bidirectional bridge connects these two environments, allowing users to seamlessly transfer assets between the transparent BSC layer and the confidential native network. This architecture enables users to choose between public DeFi participation and private value transfer within a unified ecosystem.

ZorroCash has been developed through an infrastructure-first approach, prioritizing technical completeness and operational stability over promotional exposure. With a verified smart contract framework, a fully functional native blockchain, cross-chain bridge capabilities, and integrated selective disclosure tools, ZorroCash represents a privacy-oriented digital asset system designed for long-term sustainability and controlled ecosystem growth.

2. Problem Statement

Most contemporary blockchain networks prioritize transparency as a core design principle. On public smart contract platforms such as Binance Smart Chain, all transactions, wallet balances, and contract interactions are permanently recorded and publicly accessible. While this transparency enhances auditability and trust in decentralized systems, it also eliminates financial privacy. Every transfer, token holding, and interaction can be analyzed, traced, and permanently linked to wallet addresses.

Most contemporary blockchain networks prioritize transparency as a core design principle. On public smart contract platforms such as Binance Smart Chain, all transactions, wallet balances, and contract interactions are permanently recorded and publicly accessible. While this transparency enhances auditability and trust in decentralized systems, it also eliminates financial privacy. Every transfer, token holding, and interaction can be analyzed, traced, and permanently linked to wallet addresses.

For many users, this level of visibility presents a structural limitation. Transparent blockchains expose transaction histories to analytics platforms, third-party observers, and automated monitoring systems. In practice, this creates an environment where financial behavior can be profiled, correlated, and permanently archived. As decentralized finance expands, the absence of confidentiality increasingly conflicts with the legitimate

expectation of transactional privacy.

At the same time, privacy-focused blockchains often exist in isolation from major decentralized finance ecosystems. While they provide strong confidentiality guarantees, they typically lack seamless interoperability with widely adopted smart contract platforms. This creates a fragmentation problem: users must choose between participating in transparent DeFi environments or operating within closed privacy networks.

ZorroCash addresses this structural trade-off by introducing a dual-layer architecture. By combining a publicly accessible BEP-20 token on Binance Smart Chain with a fully confidential native blockchain, and connecting them through a bidirectional bridge, ZorroCash enables users to move between transparency and confidentiality as needed. This design seeks to reconcile interoperability with privacy, rather than forcing users to choose between them.

3. System Architecture

ZorroCash is designed as a dual-layer system composed of two interoperable blockchain environments: a BEP-20 token deployed on Binance Smart Chain and a native blockchain derived from the Monero protocol. These two layers operate independently yet remain interconnected through a bidirectional bridge mechanism.

ZorroCash is designed as a dual-layer system composed of two interoperable blockchain environments: a BEP-20 token deployed on Binance Smart Chain and a native blockchain derived from the Monero protocol. These two layers operate independently yet remain interconnected through a bidirectional bridge mechanism.

3.1 Binance Smart Chain Layer

On Binance Smart Chain (BSC), ZorroCash exists as a standard BEP-20 token (ticker: ZORR). This layer provides compatibility with the broader decentralized finance ecosystem, including decentralized exchanges, liquidity pools, and smart contract infrastructure. Transactions on BSC are transparent by design, meaning balances, transfers, and contract interactions are publicly visible through blockchain explorers.

On Binance Smart Chain (BSC), ZorroCash exists as a standard BEP-20 token (ticker: ZORR). This layer provides compatibility with the broader decentralized finance ecosystem, including decentralized exchanges, liquidity pools, and smart contract infrastructure. Transactions on BSC are transparent by design, meaning balances, transfers, and contract interactions are publicly visible through blockchain explorers.

The BSC layer enables efficient token distribution, liquidity provisioning, and integration with existing DeFi tools. Smart contracts associated with the token infrastructure, token sale, and reseller program are deployed on Binance Smart Chain and publicly verifiable. For example, the token contract is accessible at:

0x02Ed3DeD768E8411df33E87076171c7633601e42

Public verification of deployed contracts ensures transparency at the smart contract level while maintaining the broader architectural separation between the transparent BSC environment and the confidential native ZorroCash blockchain.

3.2 Native ZorroCash Blockchain

The native ZorroCash blockchain is derived from the Monero codebase and operates as an independent distributed ledger. It implements confidentiality mechanisms including ring signatures, stealth addressing, and confidential transaction structures. These technologies obscure sender, recipient, and transaction amounts at the protocol level.

The native ZorroCash blockchain is derived from the Monero codebase and operates as an independent distributed ledger. It implements confidentiality mechanisms including ring signatures, stealth addressing, and confidential transaction structures. These technologies obscure sender, recipient, and transaction amounts at the protocol level.

Unlike transparent smart contract platforms, the native chain does not expose publicly traceable transaction histories. Instead, transaction validation is performed cryptographically without revealing transactional metadata. Users interact with the native network through dedicated GUI wallets available for Windows, Android and Linux systems.

In addition to private transaction functionality, the wallet supports the generation of view keys. View keys allow selective disclosure of transaction details to designated third parties without compromising the broader privacy guarantees of the network.

3.3 Cross-Chain Bridge Mechanism

A bidirectional bridge connects the Binance Smart Chain layer and the native ZorroCash blockchain. This mechanism enables users to transfer value between the transparent BEP-20 environment and the confidential native network.

A bidirectional bridge connects the Binance Smart Chain layer and the native ZorroCash blockchain. This mechanism enables users to transfer value between the transparent BEP-20 environment and the confidential native network.

When transferring from BSC to the native blockchain, BEP-20 tokens are deposited through the bridge, and the corresponding amount of native ZorroCash is issued. In the reverse direction, native ZorroCash is sent to a designated bridge address, and equivalent BEP-20 tokens are released on Binance Smart Chain. This process maintains supply consistency across both layers while allowing users to choose their preferred transactional environment.

Through this architecture, ZorroCash combines public interoperability with confidential value transfer, forming a unified yet flexible blockchain ecosystem.

4. Privacy Model

ZorroCash operates under a dual-environment privacy model that distinguishes between public smart contract transparency and confidential native-layer transaction privacy. This model allows users to consciously choose their preferred level of visibility depending on context and use case.

ZorroCash operates under a dual-environment privacy model that distinguishes between public smart contract transparency and confidential native-layer transaction privacy. This model allows users to consciously choose their preferred level of visibility depending on context and use case.

On Binance Smart Chain, ZorroCash functions as a standard BEP-20 token. As with all transactions on BSC, transfers, balances, and contract interactions are publicly recorded and accessible through blockchain explorers. This transparency enables decentralized exchange integration, liquidity provisioning, and verifiable smart contract execution. The public nature of the BSC layer is an inherent characteristic of the underlying network.

In contrast, transactions conducted on the native ZorroCash blockchain are confidential by design. The protocol inherits privacy-preserving mechanisms from the Monero codebase, including ring signatures, stealth addressing, and confidential transaction structures. These mechanisms conceal the sender, recipient, and transferred amounts at the protocol level. As a result, transaction flows on the native chain are not publicly traceable, and wallet balances are not externally visible.

Importantly, the ZorroCash privacy model supports selective disclosure. Users may generate view keys within the GUI wallet to reveal transaction details to designated third parties without exposing broader wallet activity. This enables use cases such as voluntary auditing, proof of payment, or regulatory compliance, while preserving default confidentiality.

To extend selective transparency beyond the wallet environment, ZorroCash provides a browser-based Transaction Proof Viewer. By entering a transaction ID, recipient address, and corresponding view key, users can independently verify transaction validity without requiring access to the full wallet. This approach balances strong default privacy with optional transparency, ensuring that confidentiality does not prevent legitimate verification when required.

Through this layered privacy model, ZorroCash reconciles interoperability with confidentiality, enabling users to move between public and private environments without fragmenting their asset base.

5. Tokenomics Overview

ZorroCash is structured around a fixed-distribution token sale model designed to support liquidity formation, ongoing development, and long-term ecosystem sustainability. A total of 18,000,000 ZORR tokens are allocated for public distribution through the official token sale at a fixed exchange rate of 1 BNB = 1,000 ZORR, corresponding to a target raise of 18,000 BNB.

ZorroCash is structured around a fixed-distribution token sale model designed to support liquidity formation, ongoing development, and long-term ecosystem sustainability. A total of 18,000,000 ZORR tokens are allocated for public distribution through the official token sale at a fixed exchange rate of 1 BNB = 1,000 ZORR, corresponding to a target raise of 18,000 BNB.

A substantial majority of the funds raised are designated for liquidity provisioning. Specifically, 80% of the proceeds are allocated to the creation of ZORR–BNB liquidity pools on multiple BNB-based decentralized exchanges. This allocation is intended to enable open market trading and decentralized price discovery following the completion of the token sale.

The remaining funds are distributed across structured operational categories, including a Development Fund, marketing and operational expenses, and a Charity Fund. The Development Fund supports continued blockchain maintenance, infrastructure scaling, security improvements, and feature expansion. Marketing and operational allocations ensure sustainable project management and ecosystem growth. The Charity Fund is reserved for charitable initiatives aligned with the project’s long-term social objectives.

The tokenomics model reflects a capital deployment strategy centered on liquidity formation, technical sustainability, and responsible operational funding. By prioritizing liquidity and infrastructure over short-term incentives, ZorroCash seeks to establish a balanced economic foundation for long-term ecosystem development.

6. Governance and Incentive Structure

ZorroCash is designed as a decentralized infrastructure project with open participation and automated incentive alignment. The ecosystem does not require user registration, account creation, or identity disclosure to participate in the token sale or reseller program. This approach reflects the project’s broader philosophy of minimizing centralized control while preserving operational transparency at the smart contract level.

ZorroCash is designed as a decentralized infrastructure project with open participation and automated incentive alignment. The ecosystem does not require user registration, account creation, or identity disclosure to participate in the token sale or reseller program. This approach reflects the project’s broader philosophy of minimizing centralized control while preserving operational transparency at the smart contract level.

A key component of the incentive structure is the decentralized reseller program. Any participant may generate a reseller code without prior approval or registration. When a token purchase is conducted using a reseller code, a commission of 5% is distributed automatically and in real time through the associated smart contract. This mechanism operates without manual intervention, centralized tracking, or discretionary payout decisions.

The reseller system is implemented directly at the smart contract level, ensuring that commission logic is deterministic and publicly verifiable on Binance Smart Chain. By embedding the incentive mechanism into the contract infrastructure itself, ZorroCash reduces administrative overhead while aligning incentives between project growth and community participation.

Governance within the ZorroCash ecosystem follows a development-led model during the early stages of network growth. Infrastructure maintenance, protocol upgrades, and strategic decisions are managed by the core development team to ensure technical stability and continuity. As the ecosystem matures, governance structures may evolve to incorporate broader stakeholder participation while preserving the foundational principles of privacy, decentralization, and operational transparency.

7. Security Considerations

Security is a foundational principle of the ZorroCash ecosystem and is addressed at multiple architectural layers, including smart contracts, native blockchain infrastructure, bridge operations, and user-level responsibility.

Security is a foundational principle of the ZorroCash ecosystem and is addressed at multiple architectural layers, including smart contracts, native blockchain infrastructure, bridge operations, and user-level responsibility.

On Binance Smart Chain, the ZorroCash token contract, token sale contract, and reseller contract are publicly deployed and verifiable. Public verification allows independent review of contract logic and transaction flows, ensuring transparency in token distribution and commission mechanisms. The use of established BEP-20 standards reduces implementation risk by relying on widely adopted smart contract frameworks.

The native ZorroCash blockchain is derived from the Monero codebase, inheriting a mature and privacy-focused protocol architecture. Confidential transactions, ring signatures, and stealth addressing mechanisms are implemented at the protocol level, ensuring that transaction privacy does not depend on optional

application-layer settings. Network validation is performed cryptographically, preserving consensus integrity without exposing transactional metadata.

The bidirectional bridge between Binance Smart Chain and the native ZorroCash blockchain represents a critical interoperability component. Bridge operations are designed to maintain supply consistency across both environments. Transfers require explicit user initiation, and cross-chain issuance mechanisms are structured to prevent unauthorized token creation. Operational monitoring and infrastructure oversight are maintained to ensure reliability and continuity of bridge functionality.

At the user level, security remains a shared responsibility. Private keys, seed phrases, and wallet credentials are generated and stored locally within user-controlled environments. The project does not collect or retain sensitive wallet information. Users are responsible for safeguarding their credentials and ensuring secure device usage.

Through layered architectural safeguards, contract transparency, and cryptographic privacy mechanisms, ZorroCash seeks to balance confidentiality, interoperability, and operational security within a unified ecosystem.

8. Development Philosophy

ZorroCash has been developed through an infrastructure-first approach, prioritizing technical completeness, operational stability, and architectural integrity over rapid promotional expansion. Since its inception, development efforts have focused on building functional systems rather than pursuing short-term market visibility. This deliberate pace reflects a commitment to structural reliability and long-term sustainability.

ZorroCash has been developed through an infrastructure-first approach, prioritizing technical completeness, operational stability, and architectural integrity over rapid promotional expansion. Since its inception, development efforts have focused on building functional systems rather than pursuing short-term market visibility. This deliberate pace reflects a commitment to structural reliability and long-term sustainability.

Over a multi-year development period, the project progressed through sequential milestones, including smart contract deployment, native blockchain implementation, wallet development, bridge integration, and selective disclosure tooling. Each component was implemented and stabilized before proceeding to subsequent phases. This staged methodology reduces systemic risk and strengthens the coherence of the overall ecosystem.

Unlike projects driven primarily by marketing cycles, ZorroCash emphasizes foundational infrastructure as the basis for ecosystem growth. The dual-layer architecture, bidirectional bridge, and optional transparency mechanisms were designed to form a technically unified system rather than a collection of loosely connected features. The objective has been to create a privacy-capable digital asset that integrates with established decentralized finance infrastructure without compromising architectural clarity.

The project remains committed to measured expansion, responsible capital allocation, and incremental technical enhancement. Future development phases will continue to prioritize usability improvements, scalability, and security while preserving the core principles of confidentiality, interoperability, and decentralized participation.

9. Roadmap Summary

The development of ZorroCash is structured across four sequential phases designed to ensure orderly progression from infrastructure deployment to ecosystem expansion.

The development of ZorroCash is structured across four sequential phases designed to ensure orderly progression from infrastructure deployment to ecosystem expansion.

Phase 1 established the Binance Smart Chain foundation, including the deployment and public verification of the BEP-20 token contract, token sale contract, reseller contract, and the launch of the official multilingual website and decentralized reseller program. This phase created the transparent smart contract infrastructure required for distribution and participation.

Phase 2 focused on the completion of the native ZorroCash blockchain and privacy infrastructure. This included the launch of the Monero-derived mainnet, development of Windows, Android and Linux GUI wallets, integration of view key functionality, deployment of the browser-based Transaction Proof Viewer, and activation of the bidirectional bridge connecting Binance Smart Chain and the native network.

Phase 3 represents market activation, targeting the completion of the token sale and the allocation of 80% of raised funds toward ZORR–BNB liquidity pools. Upon liquidity deployment, ZorroCash transitions to open market trading across multiple BNB-based decentralized exchanges.

Phase 4 outlines the long-term expansion of the ZorroCash ecosystem through continued decentralized exchange liquidity growth, further refinement of the wallet ecosystem, and deeper integration between the ZorroCash native blockchain and Binance Smart Chain infrastructure. This phase also includes the planned development of the ZRBNB chain, a confidential blockchain network designed for private BNB transactions, operating alongside Binance Smart Chain through bidirectional bridge mechanisms.

Together, these phases define a progression from foundational deployment to operational maturity, reflecting a measured and infrastructure-driven growth strategy.

10. Legal Disclaimer

This Whitepaper is provided for informational purposes only and does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation to purchase any securities, financial instruments, or digital assets in any jurisdiction. Participation in the ZorroCash token sale involves risk and may not be suitable for all individuals.

This Whitepaper is provided for informational purposes only and does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation to purchase any securities, financial instruments, or digital assets in any jurisdiction. Participation in the ZorroCash token sale involves risk and may not be suitable for all individuals.

The information contained herein reflects the current intentions and development plans of the ZorroCash project at the time of publication. While reasonable efforts have been made to ensure accuracy, no representations or warranties, express or implied, are made as to the completeness, reliability, or suitability of the information presented. Development plans, technical specifications, and roadmap objectives may be modified, updated, or adjusted without prior notice.

Digital assets and blockchain technologies involve inherent risks, including but not limited to market volatility, regulatory uncertainty, technological vulnerabilities, smart contract risks, and operational challenges. Participants are solely responsible for conducting their own independent analysis and assessment of the risks associated with acquiring and using ZorroCash.

Nothing in this document should be interpreted as legal, financial, tax, or investment advice. Prospective participants are encouraged to consult with independent professional advisors before making any decision related

to digital asset participation.

The ZorroCash project does not guarantee future value, liquidity, exchange listings, or profitability. Users are responsible for safeguarding private keys, wallet credentials, and digital assets. Loss of private keys or unauthorized access to wallets may result in irreversible loss of funds.

By participating in the ZorroCash ecosystem, users acknowledge and accept the risks inherent in decentralized blockchain systems and agree that the project team shall not be held liable for losses arising from the use of the technology, smart contracts, or associated infrastructure.