Wire Network: Revolutionizing the Internet with Trustless Alternatives to Web 2.0 Protocols, IT Infrastructure, and Application Layer Solutions

Kyle Dolan, Ken DiCross, Joseph Rubin

Abstract. Wire Network presents a state-of-the-art blockchain platform that addresses the pivotal challenges holding back the third generation of the internet. We offer a holistic approach to solving the decentralization, security, scalability, onboarding, and interoperability problems in blockchain. Wire Network's novel Appointed Proof of Stake (APoS) consensus model ensures optimal decentralization and robust security. Moreover, Wire Network establishes the world's first truly trustless cross-chain communication by combining Wire Name Service (WNS) with the open-source Universal Polymorphic Address Protocol (UPAP). Furthermore, Wire Network introduces a revolutionary Crypto Single Sign-On (SSO), coupled with the world's first on-chain & decentralized password reset feature, significantly simplifying the onboarding process and user experience. In addition, Wire Network is the only blockchain to consider and solely run on trustless hardware, operating on open-source principles and eliminating dependencies on third-party entities, while an inventive node and governance structure further fortify network integrity. Collectively, Wire Network's breakthroughs harbor the potential to be a catalyst in propelling blockchain technology to new horizons and facilitating mass adoption.

1 Introduction

In virtually every industry, blockchain technology harbors transformative potential. But, for blockchain to actualize its potential, it needs to offer equivalent or superior performance compared to traditional centralized systems, at a competitive price, while providing new capabilities. As of now, the combined transaction per second (TPS) capacity of all existing blockchains still falls far short of what is required to support even a single mainstream enterprise application. Wire Network is designed to fill this void. In this paper, we present a blockchain ecosystem with the ability to scale to never-before-seen TPS benchmarks. This paper introduces Wire Network, not as an insular platform, but as an offering of holistic web3 standards that can operate and grow via the open-source community, independent of us. With innovative features like trustless cross-chain transactions, a shared pool of decentralized computing resources, a crypto-based single sign-on, and decentralized password reset, Wire Network aims to redefine blockchain technology and catalyze its mass adoption. This study presents an in-depth exploration of the Wire Network's core technologies, potential applications, trustless hardware, and potential for enhancing blockchain adoption at scale.

2 Background & Related Works

Bitcoin [1] and Ethereum [2], as pioneering blockchain networks, have undeniably revolutionized the landscape of digital currencies and decentralized applications; however, their scalability constraints and exorbitant transaction fees present critical challenges that necessitate the development of more efficient, faster, and cost-effective blockchain protocols. Subsequent protocols have endeavored to address various fundamental issues inherited from Bitcoin and Ethereum, yet a holistic solution has remained elusive in the blockchain domain; this gap is addressed by Wire Network, which offers an integrated approach to overcoming the industry's pervasive challenges.

In our analysis, the quintessential hurdles impeding the advancement of the blockchain industry encompass (1) decentralization, reflecting the dispersion of control and avoidance of single points of failure; (2) security, concerning the safeguarding of network integrity and user assets; (3) scalability, or the capacity to efficiently handle a burgeoning volume of transactions; (4) onboarding, involving the ease and accessibility for users and developers to adopt and interact with blockchain technologies; and (5) interoperability, the ability for diverse blockchain networks to communicate and collaborate seamlessly in a trustless and decentralized manner.

2.1 Decentralization & Security In public blockchains, decentralization is primarily assessed by examining the distribution of resources governing block generation, which is intrinsically linked to security and scalability. A concentration of these resources among a few entities signifies centralization, thereby compromising security. This security concern arises from the potential for collusion among these entities, enabling denial-of-service attacks and censorship against selected users or the alteration of blockchain historical records [3]. Even today, Ethereum is still plagued by serious censorship challenges, where a significant portion of blocks are created by entities that selectively exclude transactions to comply with regulations and sanctions, which undermines the intended neutrality and openness of the blockchain [4][5].

All networks seem to suffer from some degree of centralization [6], but there seems to be general agreement that Bitcoin is still one of the most secure and decentralized networks [7], despite its other limitations. However, Li and Palanisamy argue that Larimer's Delegated Proof-of-Stake (DPoS) [8], used in Steemit, BitShares, and EOS, offers greater levels of decentralization than Bitcoin [3]. We agree; however, DPoS is still flawed due to issues regarding low voter turnout [9], wealth concentration [10], and voter collusion [11], due to the lack of complete separation of powers by conflating the roles of staking, voting, block production, and key authorization. Moreover, both Bitcoin and EOSIO-based networks lack the ability to measure the physical machine underpinning block production from a trusted boot-state.

2.1.1 The Hardware Problem Although the landscape of blockchain networks is replete with endeavors to achieve impeccable trustlessness through software innovations, an under-addressed dimension is the incorporation of trustless hardware, a critical component needed to properly fortify the security and integrity of these networks. In particular, the Intel Management Engine (IME), a microcontroller embedded within Intel's chipsets, poses a substantial security concern for blockchain systems due to it operating black-box, closed-source software at the kernel level, or ring zero, which is below the main operating system [12].

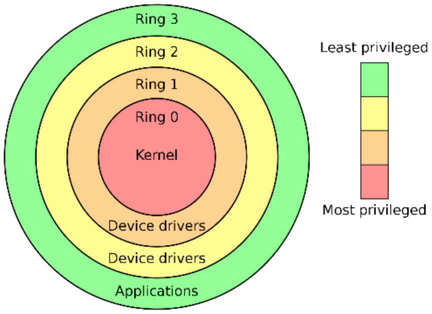

Figure 1. Diagram showing the privilege rings for the x86 available in protected mode.

With access to vital system resources and operating in such a cloistered domain, the IME could potentially be exploited, critically undermining the foundational trust and security that blockchain networks strive to build [13]. With respect to Figure 1, activities or exploits occurring in the lower-level rings (especially ring 0) have the potential to influence or compromise operations in the higher-level rings. Blockchain software primarily operates at the application level, corresponding to ring 3, rendering it susceptible to any compromises that may originate from the more privileged rings, including the kernel level at ring 0. Any closed-source proprietary software running on the machines can pose a threat to the security of the blockchain and user data; and, reliance on such software implicitly places trust in third-party entities like Intel, thereby puncturing the notion of full decentralization, as the blockchain remains tethered to and contingent upon the integrity of external, closed-source components.

2.1.2 Cross-Chain Transactions In the current landscape of blockchain technology, achieving secure and truly decentralized transactions across different chains remains an elusive goal. To facilitate cross-chain interactions, bridges and oracles are commonly employed; bridges serve as point-to-point mechanisms for transferring assets and data between different blockchains, while oracles provide external data to smart contracts to facilitate those transactions. However, both bridges and oracles often entail elements of centralization and present security vulnerabilities, as they become critical points of control and potential failure, thus compromising the trustless nature that is the hallmark of blockchain systems [14][15].

In February 2022, the Wormhole token bridge was hacked for $321 million [16]; in March 2022, the blockchain game Axie Infinity lost $625 million from a bridge exploit [17]; and, in June 2022, the network Harmony's Horizon Bridge was hacked for $100 million [18]. Atomic Cross-Chain Swaps (ACCS) present a promising alternative to bridges for facilitating decentralized asset transfers between blockchains [19]; however, their path to scaling and mass adoption is impeded by a confluence of challenges and limitations, including technical complexity that makes them less accessible to average users, liquidity constraints particularly for less popular assets, limited compatibility with various blockchains, and a user experience that often lacks the polish and ease of use provided by centralized solutions [20].

A major challenge within the current landscape lies in the lack of standardization. Similar to significant transitions seen in the history of internet technology, such as the shift from SSL to TLS for secure internet communication or the evolution of JavaScript and gradual phase-out of older technologies like Flash and ActiveX, blockchain transactions necessitate standardization in addressing and transaction form factors to foster better compatibility, security, and user experience [21][22][23].

2.2 Scalability In the nascent stages of blockchain technology, exemplified by the launch of Bitcoin in 2009, scalability was not a central concern; however, as the technology gained traction, the limitations of early blockchains, such as Bitcoin's 7 transactions per second, became apparent, highlighting the critical need for scalability [24]. Scaling is indispensable for blockchain networks to handle an increasing volume of transactions efficiently, accommodate a growing user base, and meet the diverse requirements of various use cases, ranging from financial services to supply chain management. As of today, despite numerous efforts and innovations ranging from sharding and layer-2 solutions to alternative consensus algorithms, the blockchain space continues to grapple with the trilemma of seeking a balanced trade-off between scalability, security, and decentralization, and a consensus on an optimal approach to achieve scalability without compromising the fundamental tenets of blockchain remains elusive [25].

2.3 Onboarding & User-Friendly Tools During the initial proliferation of blockchain, the technology was primarily geared towards enthusiasts and early adopters, with little emphasis on ease of use or accessibility for a broader audience. The multifaceted nature of blockchain interactions, encompassing cryptographic keys, addresses, gas fees, and token management, poses significant barriers to entry for non-technical users or laymen, stifling broader adoption. Today, there is an increasing recognition within the blockchain ecosystem that user-friendly tools, intuitive interfaces, and streamlined onboarding processes are essential for democratizing access to blockchain technologies [26]. By reducing the complexity and technical know-how required for engagement, these user-centric solutions have the potential to open the gates for a more diverse audience, fostering the integration of blockchain technologies into everyday applications and services.

3 Consensus

3.1 Appointed Proof of Stake Model For Wire Network, we have invented a novel consensus mechanism called Appointed

Proof-of-Stake (APoS), similar to DPoS, but APoS seeks to further separate the powers of stakeholders from influencing the block production and validation process by implementing a governing council (the "Council") as an intermediary. Moreover, Wire Network uses a hierarchical node structure where the Council is "appointed" by the network's Tier-1 ("T1") Node Owners, and after the Council is elected, the T1 Node Owners have no ability to impeach or control them within the Wire protocol. In the Wire ecosystem, the stakers or stakeholders are the Node Owners, and the block producers are the Node Operators. Furthermore, the Council selects the Node Operators and the order in which the Node Operators are utilized is determined by their length of compliance with the network. Node Owners are tasked with authorizing and deauthorizing public keys, which provide authority to the Node Operators, and Owners are also tasked with measuring that Operators remain in compliance. By separating the block production, staking, and governing into these three independent roles, Wire Network avoids virtually all of the deficiencies of traditional proof-of-stake and DPoS chains, thereby enhancing security, decentralization, and fairness within the ecosystem.

3.2 Node Structure and Tiers Wire Network's tiered node structure provides distinct roles and responsibilities for different levels of commitment to the network. For the first three tiers, a significant amount of Wire tokens ($WIRE) must be staked. The node tier's hierarchical arrangement, along with the economic incentives from the Wire token and the allocation of system resources, helps maintain the robustness, security, and decentralization of the network.

Tier 1: Primary Node Owners

The T1 Nodes, with a limited number of 21 seats at the outset, are the backbone of the network, entrusted with maintaining consensus and verifying transactions. T1 Nodes play a pivotal role in the network's governance: they are tasked with submitting flights of candidates and voting in candidates to the Council (see Sections 4.1.3 and 4.1.5, respectively). Each T1 node stakes 7.5 million $WIRE, rewarded back over 12 months, and shares 4% of the existing inventory of network resources. T1 node owners enjoy privileged access to future nodes in Wire Node Expansion (see Section 5.2).

Tier 2: Secondary Node Owners

Tier-2 ("T2") Nodes hold an equal share of 0.15% of the existing inventory. Each T2 Node stakes 1 million $WIRE, rewarded back over 24 months. If a T1 Node is out of compliance, then a Tier-2 ("T2") Node will replace the non-compliant T1 Node and contribute to maintaining consensus and verifying transactions. T2 Nodes are also tasked with endorsing Wire Improvement Proposals (WIPs), which determines the priority in which the proposals are presented to the Council. In the first generation of Wire Network, there are 84 T2 Node seats.

Tier 3: Premier Citizens

Tier-3 ("T3") Nodes, numbering 1,000 seats at launch, stake 100,000 $WIRE that is rewarded back over 36 months. Each T3 Node holds an equal share of 0.00045% of the existing inventory. T1 and T2 Nodes are the only ones that can power smart contracts, whereas T3 nodes can simply use their own resources given to their account.

Auxiliary Tiers

Wire Network has four additional tiers (Tier-4, Tier-5, Tier-6, and Tier-7) that each have their own role in the network. For example, Tier-4 Nodes represent a namespace in the Wire ecosystem. In addition, Tier-5 Nodes fund WIPs and reward a yield to backers that stake. See Section 4.3 for more on WIPs.

3.2.1 Wire Token Utility and System Resources The Wire token serves as the primary digital asset within the Wire Network ecosystem, underpinning various functionalities across the platform. The token is employed to process transactions, store data, facilitate staking for Node Owners, and participate in the network's governance processes. Although $WIRE serves as the core token for the Wire Network, $WIRE is an ERC-20 token on the Ethereum mainnet.

Wire Network introduces two types of system resources: $PWR and $INV. $PWR represents the computational power and network bandwidth associated with accounts, functioning as a regenerative resource. In contrast, $INV represents the RAM or storage capacity an account can consume, which is a non-regenerative resource. Users in need of more resources interact with the Resource Management Exchange (RMEX) system contract. Power and inventory are resources that are issued on lease from the smart contract deployer and cannot be transacted by the end-user. These resources have no max supply or total supply and are not fungible—these resources are delegated to each Node Owner account.

The network's transactions per second (TPS) is directly influenced by the computational power, which dictates transaction processing speed, and storage capacity, which determines the volume of transaction data that can be handled.

3.2.2 Tokenomics and Sustainability Wire's tokenomics aim to stimulate both short-term and long-term incentives, fostering an environment conducive to effective operation of the platform. The Wire Network is fundamentally a marketplace, balancing supply from stakeholders and infrastructure providers against demand from developers and end-users. Through well-designed economic incentives, the platform fosters decentralization and broad participation, helping to ensure its sustainability. Moreover, the $WIRE token serves as the linchpin for decentralized computation within the Wire Network ecosystem, effectively aligning with Moore's law by encapsulating the increasing affordability and demand for computational resources. As such, $WIRE symbolizes a fair-priced mechanism for decentralized compute, with its scalability inherently bound by the limits of computational advancements.

Unlike other blockchain designs, as computing becomes cheaper in line with Moore's Law, so will the economic costs involved with Wire Network usage. Given that Wire consensus does not require exorbitant redundancies like the Ethereum consensus, Wire Network has a path to scaling that is equivalent to centralized compute workflows. Wire Network only needs to be as redundant as a traditional centralized enterprise would want its IT infrastructure.

3.3 Integration of Asynchronous Byzantine Fault Tolerance The APoS model only represents one-half of Wire Network's consensus. The other half is the process of confirming each block until it reaches an immutable state, or finality, and this is performed via an asynchronous byzantine fault tolerant (aBFT) approach. Thus, there are two layers comprising the Wire Network consensus model:

Layer 1 - Native Consensus Model (aBFT)
Layer 2 - Appointed Proof-of-Stake (APoS)

The Wire Network consensus includes a strict time schedule whereby each block is produced every 500 milliseconds (0.5 seconds) and the model permits only a single Node Operator to create a block within the given time slot. Any failure in block production within the designated time frame results in a skipped slot and, in instances where one or more blocks are omitted, a temporal gap of at least 0.5 seconds ensues.

In terms of finality, the Wire layer-1 blocks become irreversible once they have been confirmed by two-thirds plus one of the T1 Nodes (i.e., 15 out of 21). Each Node Operator in the network produces a series of 12 blocks. When producing a block, an Operator includes a unique ID, which is essentially a hash digest of the content of the block. Importantly, this ID also contains the hash of the previous block, establishing a cryptographic link to the prior state of the blockchain. As the next Operator in the sequence produces its set of 12 blocks, it also includes the ID and confirmation of the blocks produced by the previous Operator. These confirmations serve as validations of the state of the blocks produced by the preceding Operator. When 14 subsequent Operators have validated the blocks produced by an Operator through this hash linking and confirmation process, the blocks are considered irreversible. At this point, the network has achieved finality for these blocks. Given the two-thirds plus one quorum and the 0.5-second block time, the time to finality on the Wire layer-1 blockchain is at least 90 seconds.

4 Governance Structure

Harnessing the power of decentralized blockchain technology, the Wire Network's governance model fosters fairness and transparency through a Council elected in a fair multistep process. This system can dynamically adapt to users' needs and demands, continually improving the platform through a robust, user-influenced proposal system. Similar to the Wire token, the Wire Network governance will take place on other layer-1 and layer-2 networks, starting with the Ethereum mainnet, enabling greater transparency and decentralization, due to the separation of powers of the governance from the Node Operators who have custody of Wire's layer-1 blockchain.

4.1 Council Elections The governance of the Wire Network is managed by the Council elected through a multi-step process. This Council is tasked with reviewing and voting on Wire Improvement Proposals (WIPs). The election process is as follows:

4.1.1 Defining a Qualified Candidate Any individual can become a candidate to be considered for the Council by providing their Wire username, verifying their Twitter account, and providing any necessary KYC data. The Council members will be public figures, so it is recommended that candidates campaign accordingly, ideally sharing video or written statements explaining their motivations for wanting to join the Council.

4.1.2 Submission to the Candidate Pool So long as a candidate is willing and is a Qualified Candidate, they can submit themselves to the Candidate Pool. Every Qualified Candidate is able to submit themselves and will be accepted to the Candidate Pool. Even T1 Node Owners are allowed to submit themselves as potential candidates, but there is no guarantee that they will be elected to the Council.

4.1.3 Flight Submission T1 Node Owners then must each submit a flight of three Qualified Candidates from the Candidate Pool, and their submissions must be ranked in order of preference: first string, second string, and third string. All T1 Node Owners then vote on these submissions one-by-one, with a two-thirds plus one supermajority needed for a submission to pass.

4.1.4 Acceptance Prior to Flight Submission, the selected candidates must first accept their nomination by signing an ECDSA signature.

4.1.5 Voting After the flights have been submitted, voting begins. The voting process is an on-chain process structured in a circular manner, which can span three rounds – first, second, and third string. In each round, each T1 Node Owner casts a vote on each candidate. The votes are cast in phases, with each phase representing a vote on an individual candidate. If a candidate secures a supermajority in a round, they are selected. So, for example, if a first-string candidate receives a supermajority, then they get approved to the Council and the second- and third-string candidates are not considered. Moreover, it doesn't matter if the second- or third-string candidates would have received more votes if voted upon.

If none of a T1 Node Owner's candidates pass the first three rounds, the Council seat is then delegated to a vote by the T2 Nodes and a T2 Node Owners are randomly selected to submit flights of candidates until one achieves supermajority (and, in this first generation, it would require two-thirds plus one of the 84 T2 Node Owners). If the T2 Node Owners are unable to elect the required Council members, then the responsibility is similarly passed on to the T3 Node Owners; however, such a scenario is highly unlikely.

4.1.6 Confirmation After candidates are elected (i.e., they receive 2/3 + 1 in the voting process), then the electees must confirm their acceptance and appointment to the Council by signing another ECDSA signature.

4.2 Proposed Instruction Sets Instruction sets form the core of the Wire Network's operation. These sets, also known as Instruction Set Architecture (ISA), provide a precise definition of all the operations that a computer or device must support. Each instruction is represented by a sequence of bits and is divided into fields corresponding to the constituent elements of the instruction.

4.3 Wire Improvement Proposals (WIPs) WIPs are design documents providing information to the Wire community or describing new features for Wire or its processes. WIPs serve as the primary mechanism for proposing new features, collecting community input, and documenting design decisions that will shape Wire.

A WIP must provide a concise technical specification of the feature and a rationale for the feature. The WIP author is responsible for building consensus within the community and documenting dissenting opinions. For Wire implementers, WIPs provide a convenient way to track the progress of their implementation.

The lifecycle of a WIP is as follows: Create > Draft > Last Call > Accepted > Final. The submission process involves reviewing the WIP structure, forking the WIP repository, adding the WIP to the fork of the repository using a provided template, and finally, submitting a Pull Request to Wire's WIP repository.

A WIP must include a preamble, a simple summary, an abstract, specification, rationale, information on backward compatibility, test cases, and implementations. Including the motivation behind the proposal is not required but is highly encouraged.

5 Scaling and Network Expansion

The Wire Network is designed to tackle the challenges associated with scalability, a critical issue in both centralized and decentralized systems of today. It leverages a unique approach to maintain an efficient platform that scales based on network usage, allowing the network to support enterprise-grade, globally-used applications with no upper limit.

5.1 Scalability Wire Network is designed to allow for both scaling vertically and horizontally. Vertical scaling in the network would involve increasing the hardware requirements to be in compliance as a Node Operator. The Node Operators, who should be skilled in managing hardware, would have to make these changes and meet these specifications if they want to remain in compliance. Moreover, there are opportunities for commercial agreements to exist between the Wire Network Foundation and the Node Operators, whereby the Operators invest in compliant hardware to power the network, and in return, they stand to gain based on their length of compliance and as the network expands its requirements. Horizontal scaling, however, would involve the deployment of more block-producing nodes in the network, distributing the workload among them. Wire Network could employ a dual-chain state analogous to hyperthreading in computing. This involves the division of a single state into multiple parallel states, akin to multi-core processors. These parallel states are interdependent, meaning they are threads of each other and cannot function independently. This approach is likened to RAID 0 in data storage, where data is striped across two hard drives in an array; if one breaks, there is total data loss as the data is distributed across both drives. In Wire Network's case, both sub-states would need to exist for the system to function effectively. This combination of both vertical and horizontal scaling options makes Wire Network highly scalable, ensuring efficiency and reliability as it grows.

Inherent to Wire Network's design is the implementation of Asynchronous Byzantine Fault Tolerance (ABFT), which also confers upon Wire Network an ability to sustain network consensus without compromising on the speed and efficiency of communication. By assigning users to different instances and time slots, the transaction load is evenly distributed across the network. This reduces the risk of any single instance becoming a bottleneck.

By allowing for both vertical and horizontal scaling, supported by aBFT consensus, the Wire Network effectively addresses the scalability trilemma. The network's unique architecture can optimize transaction efficiency and communication speed, allowing for robust scalability while maintaining security and decentralization, thus offering a viable solution to one of the most significant challenges faced by traditional blockchain networks.

5.2 Network Expansion Events The current iterations of Wire Network represent the first generation of the network. In order to scale and improve performance, the network must expand to bring in additional resources and nodes. The additional compute added into the network as a result of these expansion events represents resources for the new nodes. These expansions, the Network Expansion Events, are triggered when a certain threshold of usage is reached. This threshold is a rolling average, and the parameters triggering these expansions must be determined by the Council.

When a Network Expansion Event is triggered, new nodes become available to claim by staking large amounts of $WIRE. In addition, when these events occur, the Council's term ends, which means that no new WIPs are considered until all the new nodes have been claimed and another Council is properly elected.

6 Wire Name Service & UPAP

The key to Wire Network's cross-chain solutions and interoperability is the Universal Polymorphic Address Protocol (or UPAP), which is an open-source communications standard. UPAP allows for seamless and trustless transactions across different blockchain networks by employing universal addressing in a deterministic mechanism and universal standards for transaction form factor. The goal of UPAP is to create a universal public key that you can get to from any addressing format created by blockchains (e.g., in this framework, if you know a user's Ethereum address, then you can derive their Solana address deterministically). This technology provides developers with the ability to create applications that allow for cross-chain communication without the need for bridges and oracles, which are both prone to exploitation. The Name Service Framework built on UPAP manifests itself as a chain-agnostic smart contract factory that enables the deployment of name service smart contracts on each network. These contracts allow asset ownership to be abstracted and finality enforced from the settlement layer. For Wire, we are deploying our own name service implementation called Wire Name Service (WNS).

With WNS, we will be deploying name service smart contracts on a number of popular blockchain networks like Ethereum. These smart contracts can be conceptualized as universal escrow buckets that hold assets and enable a novel form of abstracted ownership. In essence, all the assets deposited within these smart contracts are owned by the users, yet they can span multiple networks without users needing native accounts or incurring the associated transaction costs on each network. The name service smart contracts act as enforcement of asset ownership state from deposit to finality, and in this case, finality refers to withdrawal from WNS.

One key feature of WNS is the reverse compatibility with existing top-level domains (like .eth and .sol). Wire Network has reserved the “WNS” namespace on both Ethereum and Solana (i.e., wns.eth and wns.sol). As a result, Wire Network namespaces can be used as recipients on either of these networks by prepending the beginning of the address with their username. For example, the user Bob.wire can receive assets on Ethereum at bob.wns.eth or on Solana at bob.wns.sol, alongside his ability to receive assets on the Wire layer-1 or any WNS-integrated networks via his Bob.wire username.

There are four types of transactions in this UPAP and name service framework:

1.) Native wallet through a UPAP-enabled dApp to another native wallet,
2.) Transferring assets from a native wallet into the name service system,
3.) Transacting assets within the name service system, and
4.) Transferring assets out of the name service system.

Let us consider the Wire blockchain network, Ethereum, and Solana in conjunction with WNS to illustrate UPAP's capabilities. When a WNS smart contract is deployed on each of these three separate layer-1 blockchains, these contracts communicate with both the Wire settlement layer and native layer-1s to transact with assets both within and outside the WNS system.

Use Case #1: Atomic Swap Across Blockchains

Suppose Bob possesses $100 of ETH on Ethereum and Alice has $100 of SOL on Solana, both stored in their respective UPAP-enabled wallets. If they wish to swap these assets, the WNS system can perform an atomic swap on the Wire blockchain, which acts as the settlement layer. Either party can initiate this transaction using their UPAP-enabled wallet. For instance, Bob proposes a transaction to exchange his $100 in ETH for Alice's $100 in SOL. Alice then finalizes the transaction in her UPAP-enabled wallet, resulting in the updated ownership being confirmed and reflected in the WNS system.

Use Case #2: Cross-chain Payments

Now, suppose Bob owes Alice $100 for dinner and has $100 of USDC in the Ethereum's WNS smart contract. If Alice possesses a UPAP-enabled wallet or a Wire username, Bob can simply send his USDC to Alice, with the transaction being settled on the Wire blockchain. But, if Alice only has a Solana wallet with a traditional Solana address, Bob can withdraw his USDC directly to Alice on Solana using his UPAP-enabled wallet, sending to her directly. This versatility highlights the protocol's capability to perform cross-chain transactions seamlessly.

UPAP's essence lies in the principle of "abstracted ownership," where assets can be held and transacted across multiple blockchain networks without the need for native accounts or incurring network-specific fees. This not only enables seamless cross-chain transactions but also opens up many new opportunities for users to engage with digital assets, such as buying Ethereum NFTs on Ethereum without the need to pay for Ethereum’s immense gas fees.

7 Crypto SSO & Password Recovery

Wire Network employs a novel account registration and onboarding for blockchain, which we are referring to as the Wire Network Crypto Single Sign-On (or Crypto SSO). In addition, our framework includes a decentralized password reset system. The inclusion of these two features makes Wire Network geared for mass adoption, given the close parallels the features have to traditional web2 user experiences.

7.1 Account Structure Wire Network features an account structure with a permission-based system. Every Wire account possesses two default permissions: owner and active. The owner permission can change both owner and active permissions, while the active permission can only modify itself. Additionally, these permissions can have individual keys or scoped permission links to other Wire namespaces, including people or smart contracts. A Wire Network account is identified by a namespace comprising 13 characters with a decimal point or 12 characters without. These characters range from A-Z and 1-5. After registering this namespace, two roles (owner and active) are linked to keys.

7.2 User Registration Process To sign-up for an account, a new user will simply input their username, email, and password, which establishes a permission link from the owner to the recovery contract. The creator of the account then revokes their authority over the owner’s permission, and an active key is set. This key is generated securely from the username, email, and password provided by the user without being transmitted over the internet. It mimics a web2 workflow since consistently entering these values in any compatible system will deterministically generate the same key pair.

The key provided to the user carries limited authority, with a higher authority linked to an immutable smart contract. This smart contract can reset the owner or active keys. When a user accumulates significant assets, they can use the active key to perform a transaction that sets a self-generated owner public key, unlinking it from the smart contract, and effectively assuming full control over the account.

7.3 Password Recovery Wire Network's decentralized password reset/recovery process involves a recovery smart contract and the cooperation of authorities, which are the T1 and T2 Node Owners. These authorities commit partial secrets on-chain, which are used to generate a code that is sent to the user's email. The password reset is finalized when the authorities reveal their sections of the code, and the user submits this combined code through an authorized dApp.

8 Trustless Open-Source Hardware

Wire network has built a fully open-source server platform including an open-source Hardware Security Module (HSM) as a foundation for its core consensus architecture. The goal is to create a secure and measurable computing environment for the operation of Wire Network and its layer-1 blockchain. This is achieved by neutralizing typical proprietary firmware, such as Intel's Management Engine (IME), and ensuring the system boots from a trusted state using open-source firmware. The hardware employs Coreboot, an open-source framework for building firmware, and places emphasis on securing Ring Zero, which underpins the kernel. Moreover, Wire Network's HSM is custom-built and acts like a hardware wallet for the server, with all components and firmware being open-source. This module is crucial in ensuring security and can be audited and verified as it is isolated from the rest of the system. By employing this architecture, Wire Network makes sure that the computing environment is as trustworthy as the blockchain, allowing for remote measurement of the machine state analogous to the blockchain state.

9 Conclusion

Wire Network, through its transformative technologies, presents a paradigm shift in the blockchain landscape. It is the first blockchain ecosystem to holistically address both software and hardware layers, showcasing unwavering dedication to open-source principles and standing as a beacon of transparency and integrity. At its core, the novel Appointed Proof of Stake (APoS) consensus model, coupled with Wire Name Service smart contracts and UPAP, offers powerful solutions for the central challenges of blockchain security, scalability, and interoperability.

Pioneering efforts have been undertaken to address the overlooked hardware security issues plaguing the industry. With the introduction of a trustless hardware model, Wire Network aims to fortify the very foundation on which blockchain operates. Moreover, user experience, a vital determinant of mass adoption, has been significantly enhanced through a groundbreaking decentralized Crypto Single Sign-On (SSO) and a first-of-its-kind decentralized password reset feature.

These collective breakthroughs not only redefine the potential of blockchain technology but also set a new benchmark for its adoption. As we continue to push the boundaries of what's possible with blockchain, Wire Network invites the broader open-source community to participate in this exciting journey toward a decentralized and scalable future. The immense potential of Wire Network is still unfolding, and future studies will delve deeper into its innovations and potential impact.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” 2014. [Online]. Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf.

[3] C. Li, and B. Palanisamy, “Comparison of Decentralization in DPoS and PoW Blockchains.”

[4] Z. Wang, X. Xiong, and W. J. Knottenbelt, “Blockchain Transaction Censorship: (In)secure and (In)efficient?” [Online]. Available: https://eprint.iacr.org/2023/786.pdf.

[5] A. Wahrstätter et al., “Blockchain Censorship,” 29 May, 2023. [Online]. Available: https://arxiv.org/pdf/2305.18545.pdf.

[6] B. Kusmierz, and R. Overko, “How centralized is decentralized? Comparison of wealth distribution in coins and tokens.”

[7] Q. Li, C. Li, X. Zhao, and X. Chen, “Measuring Decentralization in Bitcoin and Ethereum using Multiple Metrics and Granularities.”

[8] D. Larimer, “Delegated Proof of Stake (DPOS),” [Online]. Available: https://how.bitshares.works/en/master/technology/dpos.html#voting-algorithm.

[9] Q. Hu, B. Yan, Y. Han, and J. Yu, “An Improved Delegated Proof of Stake Consensus Algorithm.”

[10] X. Wei, A. Li, and Z. He, “Impacts of Consensus Protocols and Trade Network Topologies on Blockchain System Performance.”

[11] H. Choo, “Comprehensive data analysis on the EOS blockchain,” 2020. [Online]. Available: https://koasas.kaist.ac.kr/handle/10203/285070.

[12] Wikipedia, “Intel Management Engine,” [Online]. Available: https://en.wikipedia.org/wiki/Intel_Management_Engine.

[13] E. Portnoy, and P. Eckersley, “Intel's Management Engine is a security hazard, and users need a way to disable it,” [Online]. Available: https://www.eff.org/deeplinks/2017/05/intels-management-engine-security-hazard-and-users-need-way-disable-it.

[14] S.-S. Lee, A. Murashkin, M. Derka, and J. Gorzny, “SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks,” October 31, 2022. [Online]. Available: https://arxiv.org/pdf/2210.16209.pdf.

[15] G. Caldarelli, and J. Ellul, “The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach,” August 18, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/16/7572.

[16] B. Newar, “Wormhole token bridge loses $321M in largest hack so far in 2022,” February 03, 2022. [Online]. Available: https://cointelegraph.com/news/wormhole-token-bridge-loses-321m-in-largest-hack-so-far-in-2022.

[17] A. Thurman, “Axie Infinity’s Ronin Network Suffers $625M Exploit,” March 29, 2022. [Online]. Available: https://www.coindesk.com/tech/2022/03/29/axie-infinitys-ronin-network-suffers-625m-exploit/.

[18] B. Newar, “Breaking: Harmony’s Horizon Bridge hacked for $100M,” June 24, 2022. [Online]. Available: https://cointelegraph.com/news/breaking-harmony-one-s-horizon-bridge-hacked-for-100m.

[19] M. Herlihy, “Atomic Cross-Chain Swaps,” July 23-27, 2018. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3212734.3212736.

[20] M. H. Miraz, and D. C. Donald, “Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities,” 20 September 2019. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1902/1902.04471.pdf.

[21] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” August 2018. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8446.

[22] D. Flanagan, “JavaScript: The Definitive Guide,” 7th ed., May 2020. [Online]. Available: https://www.oreilly.com/library/view/javascript-the-definitive/9781491952016/.

[23] Adobe, “Flash & The Future of Interactive Content,” July 25, 2017. [Online]. Available: https://theblog.adobe.com/adobe-flash-update/.

[24] Wikipedia, “Bitcoin scalability problem,” [Online]. Available: https://en.wikipedia.org/wiki/Bitcoin_scalability_problem.

[25] M. H. Nasir et al., “Scalable blockchains — A systematic review,” 30 July 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21002971?via%3Dihub.

[26] L. Glomann, M. Schmid, and N. Kitajewa, “Improving the Blockchain User Experience - An Approach to Address Blockchain Mass Adoption Issues from a Human-Centred Perspective,” 11 June 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-20454-9_60.