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

Important Notice: *This paper is a living document that will be actively updated as Wire Network evolves. We welcome contributions from the open source community to expand and refine its content.*

Abstract. Wire Network presents a 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 Appointed Proof of Stake consensus model, combined with aBFT, ensures optimal decentralization and scalability. Moreover, Wire Network establishes the world's first Universal Transaction Layer by combining our layer-1 with Wire Name Service with the Universal Polymorphic Address Protocol. Wire also presents a novel economic model introducing a Techno Capital Machine and the Resource Owners' Association, promoting sustainable growth and rewarding ecosystem contributors. Furthermore, Wire Network introduces a decentralized Crypto Single Sign-On significantly simplifying the onboarding process and user experience in blockchain. In addition, Wire's hierarchical node structure and governance further fortify network integrity. Collectively, Wire Network has 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 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 interoperability, a shared pool of decentralized computing resources, a crypto-based single sign-on, and more, Wire Network aims to redefine blockchain technology and catalyze its mass adoption. This study presents an in-depth exploration of Wire Network's core technologies, potential applications, 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 few entities signifies centralization, 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 significant 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 decentralization [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 to Bitcoin [3]. We agree; however, DPoS is still flawed due to issues regarding low voter turnout [9], wealth concentration [10], and voter collusion [11].

2.1.1 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. 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 [12][13].

In February 2022, the Wormhole token bridge was hacked for $321 million [14]; in March 2022, the blockchain game Axie Infinity lost $625 million from a bridge exploit [15]; and, in June 2022, the network Harmony's Horizon Bridge was hacked for $100 million [16]. Atomic Cross-Chain Swaps (ACCS) present a promising alternative to bridges for facilitating decentralized asset transfers between blockchains [17]; 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 [18].

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 [19][20][21].

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 [22]. 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 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 [23].

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 [24]. 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.

2.4 Techno Capital Machine The Techno Capital Machine (TCM) is an innovative framework developed by the decentralized AI project Morpheus to streamline the creation and deployment of open-source software in the blockchain and AI space [25]. TCM operates as a novel fundraising method where users stake yield-generating assets like Ethereum (ETH), directing the yield that is generated toward the projects they want to support, in exchange for receiving a proportional reward in the project's token. This contrasts with traditional token sales or ICOs because the users retain their staked principal and can unstake it any time, thereby reducing their financial risk while still supporting the project.

3 Wire's Layer-1 Consensus

3.1 Background & Issues with DPoS Consensus While Delegated Proof-of-Stake (DPoS) is a highly performant and scalable consensus mechanism that enables efficient transaction validation and block production, it raises concerns regarding the concentration of power and the lack of separation of duties. In systems like EOSIO, token holders influence block production by voting for block producers (BPs), resulting in a select group wielding significant authority over both network operations and governance decisions. This convergence of roles means that the same entities responsible for validating transactions also have the power to propose and implement protocol upgrades, manage inflation rates, and even reverse transactions under certain conditions. Such a concentration of influence can undermine decentralization and expose the network to risks like collusion or governance capture. The absence of a clear separation between those who govern and those who validate compromises the robustness of the consensus mechanism, potentially affecting the security and fairness of the blockchain network.

3.2 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 order in which the Node Operators are utilized is determined by their length of compliance with the network. T1 Node Owners are tasked with monitoring Node Operators to ensure they remain in compliance. The Node Owners also are tasked with authorizing and deauthorizing public keys, which provide authority to the Node Operators. By separating the block production, staking, and governing into these three independent roles, Wire Network avoids many of the deficiencies of traditional proof-of-stake and DPoS chains, thereby enhancing security, decentralization, and fairness within the ecosystem.

3.3 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: The T1 Nodes, with a limited number of 21 seats at the outset, are the backbone of the network, entrusted with helping oversee Node Operators and authorizing & deauthorizing keys. 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. Each T1 node stakes 7.5 million $WIRE, rewarded back over 12 months, and is allotted 4% of the network's resources in the first generation.

Tier 2: Tier-2 ("T2") Nodes hold an equal share of 0.15% of the network's initial resources. 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 take over its duties with respect to overseeing Node Operators and key

delegation. T2 Nodes are also tasked with endorsing Wire Improvement Proposals (WIPs), and these endorsements determine 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: Tier-3 ("T3") Nodes, numbering 1,000 seats at launch, will require would-be owners to stake 100,000 $WIRE, which is rewarded back over 36 months. Each T3 Node holds an equal share of 0.00045% of the existing network resources in the first generation.

One additional benefit that each of these three tiers of nodes (i.e., T1, T2, and T3) share is that they can be used to power smart contracts, providing a gas-free experience for the end-users. To enable this benefit, Node Owners can select specific contracts to whitelist in the Node Owner Dashboard, and then the whitelisted contracts will use from the node's resources to cover the transaction fees, rather than prompting the users themselves to spend Wire token (see Section 6.1 for more details).

Tier 4: Tier-4 ("T4") Nodes in the Wire ecosystem represent namespaces or universal identities. These will be sold post-network launch and this sale will include a total of 3,000,000 T4 Nodes. Each of these sold will also include 48 Wire tokens distributed back to the buyer over a period of 12 months.

3.4 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 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-third 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, Wire Network's governance model fosters fairness and transparency through a Council elected in a fair multistep process. This system can dynamically adapts to user needs and demands, continually improving the platform through a robust, user-influenced proposal system. Similar to the Wire token, Wire Network's 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 The Council The Wire Network Council is voted in by the T1 Node Owners. The election process involves T1 Node Owners submitting flights of candidates to be considered and voted on by all T1 Node Owners. Candidates must receive a 'two-thirds plus one' majority vote to be elected. The individuals serving on the Council must all be public figures, meaning anonymous or pseudo-anonymous Council Members are not allowed. The role of the Council is to govern Wire Network through reviewing and voting on Wire Improvement Proposals (WIPs).

4.2 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 have shaped 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. T2 Node Owners are tasked with endorsing WIPs, and the number of endorsements on each WIP determines the order in which the Council votes on them (in order of most endorsements to least).

5 Scaling and Network Expansion

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 involves 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, on the other hand, would involve the deployment of more block-producing nodes in the network, distributing the workload among them. This method of scaling will be explored further in Future Works (see Section 9.1).

Scaling will be inherent to the Network Expansion process (see Section 5.2 below), in which the Council will vote on and decide new requirements that Node Operators need to comply with in order to continue Node Operation in the next generation of the Network. By upgrading their hardware, Node Operators will play a key role in satisfying the growing demand for resources in Wire Network, and a key role in allowing the network to scale to support enterprise-grade applications.

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 vertical (and, in future, horizontal) scaling, supported by aBFT consensus, Wire Network is poised to effectively address the scalability in blockchain.

5.2 Network Expansion Events The current iteration of Wire Network represents 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. The usage metrics that can trigger expansion are the network's RAM and CPU/NET. The RAM in Wire Network represents the storage capacity, and if the network's RAM surpasses 60% of the total allocated RAM for the system, then expansion is triggered. The CPU/NET represents the computational power and network bandwidth of the system. With this metric, an expansion is triggered if the rolling average of the CPU/NET is above 60% for a period of 90 days.

When a Network Expansion Event is triggered, a new node sale begins, where users can purchase with or stake $WIRE in exchange for the newly available nodes. During this time period, Node Operators must also upgrade their hardware to the new requirements set by the Council. Once the RAM capacity or rolling average of CPU/NET surpasses 80%, then the network will begin operating on the upgraded nodes, completing the expansion. In addition, this 80% threshold marks the end of the Council's term, which means that no new WIPs are considered until another Council is properly elected. The Council will be rewarded in Wire token for leading the network through to a successful expansion. The successful completion of an expansion indicates that the Council has effectively fulfilled its duties.

There may be scenarios in future where the network usage falls sharply, necessitating a network contraction. Under this scenario, the Council would have failed in its duties to grow the network, and the Council Members would forfeit any right to token compensation.

6 Wire Tokens, Resources, & Economy

6.1 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 used to pay for transaction fees and facilitate staking for Node Owners during expansion. Although $WIRE serves as the primary token for Wire Network, $WIRE is an ERC-20 token on the Ethereum mainnet.

In Wire Network, significant innovations have been introduced over the traditional EOSIO blockchain protocol, particularly in the approach to token utility and system resource management. Central to these innovations is the Resource Owners' Association (ROA), a novel system that redefines how resources such as CPU, NET, and RAM are allocated and consumed within the network. Unlike the EOSIO model, where users had to stake core tokens to acquire CPU and NET resources and purchase RAM through specific actions, Wire Network delegates resource management to the ROA, simplifying the user experience.

The ROA acts as a proxy for Node Owners, who collectively own all the system resources of the network. These resources are represented by a new core token called SYS, which is a non-transferable token used internally by the system. Users do not hold SYS tokens; instead, they are allocated directly to the ROA, which imposes usage limits based on the Node Owners' holdings.

When transactions are processed on Wire Network, the system uses SYS tokens to utilize the necessary resources (CPU, NET, and RAM), effectively abstracting the complexity of resource management away from the end-users. This design allows users to engage with the network without the need to stake tokens or directly manage resource allocations, enhancing accessibility and simplifying interactions.

Node Owners have the capability to establish *policies* that delegate portions of their allocated resources (i.e., SYS) to specific smart contracts. By whitelisting specific contracts, Node Owners can enable a gas-free experience for end-users interacting with them. This means that when a user interacts with a smart contract that has established a *policy* with some Node Owner, the transaction fees are covered by the Node Owner's resources managed by the ROA contract, and the user does not need to spend $WIRE tokens for that interaction. This mechanism not only enhances the user experience but also encourages the development and adoption of decentralized applications on the network by lowering the barriers to entry.

In scenarios where a smart contract is not whitelisted (i.e., has no policy associated with it), the behavior differs based on whether the user is a Node Owner. If a Node Owner interacts with a non-whitelisted contract, the transaction costs are deducted from their node's allocation of resources managed by the ROA. For users who are not Node Owners, interacting with a contract that has no policy requires them to pay transaction fees in $WIRE tokens. These fees are forwarded to the Emissions Contract (see Section 6.3), which compensates the Node Owners whose resources were utilized during the transaction. This creates an incentivization mechanism for Node Owners, providing them with compensation for unused resources and promoting resource availability across the network.

Wire Network maintains essential safeguards to ensure performance and security by preserving standard block and transaction limits, thereby maintaining network stability and preventing abuse. Resource usage is meticulously tracked based on established policies, Node Owner activities, and interactions involving non-Node Owners. In our system, CPU represents the computational time required to process a transaction, NET accounts for the amount of data transmitted over the network during a transaction, and RAM involves the storage or modification of data on the blockchain.

By streamlining resource management through the ROA and introducing the SYS token for internal accounting, Wire Network enhances scalability, performance, and user experience. We believe this approach reduces complexities associated with resource staking and management, lowers entry barriers for developers and users, and fosters a more vibrant and active blockchain ecosystem.

6.2 Tokenomics and Sustainability Wire's tokenomics aim to stimulate both short-term and long-term incentives, fostering an environment conducive to effective operation and sustainable growth of the platform. 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.

At the core of Wire Network's economic model is the Wire token (or $WIRE), which serves as the linchpin for decentralized computation within the ecosystem. The total supply of $WIRE is fixed at 1,000,000,000 tokens, allocated strategically to support various aspects of the network:

- 157,500,000 $WIRE (15.75%) are allocated to T1 Nodes,
- 84,000,000 $WIRE (8.4%) are allocated to T2 Nodes,
- 100,000,000 $WIRE (10%) are allocated to T3 Nodes,
- 144,000,000 $WIRE (14.4%) are allocated to T4 Nodes, and
- 514,500,000 $WIRE (51.45%) are allocated to the Techno Capital Machine.

Moreover, the Wire token effectively aligns 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.

6.3 Techno Capital Machine Inspired by Morpheus, Wire Network introduces its own Techno Capital Machine (TCM), which is a decentralized financial system embedded within the protocol, designed to reward and incentivize various participants for their contributions to the ecosystem. At the core of the TCM is the Emissions Contract, which manages the distribution of rewards to different parties supporting the network. Figure 1 below illustrates the structure of the TCM.

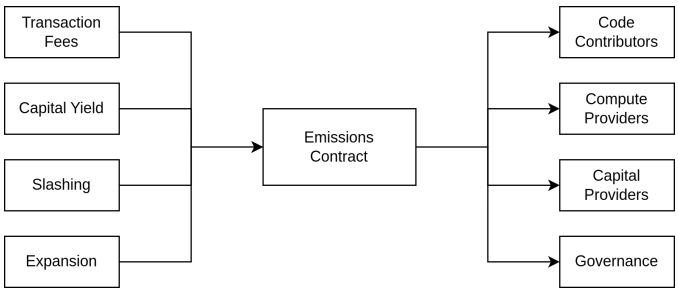

Figure 1. Diagram of Wire Network's TCM system.

The Emissions Contract is funded through multiple sources: transaction fees collected in $WIRE (gas spent within the network), capital yield from staked assets, slashing penalties from bad actors, and Wire tokens accrued during Network Expansion Events from users acquiring the newly available nodes. Transaction fees are generated as users interact with the network, while capital yield comes from Wire's upcoming lending mechanism that allows Capital Providers to stake assets like Ethereum (ETH). Slashing serves as a deterrent against malicious activities, redirecting penalized $WIRE back into the Emissions Contract.

Rewards from the Emissions Contract are allocated to four key groups:

1.) Code Contributors: Individuals who contribute code to Wire Network, enhancing the protocol or developing supporting decentralized applications (dApps). They receive $WIRE tokens based on a unique weighting system that reflects their level of contribution.

2.) Compute Providers: This category includes Node Operators, who validate transactions on Wire Network, and Batch Operators, who run software to perform batch withdrawals. Batch withdrawal operations enable users to exit Wire Network back to native networks more cost-effectively.

3.) Capital Providers: Participants who stake capital such as ETH through Wire's lending mechanism. By directing the yield earned from staking native coins towards the TCM, they accumulate weights that translate into rewards in $WIRE tokens.

4.) Governance: This group rewards the Council for successfully fulfilling their duties in expanding the network, as well as Node Owners who allow their nodes' resources to be used by others. The transaction fees paid by users who do not own nodes are funneled to the Emissions Contract to compensate these four key groups.

At the outset, the Emissions Contract is seeded with a little over half the token supply (514.5 million Wire tokens) to initiate the reward system for all participants. The overarching goal of the TCM is to establish a sustainable economic model where the inflow of value matches the outflow over time, ensuring continuous support and growth of the Wire Network ecosystem. While achieving this balance may take years, the design of the TCM aims for long-term sustainability and equitable distribution of rewards among all contributors and participants in Wire Network.

7 The Universal Transaction Layer

Wire Network is the world's first Universal Transaction Layer (UTL), a groundbreaking infrastructure that allows smart contracts to interact with assets across all connected blockchains. The UTL serves as a single, unified platform for bringing together and scaling blockchain networks, where interoperability between the connected chains is seamless and efficient, addressing the fragmentation that currently exists in the blockchain ecosystem. This universal interoperability is made possible by three key components: a novel layer-1 blockchain serving as a settlement layer, Wire Name Service, and the Universal Polymorphic Address Protocol.

7.1 The Components of the UTL The following sections delve into the three major components that make up the UTL and explain how they collectively facilitate interoperability within Wire Network.

7.1.1 Wire Name Service (WNS) Wire Name Service is a set of smart contracts and protocols deployed both on Wire Network's layer-1 blockchain and on native blockchains like Ethereum and Solana. The WNS contracts deployed to native chains are often referred to as "bucket contracts" within the UTL. These bucket contracts serve as secure storage locations for assets entering the UTL; once assets are deposited into these contracts, they are locked within the system until properly withdrawn. This mechanism ensures that the assets remain on their original blockchain, maintaining the security and consensus integrity of the native chain.

In its initial iteration, the WNS smart contracts and the UTL system support three asset types: ERC-20 tokens, ERC-721 tokens (non-fungible tokens), and ERC-1155 tokens (multi-token standard).

7.1.2 The Settlement Layer At the core of the UTL is Wire Network's novel layer-1 blockchain protocol, functioning as the settlement layer for all transactions within the network. This blockchain is designed for high performance, offering rapid transaction speeds and substantial throughput—features essential for supporting enterprise-grade applications and high-frequency trading. The settlement layer is where the tracking of asset ownership occurs within the UTL, particularly through the settle.wns smart contracts. These contracts maintain a comprehensive ledger of all assets deposited into the UTL and their ownership details. When transactions occur within the UTL, the settle.wns contracts update the ownership records accordingly, ensuring transparency, security, and immutability of the transaction history.

7.1.3 Universal Polymorphic Address Protocol (UPAP) The Universal Polymorphic Address Protocol is an open-source communication standard designed to create a universal public key derivable from any existing blockchain address format. UPAP enables the deterministic derivation of a user's address on Wire Network from their public key on the native blockchain—for example, deriving a Wire Network address from a user's Ethereum public key. In this framework, knowing a user's address on one blockchain allows for the derivation of their corresponding addresses on other supported blockchains.

To utilize the UTL, users must first create an account on Wire Network. This can be accomplished directly via the Wire layer-1 blockchain or by connecting an external network's account (such as an Ethereum wallet) and using UPAP to generate a corresponding account within Wire Network. When users connect their Ethereum wallet to a Wire-enabled decentralized application (dApp) to create an account,

UPAP takes their Ethereum public key and converts it into the format required by Wire Network. This process allows users to sign transactions and access the Wire Network ecosystem using the wallet they already know and use, without any behavior change. By leveraging UPAP, Wire Network ensures a seamless user experience and lowers barriers to adoption by eliminating the need for users to manage multiple wallets or private keys.

7.2 Mechanisms of Interoperability Interoperability within Wire Network operates through a series of coordinated actions involving the settlement layer, WNS, and UPAP, all designed to maintain security, efficiency, and user convenience.

Firstly, if the user does not have a Wire Network account, UPAP is used to create and map their native address to a Wire Network account, allowing them to sign transactions with their existing wallet.

When users decide to utilize the UTL, they begin by depositing their assets into the WNS smart contracts on their native blockchains. For example, a user holding an ERC-20 token like USDC on Ethereum would deposit it into the Ethereum WNS bucket contract. This action securely locks the asset within the contract, ensuring it remains on the original chain and is protected by the native blockchain's consensus mechanisms.

Upon depositing assets, the system records the ownership details within the settle.wns smart contracts on the layer-1 settlement layer. This contract maintains a comprehensive ledger that tracks all assets deposited into the UTL. The ownership records are updated to reflect the user's holdings, effectively mapping the user's assets from the native blockchain into the UTL environment. In this system, users maintain custody of the assets and only by signing authoritatively can the assets be transferred.

As users interact with Wire-enabled dApps, they transact based on the ownership records within the settle.wns smart contracts. For instance, if a user wishes to trade their USDC for wrapped ETH (wETH), the transaction involves updating the ownership entries in the settle.wns ledgers. Interoperability is facilitated by decentralized exchanges operating within the UTL, which maintain liquidity pools of tokens from different chains. Users can enter the UTL with an asset from one blockchain, such as an Ethereum ERC-20 token, and swap it for a token from another network, like a Polygon ERC-20 token located in the Polygon WNS bucket. They can then withdraw the Polygon asset onto the Polygon network. No actual movement of assets occurs on the native blockchains during these transactions; instead, the ledger updates represent changes in ownership rights over the locked assets.

This mechanism ensures that all transactions within the UTL are secure, efficient, and transparent. The layer-1 settlement layer validates and records each transaction, providing an immutable record that can be independently verified. When users decide to exit the UTL, they can withdraw their assets from the WNS bucket contracts on the blockchain of their choice. The settle.wns contracts update the ownership records accordingly, and the assets are unlocked from the bucket contracts and transferred to the user's address on the target blockchain.

7.3 Key Innovations and Benefits Beyond interoperability, Wire Network's Universal Transaction Layer (UTL) introduces several key innovations that enhance performance, scalability, and accessibility for decentralized applications and enterprises alike. These innovations not only improve the user experience but also provide significant advantages over traditional blockchain solutions.

One of the primary benefits of the UTL is its high-performance layer-1 blockchain protocol, designed for rapid transaction speeds and substantial throughput. By offering a fast and efficient platform, Wire Network serves as an ideal scaling solution for slower and more costly layer-1 networks like Ethereum. In addition to speed, the UTL provides extremely low or zero transaction costs, depending on the dApp you are using. Many dApps within the Wire ecosystem offer a completely gas-free experience due to the network's unique node ownership structure, whereby the T1, T2, and T3 Nodes can power smart contracts using their allocated resources, effectively subsidizing transaction fees for the end-users. This model makes Wire Network an excellent scaling solution for slower and more costly networks, and it provides a better user-experience by encouraging dApps to cover the cost of transaction fees for their users through node ownership.

By building on Wire Network, dApps and businesses can transform their applications into universal applications, accessible to users across all connected blockchains. For example, a decentralized exchange (DEX) operating solely on the Base layer-2 network can integrate Wire Network's technology, enabling the creation of liquidity pools with assets across different networks, effectively transforming the DEX into a central hub for cross-chain trading—a universal DEX. Moreover, by pooling the liquidity of all connected ecosystems, Wire Network facilitates the development of new types of decentralized finance applications and can establish new standards for asset protection & creator royalties.

Unlike bridges and other point-to-point interoperability solutions, Wire Network has a unique hub-and-spoke design (visualized below in Figure 2), functioning as both a transaction layer and an aggregation layer for all connected blockchains.

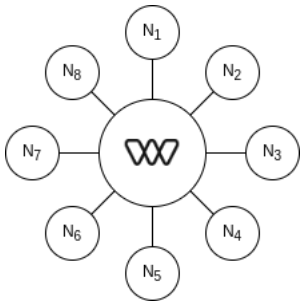

Figure 2. Diagram depicting the hub-and-spoke design of Wire Network, where N_X represent other blockchain networks connected to Wire.

Users can enter the UTL from any connected chain, transact within a low-cost, high-throughput environment, and exit on the chain of their choice. The costs associated with entering the system remain competitive since users only need to transfer assets into the WNS smart contracts, and the withdrawal process is made competitive via a bulk withdrawal system where withdrawal requests are batched and processed by providers known as Batch Operators.

Furthermore, the entire UTL is fully open-source and WNS is just the first implementation of this name service framework. Developers are free to build upon and customize this technology as they see fit. For instance, a team requiring stronger signature algorithm could modify the codebase to integrate Falcon 512 and deploy their own version. This openness fosters an environment of collaboration and continuous improvement, driving the evolution of enterprise-grade multi-chain applications.

7.3.1 Advantages Over Existing Solutions Traditional blockchain interoperability solutions often rely on point-to-point communication systems, such as bridges, to transfer assets between chains. While these bridges enable basic interoperability, they come with significant drawbacks. Users must often take a "leap of faith" by moving assets out of the protective consensus of the original chain, exposing them to potential security risks. Additionally, high transaction costs and slow speeds associated with these systems can outweigh their practical utility.

Wire Network's UTL differentiates itself by eliminating the need for bridges or oracles. Instead of transferring assets between blockchains, the UTL keeps assets securely locked within the native chains' WNS bucket contracts. Ownership rights are transacted within the UTL's settlement layer, allowing assets to benefit from *dual consensus*: they retain the security of their native blockchain while also being protected by Wire Network's layer-1 consensus mechanism.

This approach enhances security by reducing reliance on external validators or complex multi-signature schemes common in traditional bridge systems, which can introduce vulnerabilities. By transacting ownership rights rather than moving assets, Wire Network minimizes the risk associated with cross-chain transactions. Assets remain under the protective consensus mechanisms of their original blockchains, and dependency on external parties is significantly reduced.

In summary, Wire Network's UTL offers a faster, more secure, and cost-effective solution for blockchain interoperability. By maintaining assets on their native chains and transacting ownership rights within a high-performance environment, it provides distinct advantages over existing point-to-point communication systems, positioning itself as a superior alternative to other interoperability solutions.

7.3.2 Criteria for Becoming a Connected Chain The UTL is an open framework that most blockchain networks can connect to to access the benefits that the UTL has to offer. The criteria for becoming a connected chain is (1) the network must ensure support for signed proofs in the chain’s native format, (2) ensure there is an implementation of the external WNS contracts deployable to that chain, and (3) deploy a settlement contract from the settlement factory for that specific chain. If a network lacks support for standard methods of generating and verifying signed proofs, intentionally restricts these capabilities, or does not support custom smart contracts, it will require a more bespoke integration with the UTL.

8 The Crypto SSO

Wire Network employs a novel account registration and onboarding for blockchain, which we refer to as the Crypto Single Sign-On (or Crypto SSO). This features helps make Wire Network geared for mass adoption, given the close parallels that this login method has to traditional web2 user experiences.

8.1 Account Structure Wire Network features an account structure inherited from EOSIO that is 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. Auth.ext, in contrast, is limited to a single key record and is used in the UTL system to enable users to sign transactions with their preferred wallets —like Ethereum wallets—when interacting with Wire 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.

8.2 Crypto SSO Mechanism To sign-up for an account, a new user can simply fill in a form input, such as entering a username, email, and password. This process generates a key securely from the provided form entries (e.g., username, email, and password) 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.

9 Future Works

As Wire Network continues to evolve, several promising areas have been identified for future research and development. These initiatives aim to enhance the network's capabilities and address challenges that require further exploration. This section outlines concepts and technologies currently under consideration, which may necessitate additional research or dedicated papers to fully realize their potential.

9.1 Horizontal Scaling While Wire Network has a clear vision for vertical scaling by increasing hardware requirements for Node Operators, horizontal scaling remains a topic for future exploration. Horizontal scaling involves deploying additional block-producing nodes to distribute the workload more evenly across the network. This approach can significantly enhance the network's capacity to handle a growing number of transactions without compromising performance.

One proposed method for horizontal scaling is employing 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. Implementing this model would allow for greater transaction throughput and enhanced scalability, enabling the network to support enterprise-grade, globally-used applications without an upper limit.

9.2 Password Recovery Wire Network initially developed a decentralized password reset and recovery process involving a recovery smart contract and the cooperation of authorities—specifically, T1 and T2 Node Owners. In this system, authorities commit partial secrets on-chain to generate a code 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.

However, the preliminary implementation relied heavily on the security of the user's email, which is not sufficiently secure for safeguarding blockchain assets. Future work will focus on enhancing this password recovery mechanism to provide greater security and user protection. This may involve exploring alternative methods of identity verification and secret sharing that do not depend solely on email security, thereby creating a more robust and trustless recovery process.

9.3 Trustless Hardware While significant efforts in blockchain technology have concentrated on achieving 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 chipsets, poses a substantial security risk 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 [26].

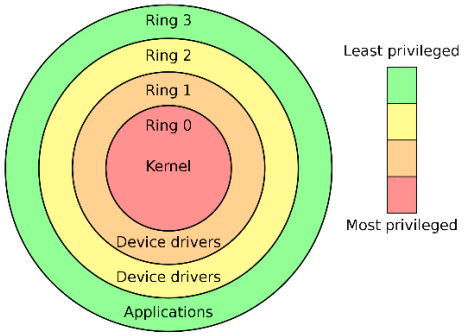

Figure 3. Diagram showing the privilege rings for the x86 available in protected mode.

With access to vital system resources and operating in such a cloistered domain, the IME is a potential attack vector with a track record of being exploited, which critically undermines the foundational trust and security that blockchain networks strive to build [27]. Similarly, AMD's Platform Security Processor (PSP) and Nvidia's proprietary GPU firmware introduce comparable threats due to their operation in high-privilege domains with closed-source code, and these have also had a history of security exploits that could undermine the trust and security of blockchain systems [28][29]. 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.g

To address this, Wire Network is developing a fully open-source server platform, including an open-source Hardware Security Module (HSM), as the foundation for its core consensus architecture. By neutralizing proprietary firmware like IME and ensuring the system boots from a trusted state using open-source firmware (such as Coreboot), Wire Network aims to secure the most privileged levels of system operation. The custom-built HSM acts as a hardware wallet for the server, with all components and firmware being open source, allowing for auditing and verification. Isolated from the rest of the system, this module will be crucial for ensuring security and trustworthiness.

By employing this architecture, Wire Network seeks to make the computing environment as reliable as the blockchain itself, enabling remote measurement of machine state analogous to blockchain state verification. Although this concept has been modeled and the HSM design established, the physical hardware has yet to be built. Future research and development will focus on bringing this from a concept to a live system, further solidifying the network's trustless foundation.

9.4 Consensus Refactoring Wire Network's layer-1 consensus mechanism is major innovation that is a critical component of to network operations, initially described as a combination of Appointed Proof-of-Stake (APoS) and Asynchronous Byzantine Fault Tolerance (aBFT). However, this APoS over aBFT model described herein this paper does not represent the full protection of consensus in the Universal Transaction Layer, given that assets in the UTL benefit from the protection of the consensus mechanisms of the native networks where the assets are located. The combination of Wire's layer-1 consensus and these external networks provides an extra layer of security – tentatively dubbed as *dual consensus* – and this warrants further exploration and refactoring of how we analyze and describe Wire Network's consensus as a whole.

10 Conclusion

Wire Network represents a significant advancement in blockchain technology, introducing transformative solutions to longstanding challenges in the industry. By combining Wire Name Service, our highly-performant layer-1 blockchain, and the Universal Polymorphic Address Protocol, Wire Network is the world's first Universal Transaction Layer. The UTL, through the combination of these technologies, enables seamless and trustless interoperability across multiple blockchains, effectively bridging isolated ecosystems and fostering a more connected and efficient decentralized environment.

Our novel Appointed Proof-of-Stake consensus mechanism enhances decentralization and security by distinctly separating governance, staking, and block production roles. This, coupled with our hierarchical node structure, ensures optimal network performance while minimizing the risk of centralization. The Resource Owners' Association and the Techno Capital Machine further contribute to a robust and sustainable economic model, incentivizing long-term engagement and rewarding contributors across the ecosystem.

Moreover, Wire Network is poised to facilitate mass adoption by addressing critical issues such as scalability, security, and user experience. Our approach to scalability, leveraging both vertical and (in future) horizontal scaling, allows the network to dynamically grow without compromising efficiency. The introduction of the Crypto Single Sign-On simplifies the onboarding process, providing users with a familiar and seamless experience akin to traditional web2 platforms, lowering the barriers to entry for new participants.

As the world moves closer to an Ai-driven future, Wire Network is uniquely positioned to underpin the Ai agent economy. Its high-performance infrastructure, universal interoperability, and unique node structure allowing gas-free transactions make Wire Network an ideal platform for supporting the financial interactions of autonomous Ai agents.

These collective breakthroughs invite the broader open-source community to participate in this exciting journey toward a decentralized, scalable, and Ai-ready future. The immense potential of Wire Network is still unfolding, and future studies will delve deeper into its innovations and potential impact. By pushing the boundaries of what's possible with blockchain technology, Wire Network aims to be at the forefront of the next technological revolution.

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] 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.

[13] 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.

[14] 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.

[15] 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/.

[16] 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.

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

[18] 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.

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

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

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

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

[23] 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.

[24] 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.

[25] Morpheus, Trinity, and Neo, “A Network For Powering Smart Agents,” September 2, 2023. [Online]. Available: https://github.com/MorpheusAIs/Docs/blob/main/!KEYDOCS%20README%20FIRST!/WhitePaper.md.

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

[27] 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.

[28] CTS Labs, "Severe Security Advisory on AMD Processors," March 13, 2018. [Online]. Available: https://safefirmware.com/amdflaws_whitepaper.pdf.

[29] J. Vijayan, "NVIDIA Patches High-Severity Flaws in GPU Drivers," August 11, 2021. [Online]. Available: https://www.darkreading.com/vulnerabilities-threats/nvidia-patches-high-severity-flaws-in-gpu-drivers.