ACORN: PEER-TO-PEER CLOUD SERVICES ON THE ETHEREUM NETWORK

0xMaki and Five
2024.04
v2.0
five@nautilus

ABSTRACT

In the early days of the Internet, people set up home web servers to host their websites. Similarly, in the early days of blockchain, cypherpunks ran nodes to submit transactions to Bitcoin or Ethereum. Blockchain technology is renowned for security, immutability, resilience, and transparency. However, today, we still observe that all Web3 applications heavily depend on centralized infrastructure, posing significant risks due to single points of failure. Centralized vendors and organizations are vulnerable to censorship by governments and make availability of applications a political theater. To address this, we propose leveraging Ethereum's extensive network of nodes to build peer-to-peer cloud infrastructure, including storage, hosting, and computing. This peer-to-peer cloud services would empower developers with the tools necessary to create unstoppable Web3 applications. This paper outlines our plan to build a protocol, network, and platform aimed at enhancing censorship resistance by eliminating centralized infrastructure from Web3 apps and bolstering security of Ethereum through additional incentives to attract diverse network participants. We introduce the Nautilus Network to orchestrate and manage distributed resources, the Nautilus Protocol to incentivize and allocate profits, and the Nautilus Platform to build and scale Web3 applications. The development of peer-to-peer cloud services promises to reignite innovation and creativity within the startup community, unlocking new opportunities for experimentation, collaboration, job creation, and value generation.

1 Introduction

Pioneers like Tim Berners-Lee, who invented the World Wide Web, and Vint Cerf and Bob Kahn, who developed the foundations for the TCP/IP protocols, were the godfathers of early Internet infrastructure that became the backbone of global communication. Their work enabled the seamless exchange of information across different networks, laying the groundwork for the interconnected world we experience today. Similarly, a group of visionaries known as cypherpunks emerged and advocated for the use of cryptography, which became a standard for ensuring privacy, security, and protection of individual freedoms in the digital age. The cypherpunks' ideology influenced pioneers like David Chaum, who developed digital cash concepts, and the pseudonymous Satoshi Nakamoto, who proposed cryptography-based verification of transactions known as the Bitcoin blockchain. Hal Finney, who received the first Bitcoin transaction, also played a crucial role. Collectively, these pioneers contributed to the adoption of blockchain technology, decentralized finance, and Web3 applications. In the early days of blockchain, cypherpunks ran nodes to interact with the blockchain and submit transactions. Perhaps it was the most decentralized and secure time for blockchain. Today, we see that most interactions with blockchains rely on centralized infrastructure and tools such as storage, hosting, APIs, RPCs, databases, identity management services, oracles, messaging systems, and cloud computing platforms.

Recently, we witnessed that Tornado Cash, Coinbase, and Uniswap faced significant challenges due to their reliance on centralized infrastructure. Tornado Cash, a privacy-focused protocol, was sanctioned by authorities, highlighting the vulnerabilities of even decentralized applications when they depend on centralized components. Coinbase, a major cryptocurrency exchange, has faced regulatory scrutiny and outages, impacting users' ability to trade and access their funds. Similarly, Uniswap, a decentralized exchange, has encountered performance issues and censorship concerns due to dependencies on centralized service providers. These incidents underscore the critical need for truly decentralized infrastructure to ensure the resilience, security, and censorship resistance of Web3 applications.

We propose to build a peer-to-peer cloud infrastructure on top of Ethereum's networks to promote security, privacy, immutability, and freedom in digital communications and transactions. A decentralized peer-to-peer cloud infrastructure would significantly improve security, reliability, and immutability of Web3 applications compared to centralized solutions. With data and services distributed across a network of nodes, these systems can operate seamlessly even in the event of node failures or network outages, ensuring uninterrupted access to critical resources. Furthermore, decentralization empowers individuals by granting them greater control over their digital assets and identities through self-sovereign identity systems and decentralized financial services. This empowerment fosters a sense of trust and inclusivity in the digital age, promoting a more equitable and user-centric approach to technology. Additionally, the collaborative nature of decentralized protocols fosters innovation and ecosystem growth by lowering barriers to entry for developers and entrepreneurs, facilitating open collaboration and collective innovation.

Such an infrastructure would consist of three key components: a network, a protocol, and a platform. A decentralized network enhances security by fairly dispersing data and tasks across multiple nodes, making the system less susceptible to single points of failure and cyber attacks. The decentralized peer-to-peer approach ensures resilience and uptime, as no single node can compromise the entire network. A network governed autonomously by a protocol guarantees that control is not concentrated in the hands of a few centralized entities. This protocol facilitates secure transactions, reinforcing trust among participants, and enables seamless interoperability between different systems and applications, fostering innovation and collaboration across the ecosystem. A decentralized platform empowers individuals by providing them with greater control over their personal information and digital assets. It reduces reliance on centralized service providers, thereby minimizing exposure to censorship and data breaches. Such platforms promote user autonomy, privacy rights, and trust in digital interactions. They also encourage the development and deployment of decentralized applications, driving the growth of a robust and resilient digital ecosystem.

2 Nautilus

2.1 Network

In the realm of blockchain-based cloud platforms, the concept of a network emerges as a vital force that connects nodes and forges new pathways within the digital landscape. At its core, a network represents the intricate web of interconnected nodes, each a beacon of computation and communication, collectively orchestrating the symphony of decentralized operations. This network, operating without the shackles of central authority, embodies the essence of decentralization, where power is diffused among the many rather than concentrated in the hands of the few. Here, transactions traverse across this expansive network, validated not by a singular entity but through the collective consensus of its participants, ensuring the integrity and transparency of the distributed ledger.

Within this framework, the utilization of the existing Ethereum network to foster cloud computing capabilities further amplifies the significance of this interconnected infrastructure. It becomes the conduit through which data flows, applications thrive, and innovation blossoms in a borderless digital ecosystem. Comprised of routers, switches, and resilient data centers, this network transcends physical boundaries, enabling users to traverse virtual landscapes and access resources with unprecedented ease and efficiency. It embodies the ethos of accessibility and empowerment, offering a gateway to a decentralized realm where users reclaim sovereignty over their digital lives. Thus, in the fusion of blockchain and cloud technologies, the network emerges not merely as a conduit of connectivity but as the cornerstone upon which the future of decentralized computing is built.

2.2 Protocol

In the intricate tapestry of decentralized cloud computing, the protocol emerges as the guiding compass, delineating the rules and principles that govern interactions among network participants. Within the realm of blockchain, a protocol serves as the bedrock upon which the decentralized network is built, orchestrating the harmonious exchange of data, the validation of transactions, and the attainment of consensus. Much like the veins of a living organism, it ensures the smooth flow of information and ensures the integrity and security of the distributed ledger. Through protocols such as Bitcoin and Ethereum, nodes communicate with precision, executing transactions with transparency, and achieving consensus through democratic validation mechanisms.

Similarly, in the domain of cloud services, protocols play a pivotal role in defining the rules of engagement within the digital realm. Whether it's the ubiquitous HTTP governing web communication or the robust TCP/IP facilitating data transmission across networks, protocols serve as the language through which disparate components of the cloud infrastructure harmonize their operations. They establish the framework for seamless communication, ensuring interoperability and compatibility across diverse systems and platforms. Moreover, these protocols set the stage for fair and equitable participation within the decentralized cloud, fostering an environment where all network participants

operate on a level playing field. In essence, the protocol serves as the guardian of integrity and fairness, safeguarding the decentralized cloud against exploitation and ensuring that the collective aspirations of its participants are upheld.

2.3 Platform

In the dynamic landscape of decentralized cloud computing, the convergence of blockchain technology and cloud services holds immense promise for revolutionizing the way applications are built, deployed, and managed. Leveraging the Ethereum network as a robust foundation, a platform for decentralized cloud computing emerges as a beacon of innovation and empowerment. By building atop a protocol-driven ecosystem, this platform inherits the inherent security, transparency, and resilience of blockchain technology, laying the groundwork for a new era of digital infrastructure.

At its core, this platform offers a fertile ground for developers and entrepreneurs to sow the seeds of innovation. With smart contract functionality as its cornerstone, developers can architect complex decentralized applications (DApps) that operate autonomously, transparently, and securely. By harnessing the power of Ethereum's virtual machine and programming languages like Solidity, developers gain unprecedented flexibility in crafting solutions tailored to diverse use cases. Moreover, the platform provides a rich array of developer tools, libraries, and frameworks, empowering developers to rapidly iterate and deploy their creations with ease.

Beyond its appeal to developers, the platform for decentralized cloud computing holds transformative potential for businesses and organizations seeking scalable, cost-effective solutions. By abstracting away the complexities of traditional cloud infrastructure, this platform offers a seamless experience for deploying and managing applications in a decentralized manner. From scalable compute and storage options to resilient networking and database services, businesses can leverage a comprehensive suite of cloud services tailored to their needs. Furthermore, by tapping into the global network of Ethereum nodes, businesses can access a distributed marketplace of computing resources, unlocking new opportunities for efficiency, collaboration, and value creation. In essence, the platform for decentralized cloud computing stands poised to democratize access to digital infrastructure, ushering in a new era of decentralized innovation and prosperity.

2.4 PoS

Figure 2 analyzes key metrics of the Ethereum blockchain network from July 30, 2015, to May 1, 2024, focusing on the Network Hash Rate, Daily Deployed Contracts, Active Ethereum Addresses, and Daily Transactions. The findings highlight significant trends and transitions within the Ethereum ecosystem, particularly noting the impact of technological shifts and increased user and developer activity. The Network Hash Rate chart demonstrates a substantial increase from 2016, peaking in early 2022. This upward trajectory reflects the growing computational power dedicated to securing the Ethereum network under its Proof of Work (PoW) consensus mechanism. However, a dramatic decline is observed post-2022, coinciding with Ethereum's transition to a Proof of Stake (PoS) consensus. This shift significantly reduced the need for mining, leading to a decrease in hash rate. Notable peaks occur around 2020 and 2021, with deployment rates exceeding 250,000 contracts per day. These spikes correspond to the surge in decentralized finance (DeFi) applications and non-fungible tokens (NFTs), driving increased development activity on the Ethereum platform. Post-2022, while the number of deployed contracts fluctuates, it remains substantial, indicating ongoing developer engagement. The Active Ethereum Addresses chart shows a steady increase from 2018, with significant peaks in 2021 and 2022. This trend signifies growing user interaction with the Ethereum network, aligning with the periods of heightened development activity and the rise of new applications and use cases within the ecosystem. Ethereum Daily Transactions, which also demonstrate a similar upward trend, with peaks corresponding to those observed in active addresses. The transaction volume stabilizes at high levels post-2021, underscoring sustained user engagement and the platform's continued relevance in the blockchain space. The analysis of Ethereum network metrics from 2015 to 2024 reveals significant growth and technological evolution. The transition from PoW to PoS marks a pivotal change, reducing the network's hash rate but aligning with more sustainable blockchain practices. Meanwhile, the substantial activity in deployed contracts, active addresses, and daily transactions underscores Ethereum's robust development and persistent adoption. These findings highlight Ethereum's dynamic ecosystem and its capacity to adapt and thrive amidst changing technological landscapes.

3 Draft

Gamestop blockchain node providers uploading files, retrieving files, and updating file Building Ethereum applications is hard. Apps need to support connecting wallets, multiple chains, signing messages and data, sending transactions, listening for events and state changes, refreshing stale blockchain data, and much more.

Nautilus solves problems such as censorship by focusing on decentralized ethos, developer experience, price, performance, and stability a fundamental principle profit at the expense of The stock price is still up some 1850% from the lows of summer 2020, but the huge gains that seduced so many came in the initial wave. Gamestop hit its peak at the end of January 2021, and since then is down 84%

blockchain and bittorrent were emerged in early 2000s and influenced by similar ideas such as decentralization, peer-to-peer networking, and cryptographic security

blockchains is a distributed ledger technology that enables secure and transparent record-keeping of transactions across a network of computers. It operates on the principle of decentralization, immutability, and consensus, where transactions are recorded in blocks and linked together in a chain using cryptographic techniques.

BitTorrent is a peer-to-peer file-sharing protocol designed for distributing large amounts of data efficiently over the internet. It operates on the principle of decentralized distribution, where files are broken into small pieces and shared among multiple users, enabling faster and more reliable downloads compared to traditional client-server models

The emergence of cloud computing services, akin to AWS and GCP, presents a paradigm shift in how we develop modern applications. Currently, reliance on centralized providers is prevalent, akin to the dependency on financial institutions for electronic payments in online commerce. Despite its functionality, this centralized model is not without its shortcomings, primarily rooted in trust-based mechanisms.

Similar to electronic payments, where intermediaries mediate transactions and increase costs, centralized computing services entail dependency on trusted third parties. This reliance leads to limitations in scalability, transaction sizes, and inhibits the feasibility of small-scale, casual transactions. Moreover, the absence of irreversible transactions and the prevalence of fraud necessitate merchants to adopt stringent measures, impacting user experience and increasing operational overheads.

To address these challenges, an alternative is sought—decentralized computing services operating on cryptographic principles, rather than trust. By leveraging cryptographic proof, such systems enable direct transactions between parties without intermediary intervention. Such transactions, once executed, become computationally impractical to reverse, thereby safeguarding against fraudulent activities. Additionally, the implementation of escrow mechanisms further bolsters security, ensuring buyer protection in transactions.

In this paper, we propose a solution to the challenges of decentralized computing services by introducing a peer-to-peer distributed timestamp server. This server generates cryptographic proof of transaction chronology, rendering them immutable and secure. The efficacy of this system lies in the collective computational power of honest nodes, which surpasses that of any potential attacker nodes, ensuring the integrity and reliability of the decentralized computing ecosystem.

blockchain oracles An oracle network, in the context of blockchain and decentralized systems, serves as a bridge between the blockchain and external data sources. It addresses the challenge of accessing off-chain data (data from the real world or external systems) and bringing it onto the blockchain in a secure and trustless manner

GCP This service adds protection to your data in-use by keeping memory of this VM encrypted with keys

4 Peer-to-Peer Platform as a Service

peer-to-peer network Content identifiers (CIDs) give all files permanent hash address

Data routing and transfer Peer-to-peer network connectivity Interoperability with http

Dynamic naming Define and organize data Universal addressing for data and peers

Store Off-Chain Data in a Decentralized Way

contribute resources, such as storage and bandwidth, to the network sustainability and efficiency of decentralized systems direct payments for hosting or serving content, or through mining rewards for validating transactions or performing other network tasks. PoW and PoS are consensus mechanisms used in blockchain networks to validate transactions and secure the network Participants (miners or validators) are incentivized with cryptocurrency rewards for their computational efforts or for staking their coins to secure the network. Reputation systems track the behavior of participants in the network and assign reputation scores based on their contributions

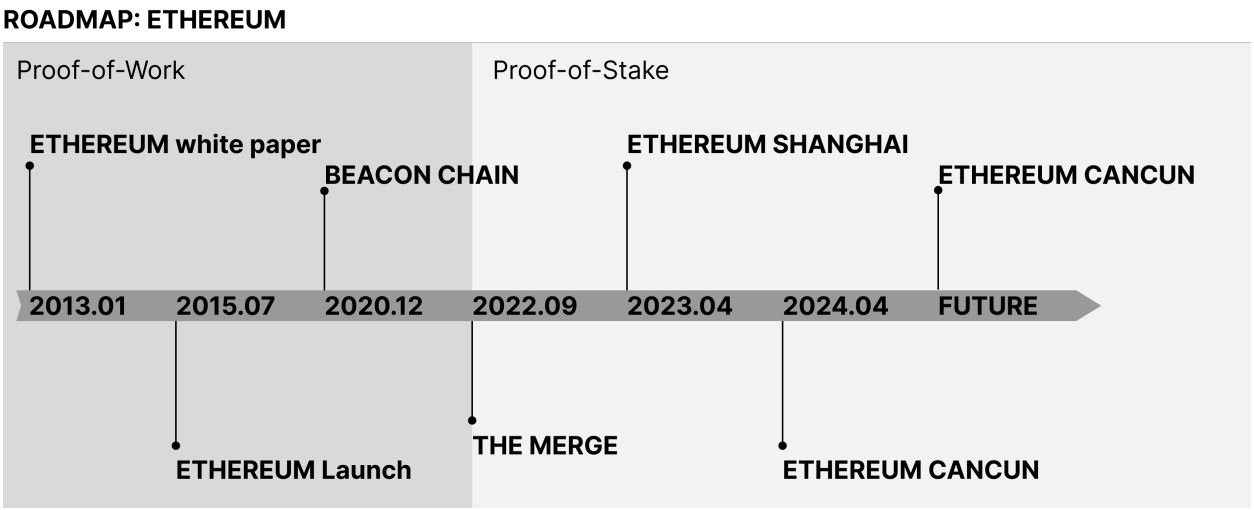

Figure 1: Roadmap: Ethereum

5 Nautilus Protocol

6 Nautilus Architecture

7 Node Validator Platform

python, vyper, flask
javascript, solidity, express

8 Conclusion

In 2008, Satoshi Nakomoto introduced Bitcoin a peer-to-peer payment system that uses cryptography and proof-of-work consensus mechanism to record and secure a public history of transactions [1]. In 2013, Vitalik Buterin introduced the Ethereum blockchain [2], which extended the concept of a peer-to-peer payment system to a new programmable blockchain, allowing for a more complex programmable form of internet money.

In December 2020, the idea of Beacon Chain was introduced to Ethereum to replace Proof-of-Work consensus mechanism with a Proof-of-Stake consensus (See Figure 1). In September 2022, the Merge event, marked the integration of the Beacon Chain into Ethereum's mainnet, transitioning the network from proof-of-work to proof-of-stake. This evolution was a critical step in improving the network's efficiency and scalability. After The Merge, Ethereum's next significant milestone was the Shanghai/Capella upgrade in April 2023. This upgrade deeply improved its network capabilities, particularly with the ability to withdraw staked ETH. This function marked a key step in making Ethereum staking more accessible to the broader crypto community. Anticipated for late 2023 or early 2024, the Ethereum Dencun upgrade is set to bring scalability improvements and new features, building on the progress made by previous updates. A key component of this upgrade is EIP-4844, which will introduce 'blobs'—a new type of transaction on the Ethereum network. This development aims to drastically reduce gas fees by 10 to 100 times, with added scalability. Danksharding is a proposed scalability solution to drastically improve the network's transaction capacity and reduce fees. When fully implemented, Danksharding will take Ethereum's proto-danksharding throughput from 100-10,000 TPS to as high as 100,000 TPS.

Acknowledgments

This work was supported in part by Heroglyphs team.

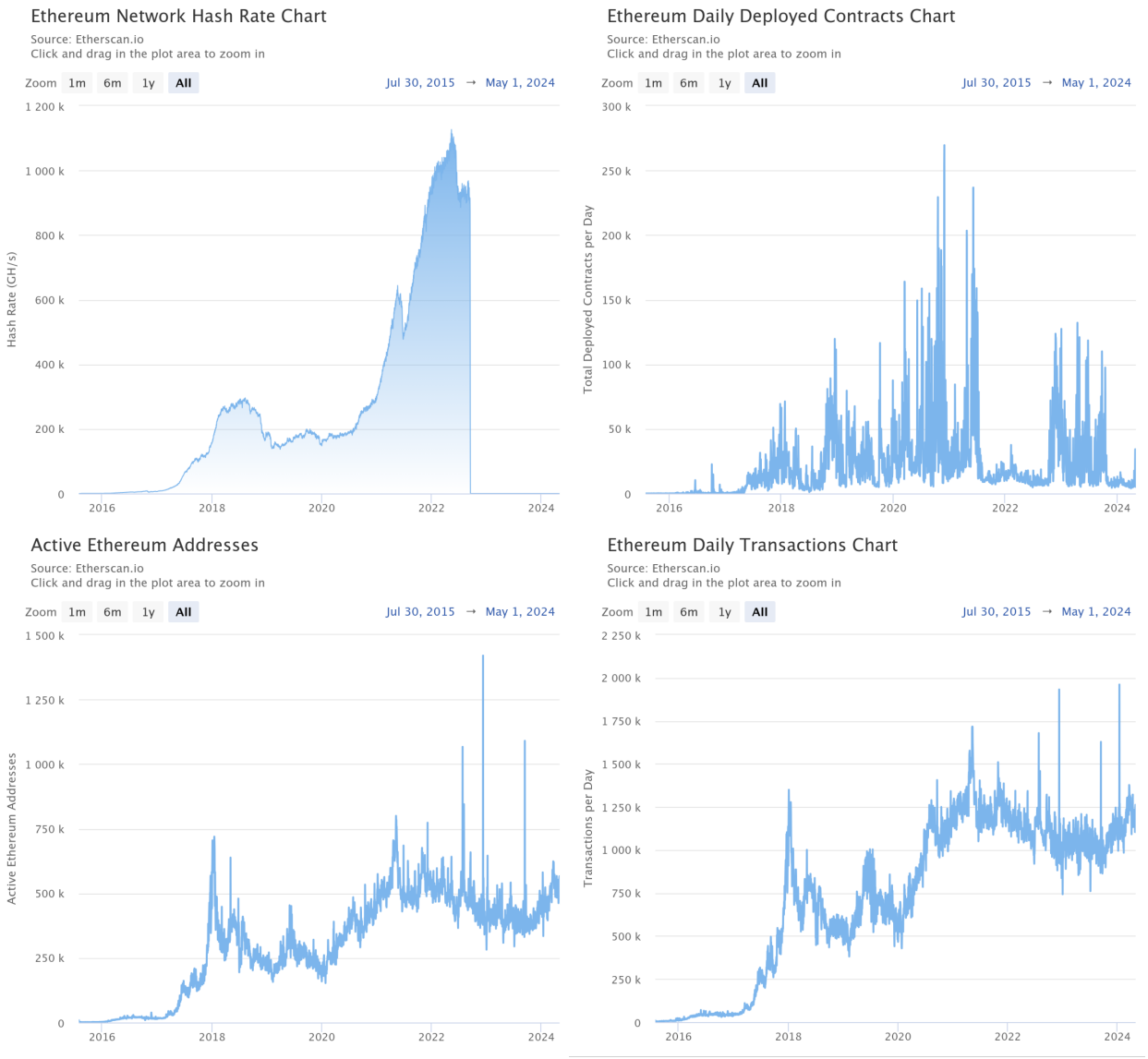

Figure 2: Ethereum Statistics: Network Hash Rate, Deployed Contracts, Active Ethereum Addresses, and Daily Transactions

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *online*, 2008.

[2] Vitalik Buterin. Ethereum whitepaper. *online*, 2014.

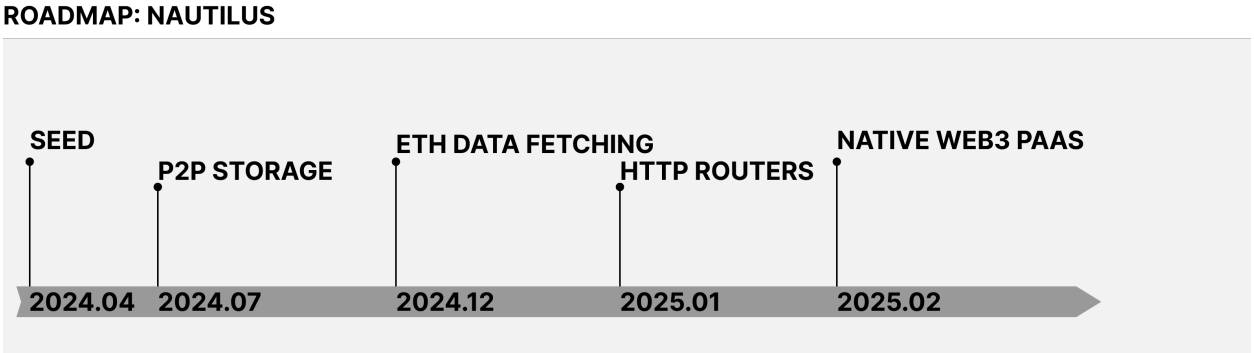

Figure 3: Roadmap: Nautilus

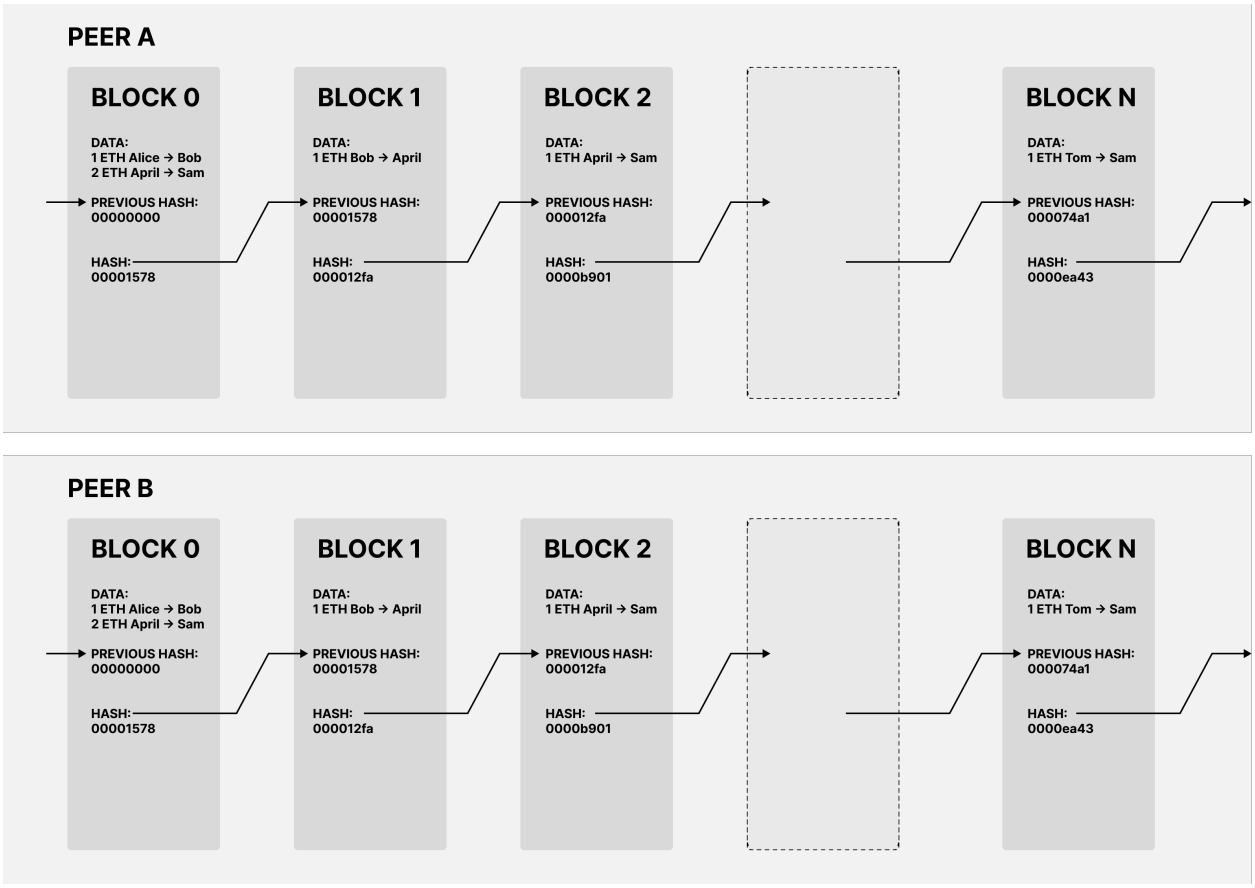

Figure 4: Peer-to-Peer Platform as a Service

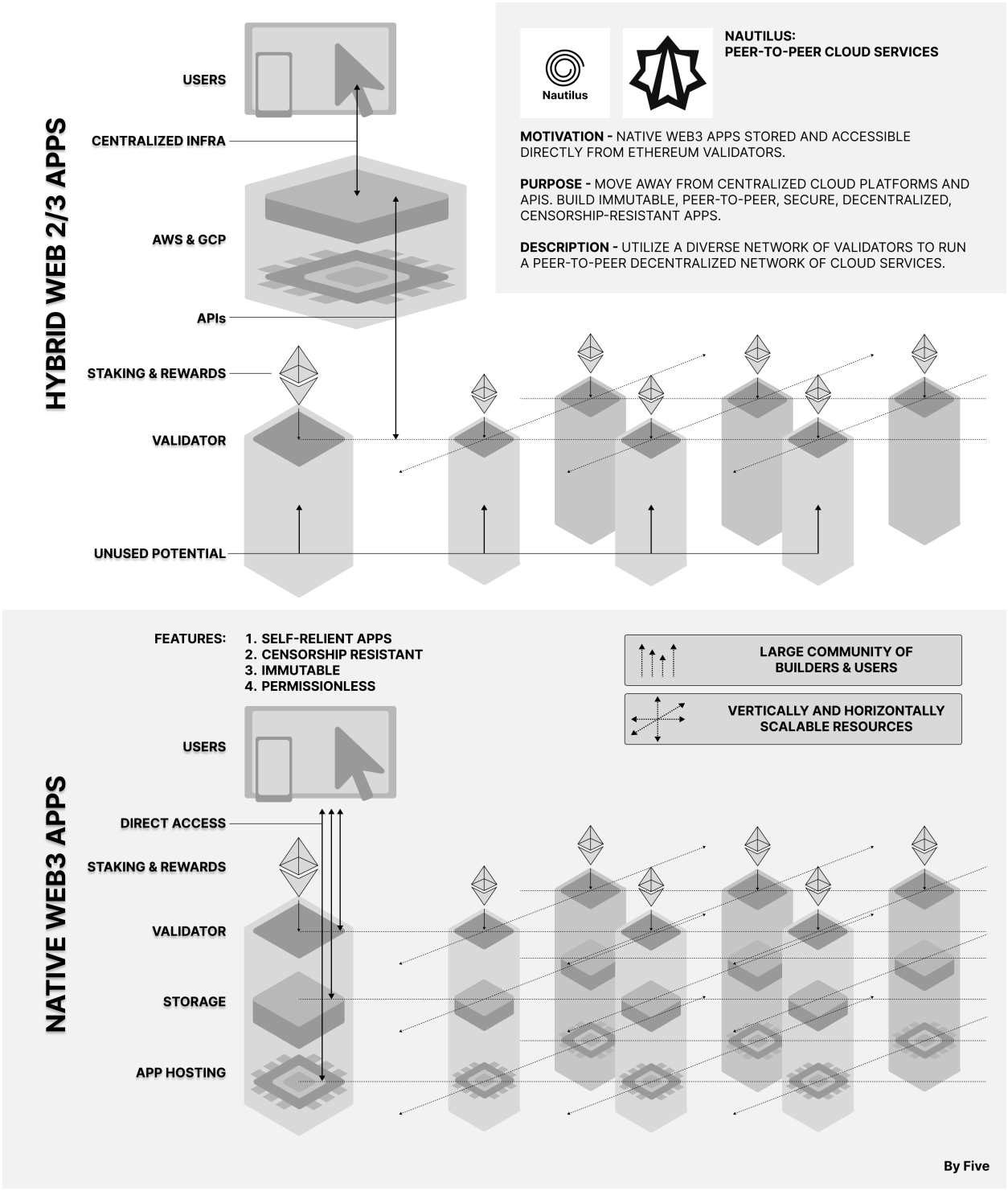

Figure 5: Blockchain explained.

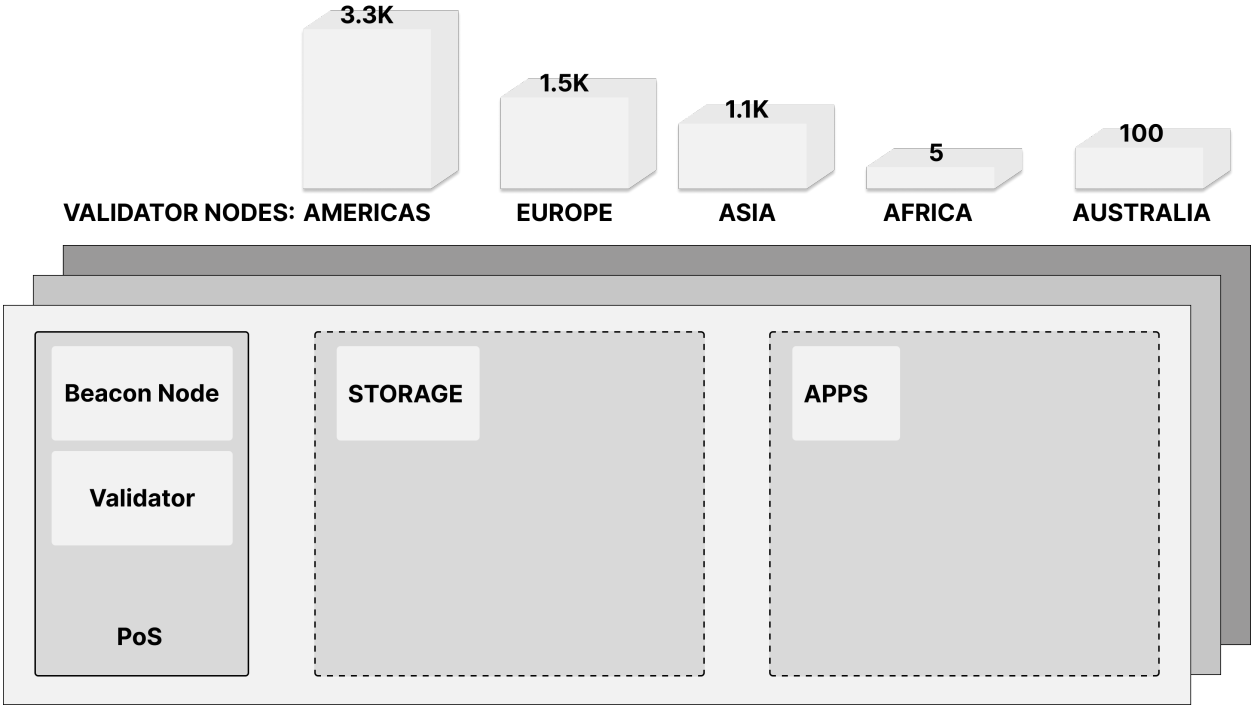

Figure 6: Ethereum Nodes as Platform-as-a-Service.