Blockchain Focus

SBC ‘24 Takeaways : Aiming To Solve Real World Problems

Aug 16, 2024
Jaehyun Ha | Research Analyst
jaehyunha@prestolabs.io

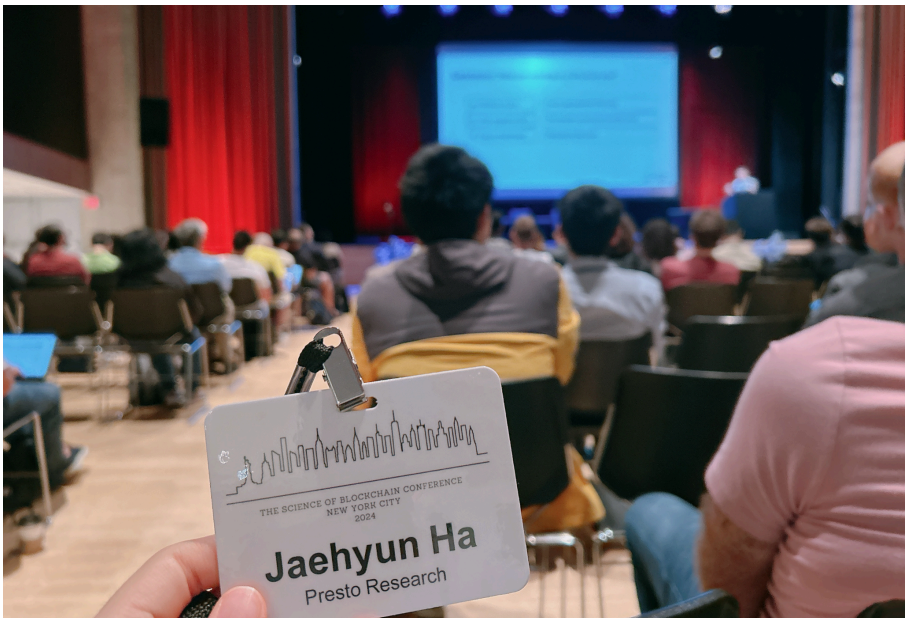
Summary

- The Science of Blockchain Conference 2024 (SBC’24), held in NYC, demonstrated a shift compared to the previous year, with a focus on implementing evolving cryptography theories into practical protocols and addressing real-world problems related to our daily lives.

- For ZK-related technologies, whose cryptographical basis have been in development for several years, there is now a growing emphasis on understanding their security (i.e., understanding security vulnerabilities in SNARKs) and exploring how their practical applications (e.g., zkLogin) can improve user experiences.

- In the area of blockchain consensus, there was a noticeable trend toward tackling current challenges faced by the blockchain industry, such as decentralized sequencing network from Espresso and re-staking from EigenLayer. The discussions on the DeFi sector included many interesting topics, such as reducing the liquidity needs in the current financial systems.

Figure 1 : SBC’24 Main Event (Columbia University)



Source: Presto Research

Introduction

The Science of Blockchain Conference 2024 (SBC'24), held in New York City from August 5th to 9th, brought together leading minds in academia and industry to explore the latest advancements in blockchain technology. The main event took place at Columbia University from August 7th to 9th, accompanied by various side events across the city during the entire conference period. Presto Research participated in the main conference and attended key sessions on "The Science of Proof: Client-Side Proving" and "Science and Engineering of Consensus". This article explores cutting-edge innovations and emerging trends that were highlighted at SBC'24.

Trend Shifts from Last Year (SBC'23)

The programs at SBC'24 were significantly restructured compared to last year (SBC'23). The most noticeable changes were in the categories of ZK, Consensus, and DeFi. These topics are individually explored in the following section.

Figure 2 : Trend Shifts from SBC'23

Categories	SBC'23/24	Programs
ZK	SBC'23	HyperNova: Recursive arguments for customizable constraint systems
		Protostar: Generic Efficient Accumulation/Folding for Special Sound Protocols
		Future directions in STARKs
	SBC'24	SoK: What don't we know? Understanding Security Vulnerabilities in SNARKs
		zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials
Consensus	SBC'23	Time is Money: Strategic Timing Games in Proof-of-Stake Protocols
		Goldfish: No More Attacks on Proof-of-Stake Ethereum
		Designing a DV Protocol for Decentralized PoS Consensus
	SBC'24	The Economic Limits of Permissionless Consensus
		The Espresso Sequencing Network: HotShot Consensus, Tiramisu Data-Availability, and Builder-Exchange
		Strong Cryptoeconomic Security for Arbitrary Validation Tasks
DeFi	SBC'23	Automated Market Making and Arbitrage Profits in the Presence of Fees
		Finding the Right Curve: Optimal Design of Constant Function Market Makers
	SBC'24	Suboptimality in DeFi
		Cycles Protocol: A Peer-to-Peer Electronic Clearing System

Source: The Stanford Center for Blockchain Research

Takeaway #1: Growing Interest in the Security and Applications of ZK

First topic to address is the growing interest in the security and applications of Zero-Knowledge (ZK) technology. While the emphasis in previous years, particularly at SBC'23, was on the development of more **advanced proof systems**—highlighting papers like Hypernova and Protostar—this year's conference saw a pivot towards the **security and practical applications** of ZK. When attention moves from pure development to security and application, it typically signals that a technology is on the brink of broader adoption. This shift suggests that ZK technology has reached a level of maturity (though there's still a space to improve), making it more viable for real-world implication. Two representative papers from SBC'24 illustrate this trend:

SoK: What don't we know? Understanding Security Vulnerabilities in SNARKs

This survey paper, written by ***Stefanos Chaliasos et al***, provides a detailed analysis of 141 vulnerabilities found in SNARK (Succinct Non-Interactive Argument of Knowledge) systems, categorizing them across different layers of the SNARK stack. These vulnerabilities were classified into four main layers: Circuit, Frontend, Backend, and Integration. The majority of vulnerabilities were found in the Circuit layer, where common issues included under-constrained circuits, which can lead to a verifier accepting invalid proofs, and computational errors, where incorrect implementation of circuit logic leads to completeness or soundness issues. In the Frontend and Backend layers, vulnerabilities often arose from incorrect constraint compilation, witness generation errors, and unsafe verifier implementations, which could compromise the entire proof system's security.

The paper also introduces a taxonomy to classify these vulnerabilities, focusing on the root causes and their impact on system security. For instance, in the Circuit layer, vulnerabilities were classified into categories such as "Under-Constrained" (where constraints are insufficient, allowing invalid proofs), "Over-Constrained" (where valid proofs are rejected), and "Arithmetic Field Errors" (issues arising from finite field computations). In the Integration layer, vulnerabilities were often linked to poor interaction between the application logic and the SNARK components, such as "Proof Delegation Errors" and "Passing Unchecked Data," which could lead to soundness or completeness failures. The authors also emphasize the challenges developers face due to the low-level nature of SNARK tools, which contribute to the prevalence of these vulnerabilities.

zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials

zkLogin, also known as ***Sui*** primitive, addresses the current problem in existing wallet authentication methods, particularly those used in blockchain systems. Traditional methods, such as mnemonic phrases or hardware wallets, are often cumbersome for users, leading to difficulties in user onboarding and broader adoption of blockchain technology.

The zkLogin system solves these problems by introducing a novel method that leverages existing identity tokens issued by widely used platforms like Google and Facebook to authenticate blockchain transactions. This approach allows users to use their existing OpenID accounts for blockchain authentication without needing to remember new secrets or rely on additional trusted entities. The core innovation of zkLogin is the use of Zero-Knowledge Proofs (ZKP) to ensure that the link between a user's off-chain identity (like an email) and their on-chain identity remains hidden, even from the platform itself.

Takeaway #2: Next Step After Refining PoS

The next noteworthy aspect is the shift in trends within consensus-related research. While most consensus research up until last year focused on making **improvements in PoS protocols**, this year's trend centered on how to design protocols with more robust cryptoeconomic security, or how to solve the centralization issues in rollups. In other words, the focus has shifted towards **better utilizing and optimizing the existing PoS protocols**. Here are two presentations worth highlighting:

The Espresso Sequencing Network: Hotshot Consensus, Tiramisu Data-Availability, and Builder-Exchange

This paper, proposed by ***Espresso systems***, claims that a ***shared*** decentralized sequencing network among rollups is essential because it addresses the limitations of existing implementation, which suffer with centralization issues and are infeasible to achieve the robust economic security as Ethereum. Additionally, the lack of interoperability between rollups leads to fragmented user bases and liquidity, further centralizing economic power due to exclusive cross-chain arbitrage opportunities.

Espresso sequencing network solves these problems through a protocol design consisting of three core components: The *HotShot Consensus layer*, The *Tiramisu DA layer*, and The *Builder-Exchange* protocol. First users generate transactions that are sent to a public or private mempool, from which builders create and order these transactions into blocks. The HotShot Consensus layer, a leader-based Byzantine Fault Tolerant (BFT) protocol, facilitates the sequencing of these transactions without executing them, while the Tiramisu DA layer ensures the availability and retrievability of the data. The Builder-Exchange protocol manages the secure and fair exchange of block content between builders and the consensus network, ensuring that blocks are committed to the chain without compromising data integrity or security. The network interacts with Layer-2 rollups and the Layer-1 blockchain to maintain a consistent and secure ledger state, enabling seamless cross-rollup transactions and state updates.

Strong Cryptoeconomic Security for Arbitrary Validation Tasks

This talk by ***Sreeram Kannan, the founder of EigenLayer***, discusses *"How do we extend the cryptoeconomics to any intersubjectively attributable fault without forking the chain?"* with EIGEN token. The EIGEN token addresses the challenge of intersubjectively attributable faults—errors in digital tasks that cannot be proven mathematically on-chain but can be widely recognized and agreed upon by observers outside the blockchain. To solve this, EIGEN enables staking within Actively Validated Services (AVSs), where the token is used to secure services against these faults. When faults occur, EIGEN stakers who are found to be dishonest can be penalized through mechanisms like slashing, which removes their stake, and token forking, which allows the community to create a new token fork that excludes the malicious actors. This approach prevents the tyranny of the majority and maintains system integrity. The four key features of EIGEN staking include *universality*, where the token can be used across various tasks and services; *isolation*, which protects non-staking uses of the token from the effects of potential forks; *metering*, which involves requiring bonds to deter frivolous or malicious challenges; and *compensation*, ensuring that any users harmed by malicious activity are compensated, thus reinforcing the overall cryptoeconomic security of the system.

Takeaway #3: More Efficient DeFi

The last (but not least) noteworthy point is the increased depth and diversity of research in the DeFi sector. While Automated Market Makers (AMMs) and Central Limit Order Books (CLOBs) have traditionally dominated the field, this year saw the introduction of new research topics, such as the suboptimality of DeFi systems and the implementation of monetary policy using blockchain technology—areas that have not been commonly explored before. Here are brief summaries of two relevant research projects:

Suboptimality in DeFi

This paper written by ***Aviv Yaish et al.*** makes contributions to understanding suboptimal behavior in the decentralized finance (DeFi) ecosystem, focusing on three core primitives: collateralized lending, flashswaps for arbitrage, and flashswap-based liquidations. The authors demonstrate that users and automated tools frequently act suboptimally, missing substantial profit opportunities, sometimes exceeding 700% in potential gains. They formalized the optimization problems for each primitive to identify the optimal execution strategies, and conducted a longitudinal study which revealed over $4 million in lost profits due to suboptimal arbitrage. Additionally, the paper uncovers potential miner-extractable value (MEV) exploitation, where miners might be using inside information from private transaction relays to gain a competitive edge, marking the first documented instance of such behavior. The findings highlight the need for more efficient tools and practices in DeFi to mitigate suboptimal actions and enhance profitability.

Cycles Protocol: A Peer-to-Peer Electronic Clearing System

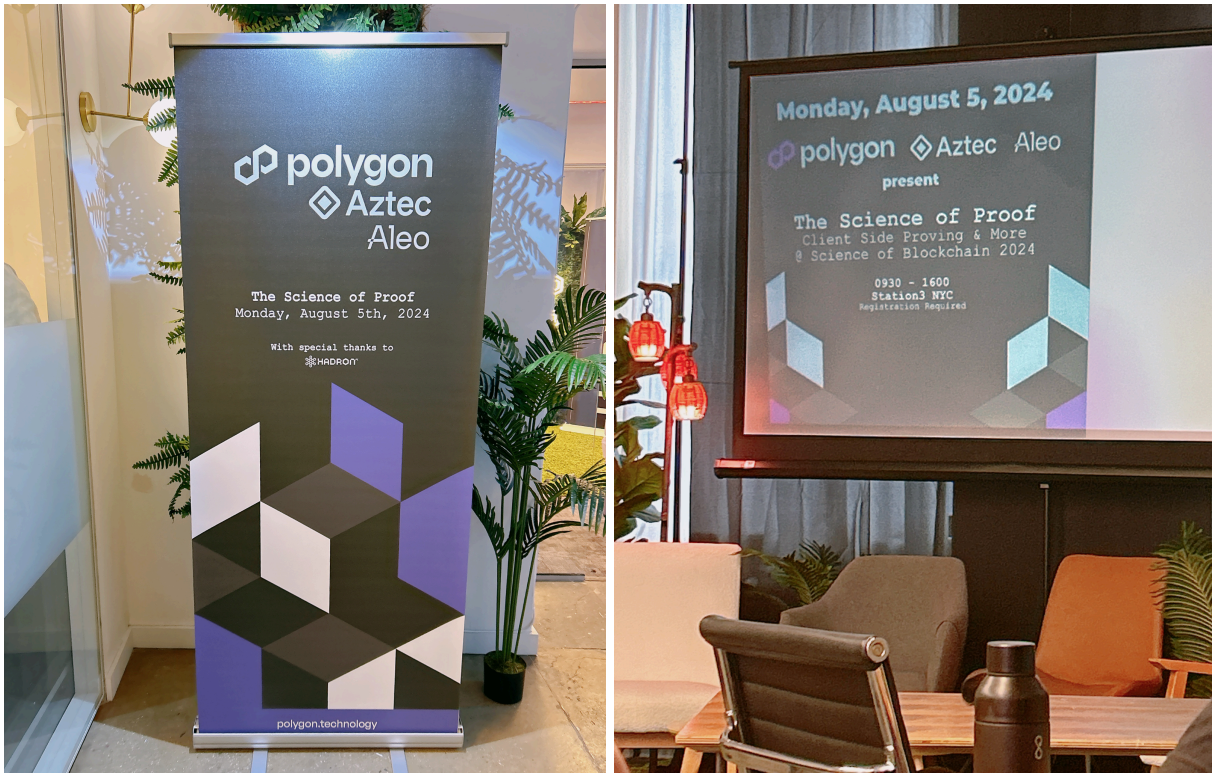
This talk by ***Ethan Buchman, founder of Informal Systems,*** introduces the Cycles Protocol, which is a blockchain protocol designed to reimagine monetary policy and the foundational structures of financial transactions. Unlike traditional DeFi models that focus on refining mechanisms, Cycles addresses the inherent flaws and inefficiencies in the current financial system by reducing liquidity requirements, simplifying compliance and accounting, and increasing transparency. By leveraging obligation clearing and mutual credit, Cycles offers a solution that protects small and medium-sized enterprises from liquidity-induced bankruptcies, fostering a more resilient and equitable financial ecosystem.

Cycles tries to solve the problem of liquidity constraints in financial transactions by enabling a network where debts can be settled without traditional intermediaries. Through obligation clearing, Cycles claims that businesses can directly exchange goods and services, with debts automatically cleared via connected transactions, reducing the need for cash and banks. Additionally, the integration of mutual credit within the protocol allows participants to extend credit to each other, which can hopefully lower the liquidity needs. *“An open clearing protocol with payments and finance engine to clear the most debt, for the most people, with the least amount of money, from the most preferred sources”*, Buchman quoted.

Side events

“The Science of Proof: Client Side Proving (CSP),” hosted by Polygon Labs, featured an excellent session on both theoretical research and practical implementation in the CSP field. Core developers from Polygon Miden, Aleo, and Aztec participated in a panel discussion on designing state models to make private execution more practical. Additionally, several CSP projects showcased their work and provided demos, illustrating how CSP developments are progressing and how users can benefit from these advancements.

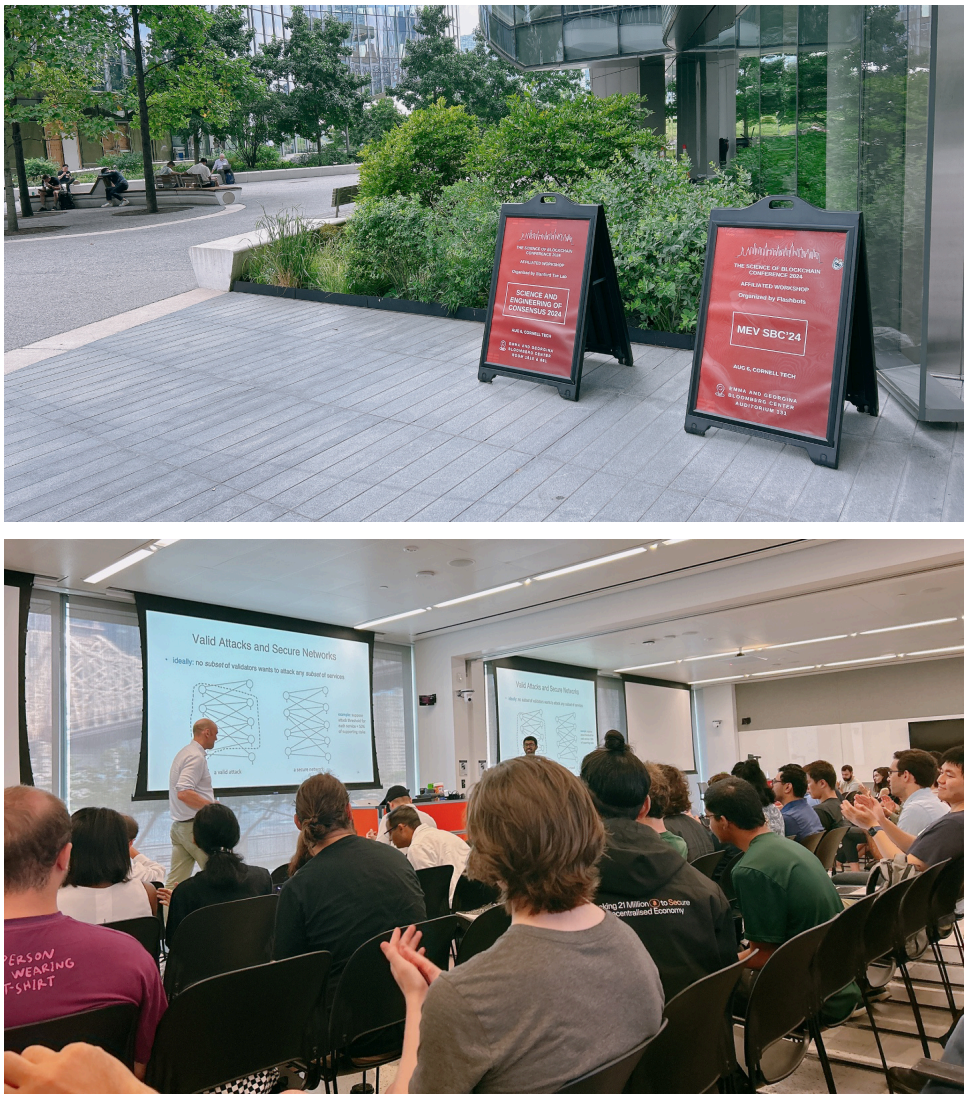
Figure 3 : The Science of Proof - Client Side Proving by Polygon Labs (Station 3, NYC)



Source: Presto Research

The “Science and Engineering of Consensus” session, hosted by TseLab (led by Professor David Tse of Stanford University), featured another outstanding session focused on theoretical research in the blockchain consensus field. This year’s event primarily covered topics such as secure staking/restaking, DePINs, TEE, and high-throughput consensus in realistic network environments. The presentation by Professor Tim Roughgarden (Columbia University, a16z crypto), “How Secure Is Your Restaking Network?” was particularly insightful, as it was the first research exploring how to define and design a secure restaking network. Additionally, Professor David Tse’s talk on “Bitcoin Staking” provided valuable insights into the implementation of a trustless Bitcoin staking protocol.

Figure 4: Science and Engineering of Consensus 2024 (Cornell Tech)



Source: Presto Research

Conclusion

SBC'24 was an outstanding event that provided researchers with invaluable experiences and opportunity to learn about the trends currently prioritized in academia and industry. While top-tier blockchain conferences like FC, AFT, and security-focused conferences such as IEEE S&P (Oakland), USENIX, ACM CCS, and NDSS already exist, SBC'24 offers a unique charm; it creates an environment where even unpublished papers or ongoing research can be freely presented and discussed. The key insights from the side events will soon be shared as part of Presto Research's content. Stay tuned!

About Presto

Presto is a Singapore-based algorithmic trading and financial services firm founded in 2014. Presto focuses on delivering exceptional value for clients through a rigorous research-driven approach to investment and trade execution. With more than a 100 million trade executions in a day, Presto is a leading financial services firm in both digital assets and traditional finance markets. Presto Research is a research unit within Presto.

Find out more at https://www.prestolabs.io.
Follow Presto for more content: X, LinkedIn
Follow Presto Research for latest research : X, Telegram

Authors

Jaehyun Ha, Research Analyst
X, Telegram, LinkedIn

Required Disclosures