Breakfast
7:30 - 8:30

Keynote: Proof of Entropy Minima

09:00 - 10:00
Dr. K, Dominant Strategies
Abstract: Nakamoto consensus has been incredibly influential in enabling robust blockchain systems, and one of its components is the so-called heaviest chain rule (HCR). Within this rule, the calculation of the weight of the chain tip is performed by adding the difficulty threshold value to the previous total difficulty. Current difficulty based weighting systems do not take the intrinsic block weight into account. This paper proposes a new mechanism based on entropy differences, named proof of entropy minima (POEM), which incorporates the intrinsic block weight in a manner that significantly reduces the orphan rate of the blockchain while simultaneously accelerating finalization. Finally, POEM helps to understand blockchain as a static time-independent sequence of committed events.

Coffee Break
10:00 - 10:30

On the Impossibility of Forging Illegitimate Proofs of Membership in Merkle Patricia Trees

10:30 - 11:00
Jérémie Albert, inBlocks and Serge Chaumette, Université de Bordeaux
Abstract: The value of an asset often depends on the capability we have to demonstrate its existence at a certain date. Blockchains provide such a service but they tend to be expensive if used intensively. Multilevel ledgers exist that make is possible to cache the operations and thus to reduce the cost of use but not many (if any) have provided proofs that they do not put at risk the assets they register. Therefore the goal of this paper is to demonstrate in an understandable and convincing manner that the so called Precedence multilevel ledger that we have developed at inBlocks does not impair the assets entrusted to it.

Fuzzing for Smart Contract Interworking Security Evaluation: An Empirical Evaluation of the State of the Art

11:00 - 11:30
Simone Zerbini, University of Padua
Abstract: The development of smart contracts offers various features and solutions to end users, including transparency, immutability, and more. These contracts play a pivotal role in the creation of various decentralized applications, such as DeFi platforms, and have shown tremendous growth with large sums of money being circulated. With their widespread adoption, various vulnerabilities have arisen, posing serious security concerns and leading to significant financial losses. To address these issues, several research studies have been conducted, and different testing methodologies have been utilized to identify and resolve these vulnerabilities. In this paper, we explore one such testing method, known as fuzzing, for discovering vulnerabilities in smart contracts. Our research undertakes a comprehensive investigation of modern fuzzing tools, emphasizing their ability to analyze interacting contracts and handle complex contract deployment steps. These features are crucial for the proper analysis of large, multi-contract projects, which are becoming increasingly common in the Web 3.0 technology landscape. This research highlights the effectiveness of these tools and their capacity to analyze large, multi-contract projects, while also shedding light on their limitations.

Invited Talk: Velocity: Scalability Improvements in Block

Propagation Through Rateless Erasure Coding

11:30 - 12:00

Hans Behrens, Topl Labs

Abstract: Blockchain technology and other distributed ledger systems fill an important role in resilient data storage and publication. However, their normally-decentralized methods also bring unique challenges distinct from more traditional approaches. One lies in the replication of data between participating nodes; since no individual node is more trusted than any other, each node maintains its own copy of the entire ledger for the purposes of validating new transactions. Improving how this information is stored and more importantly, how it propagates across the network, are open research questions. In this work, we propose Velocity, a novel block propagation approach based on fountain codes, allowing for better decentralized delivery of blocks and reduced network bottlenecks without sacrificing the security guarantees of the blockchain ledger itself. We also provide an assessment of economic incentives and their impact on participant behavior, showing that the proposed approach is financially beneficial to rational actors. We conclude by showing experimentally that this approach permits for the mining of even larger blocks, thereby increasing transaction throughput of the system compared to existing state of the art methods.

Lunch

12:00 - 13:30

Discussion Panel: The State of Blockchain Security

13:30 - 14:30

Various Speakers

Invited Talk: Bayesian Analysis of Nakamoto Proof of Stake

14:30 - 15:00

James Aman, Rice University

Coffee Break

15:00 - 15:30

Networking Time

15:30 - 17:00