WEB3SEC Preliminary Program

The inaugural WEB3SEC workshop will be held Monday, December 5, 2022, in conjunction with the Annual Computer Security Applications Conference (ACSAC). ACSAC will be held at the AT&T Conference Center in Austin, Texas.

Opening Keynote 09:00 - 10:15

TBD

Coffee Break *10:15 - 10:45*

Embedding Reverse Links in a Blockchain 10:45 - 11:15

A. W. Roscoe, Oxford University

Abstract: Blockchains provide extremely simple certainty looking backward in time because of the way each block contains a hash of its predecessor. This is not possible in the same way looking forward in time for various reasons, not the least of which is that when block N is created, block N+1, and thus its hash, are unknown. Therefore blockchains rely on more complex mechanisms to establish what the successor of any given block is, and to ensure that alternatives - known as forks - cannot be introduced either close to the time of its creation or long after. These typically rely on chains of dependency and PKIs. In this paper we show how the concept of hooks can create something closely analogous to the usual hash links, only in the other direction. These represent a powerful mechanism to counteract attempts to insert forks from relatively old blocks, and are entirely internal to the blockchain. In understanding hooks we do some detailed combinatorial analysis of the game that good and bad agents play in blockchains, introducing criteria for relatively small collections of agents to make decisions, up to stochastic certainty.

A Survey on Quantum-safe Blockchain Systems 11:15 - 11:45

Swathi Punathumkandi, Arizona State University

Abstract: Despite Blockchain technology being widely recognized for the near future, some of its components are being challenged by another incoming technology, Quantum Computing. Quantum - safe -Blockchain is quickly becoming one of the most essential future-proof blockchain designs. Because of the novelty and promise of this new technology, Quantum blockchain has a significantly greater scope than cryptocurrencies and cross-chain asset transactions. The majority of today's cryptography algorithms will be susceptible to quantum attacks. In this paper, a comprehensive literature review is performed by considering some research questions such as where, how, and what effect quantum computing will affect the classical blockchain mechanism. The survey is completed by responding to the research questions and highlighting research gaps.

Lunch *11:45 - 13:30*

Verification and Validation of Educational Documents Using Blockchain 13:30 - 14:00

Shubham Deshmukh, MIT Academy of Engineering

Abstract: With the increasing popularity of image and document manipulation software like Adobe Photoshop and GNU Image Manipulation Program (GIMP), it is increasingly becoming hard to know the credibility of some documents submitted by someone. This paper shows how credible sources like universities can control the authenticity of the documents provided by their students by hosting the documents in a blockchain with InterPlanetary File System as a storage solution and can be accessed by anyone anywhere with proper credentials. Verification and validation of documents are time-consuming and difficult for the organizations and institutions which can be overcome with the help of our work. Our work will contribute to the secure storage of the documents.

IoT Device ID Management Over Hyperledger Fabric 14:00 - 14:30

Anil Kumar, Arizona State University

Abstract: With a surge in demand for IoT products and most IoT end markets, IoT Analytic anticipates the chip shortage to have a long-term impact on the number of connected IoT devices. The Internet of Things industry is estimated to expand by 18 percent to 14.4 billion active connections in 2022. It is predicted that there will be around 27 billion linked IoT devices by 2025, as supply restrictions ease and demand increases. The majority of these devices are deployed in diverse and complex networks, posing several problems to the device management functions. One of these problems is identity management, which is concerned with how devices' identities are reconciled and confirmed, as well as how devices construct the methods for authorizing and managing access to its data and services. Blockchain, being a distributed ledger technology, promotes itself as a viable solution to the problem of Identity management. This is mostly due to Blockchain providing record immutability, cryptographical IDs, and data provenance. These capabilities, when combined, provide a foundation for implementing IoT device identity management services that may assure a worldwide and unique identity for the devices, as well as a means to preserve it over the device life cycle. Our work describes a decentralized Hyperledger fabric-based IoT identity management platform that includes features such as data collection from the manufacturer itself, ownership transfer, identity generation and detecting device anomalous operational state.

Invited Talk 1: Selected Topics in Zero Knowledge 14:30 - 15:00

Yupeng Zhang, Texas A&M University

Coffee Break *15:00 - 15:30*

Invited Talk 2: Regularized Proof of Stake 15:30 - 16:00

Aaron Schutza, Topl Labs

Closing Session 16:00 - 17:00

TBD