2020-08-05

Attendees (28)

Anshu Jain

Jim Mason

Nir Steinherz

James Dzierzanowski

Clive Boulton

Vipin Bharathan

@Rebecca Aspler

Alfonso Govela

@Andrew Park

Anshu Jain

@ Phillip Long

@Bart Cant

Daniel Bachenheimer

@Eric Holst

Harris Niavis

@Hriday Tiwari

James Dzierzanowski

Jim Mason

@Jonathon Holt

@Juan Caballero

Kamlesh Nagware

Kent G Lau

Lindsay Nuon

Mohan

Moushmi Banerjee

Nir Steinherz

@Roland - Areosurete

@Stephane Mouy

Meeting on the zoom channel is https://zoom.us/my/hyperledger.community

Antitrust Policy and introductions - VB duration-depends on participation

Main Event: **IoT Security Enabled by MPC** by Rebecca Aspler, Director Product Management UnboundTech.

While the benefits of IoT are unlimited, the reality is that the proliferation of blockchain based connected devices, systems and services that compose the IoT ecosystem has introduced risk directly into the physical world, blurring the border between virtual threats and utilities, devices and critical infrastructure. In this session, we will discuss how MPC can be used to enable every IoT device to have an embedded root of trust, while preserving the zero-knowledge proof of other devices' data. Furthermore, we will examine a few use cases, some that can be associated with a public blockchain and some that are more common within the boundaries of a permissioned blockchain.

- Ideas for Future talks (please add suggestions with contact)
    - EBSI and eIDAS, and integration into the open platform. More on this topic.
    - Discussions on Identity as seen by the state vs across regions and internationally and how that helps stitch together the blockchain infrastructures, in terms of trust, KYC etc.. Refer to FATF.
    - Further on TOIP
    - NIST 800-63: https://pages.nist.gov/800-63-3/sp800-63-3.html Call For Comment https://csrc.nist.gov/publications/detail/sp/800-63/4/draft
    - ID2020: Why is it important? Financial and societal inclusion through Digital Identity and SDGs.

Recordings

Video

Audio

Notes

IoT Blockchain E...abled by MPC.pdf

Extensive presentation covering all aspects of MPC and its advantages; Unbound's role in innovating the solution.

Qs:

1.Recovery of keys due to device loss etc. : Done through key rotation and refresh in seconds (we have to look closer at the protocol)

2. Disconnected settings (i.e. IoT device is unreachable)? - can proceed with a quorum, but there could be some other protocols with a quorum of connected devices.

3. Difference between Multi-Sig and MPC - Multi-Sig needs sophisticated smart contracts; MPC constructs the signature outside the venue.