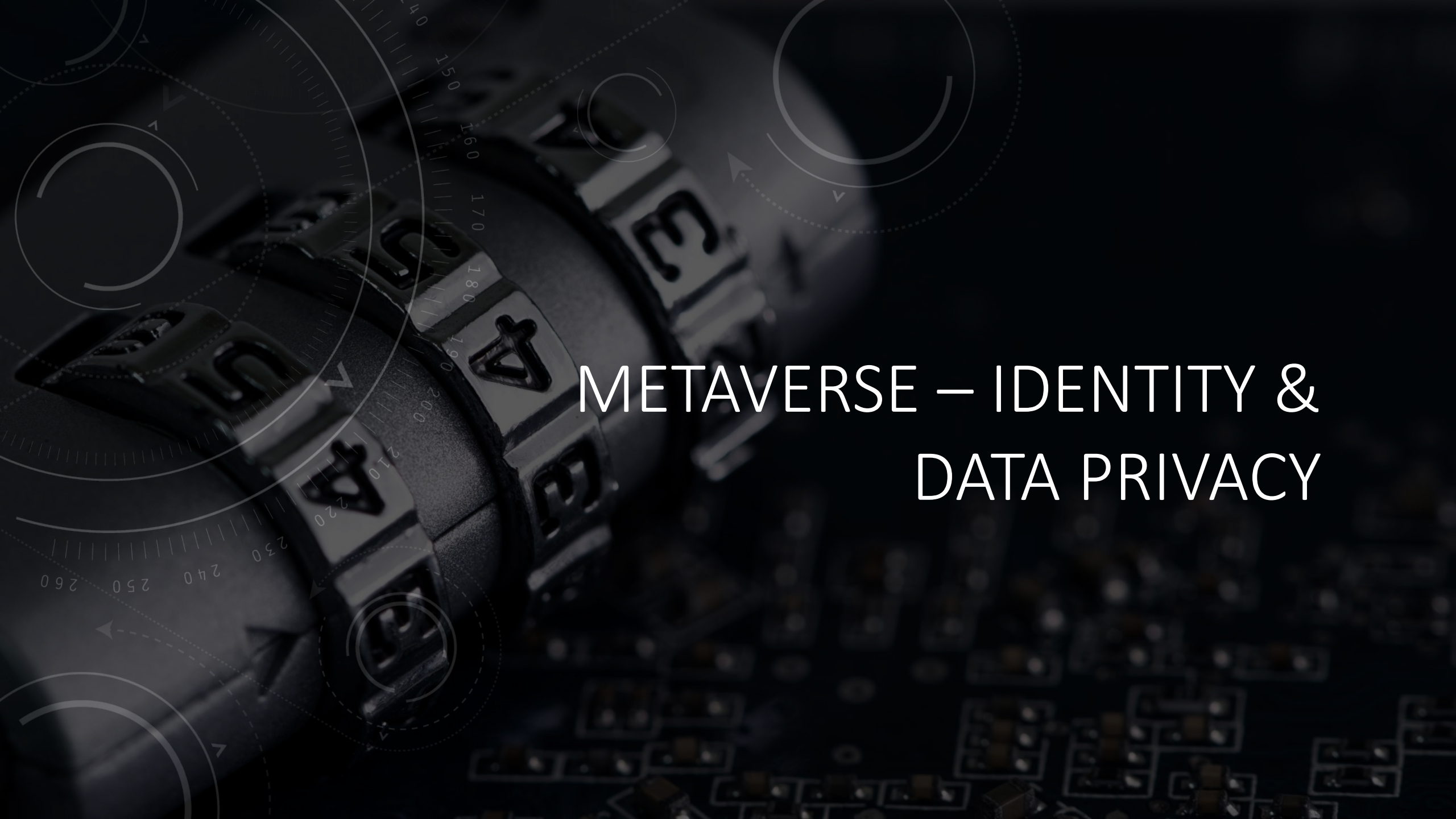


METAVERSE – IDENTITY & DATA PRIVACY

Identity & Data Privacy in the Metaverse

- **Understanding Identity in the Real World**
  - Authentication versus Authorization
  - What is identity in real world?
  - Various ways a person or system is authenticated in physical and digital worlds
- **Understanding Identity in the Metaverse**
  - How can you identify someone or something in a virtual world?
  - Data Privacy in virtual worlds and correlation to real world IDs
  - Trust is virtually impossible in the virtual worlds (Unless the programs can trust each other, AND under a governance system, which brings us to Decentralized Identity, SSI & ToIP)

IDENTITY IN THE REAL WORLD

Samantha can interface with her bank in multiple ways – in person, from a kiosk or a personal device such as a computer or a mobile device

- **Who is Samantha?**
  - Check Driver's License and verify based on appearance and stored personal info
  - Ask for SSN/SIN/Aadhar Card etc.
  - User's login credentials (things such as password, PIN or Biometrics)
  - OAuth, JWTs and Open ID Connect allows systems to establish authentication
  - Use of certificates provided by identity verifier
    - PKI Certs
    - X509 certs
    - Digital Signatures

Identity & Data Privacy in the Metaverse

Understanding Identity in the Real World

- **Authentication versus Authorization**
  - Authentication proves the incoming person/entity is who they claim they are
  - Authorization tells the system what resources they have access to (and what level of access). For example, Samantha may have a child account in the bank with her parents and is not allowed to withdraw money (this becomes claims)
- **What is identity in real world?**
  - Traditional vs Post Modern View of Identity (Traditional is based on norms such as nationality and culture/values)
  - Acquired versus Natural
  - Different forms of IDs
  - Do ants or birds or fish have identity (unless they are a pet. My dog surely has a huge ego, which means he has an identity!)
  - Cultural Identity such as rock bands or cults

WHO AM I?

- A set of claims presented by my JWT or OAuth tokens
- A set of personal traits such as my appearance and biometrics
- A set of my beliefs, habits and values which gives me cultural identity

Snapchat removes Maori tattoo filters after outcry

What is Identity?

- **Your passport**
- **The secret keys you hold, or**
- **Your Culture?**
  - Maori people consider tattoo art as sacred, and it is taken as an important marker of the wearer's identity.
  - Facial tattoos, or moko, have been a part of Maori culture for centuries. They are carved into the skin using chisels in an important ritual, and are used as a means to mark each wearer's unique genealogy and heritage.

Source: https://www.bbc.com/news/world-asia-62830322

Identity & Data Privacy in the Metaverse

Understanding Identity in the Real World

- **Various ways a person or system is authenticated in physical and digital worlds**
  - User ID and Password
  - Emails
  - Biometrics
  - PKI and x509 Certs

  Note: It's important to differentiate between Identifiers vs PII (Personally Identifiable Information)
- **Data privacy in the real world**
  - GDPR
  - California Consumer Privacy Act (multiple US states now have privacy laws)

Identity & Data Privacy in the Metaverse

Prominent frameworks for authentication and authorization

- **OAuth 2.0**

OAuth 2.0 is a delegation protocol for accessing APIs and is the industry-standard protocol for IAM. An open authorization protocol, OAuth 2.0 lets an app access resources hosted by other web apps on behalf of a user without ever sharing the user's credentials. It's the standard that allows third-party developers to rely on large social platforms like Facebook, Google, and Twitter for login.

- **JWTs (Jots)**

JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties. JWTs contain claims, which are statements (such as name or email address) about an entity (typically, the user) and additional metadata.

- **OpenID Connect**

OpenID Connect (OIDC) is an identity layer built on top of the OAuth 2.0 framework. It allows third-party applications to verify the identity of the end-user and to obtain basic user profile information. OIDC uses JSON web tokens (JWTs), which you can obtain using flows conforming to the OAuth 2.0 specifications.

Identity & Data Privacy in the Metaverse

Prominent frameworks for authentication and authorization (contd.)

- **SAML**

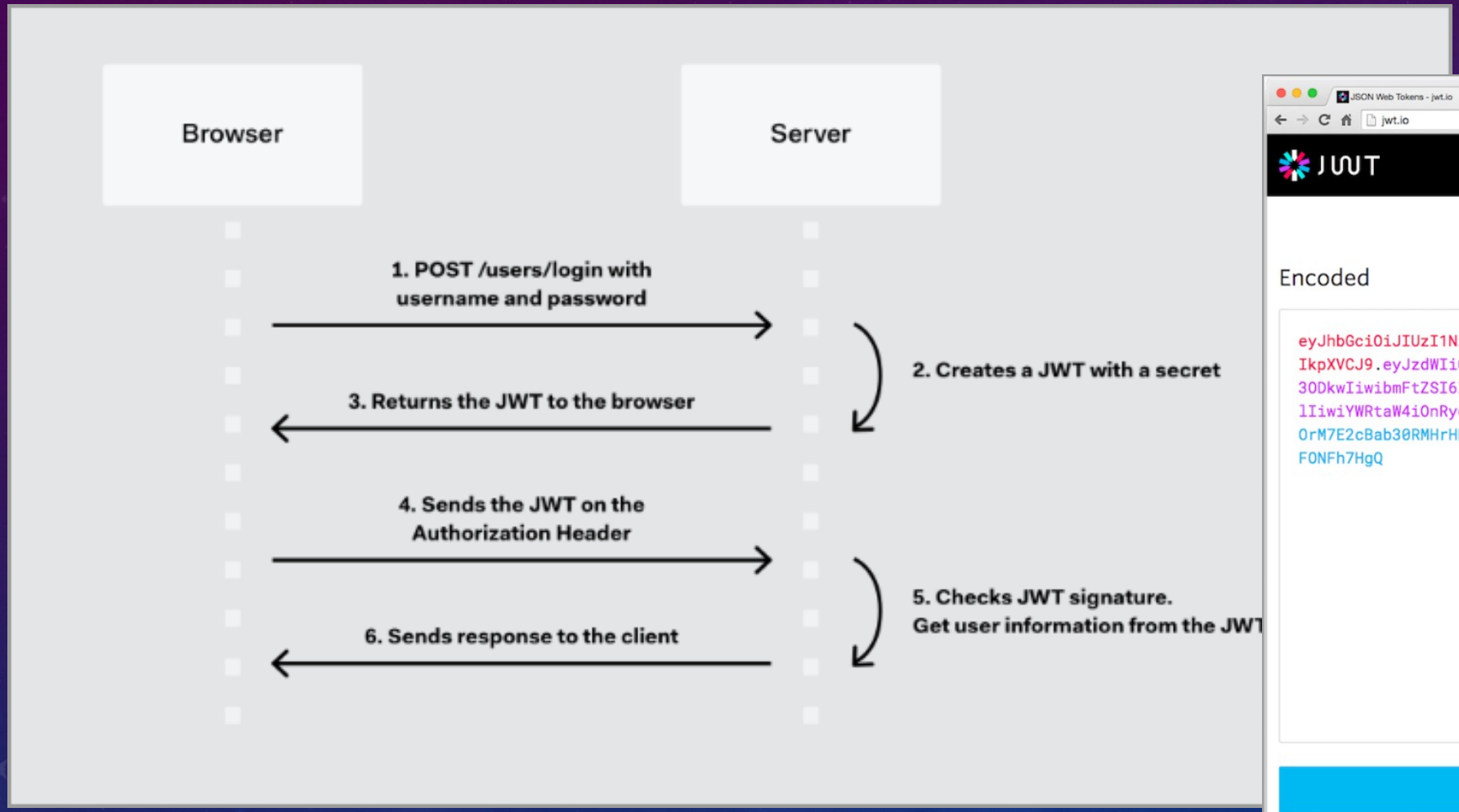
Security Assertion Markup Language (SAML) is an open-standard, XML-based data format that lets businesses communicate user authentication and authorization information to partner companies and enterprise applications that their employees use.

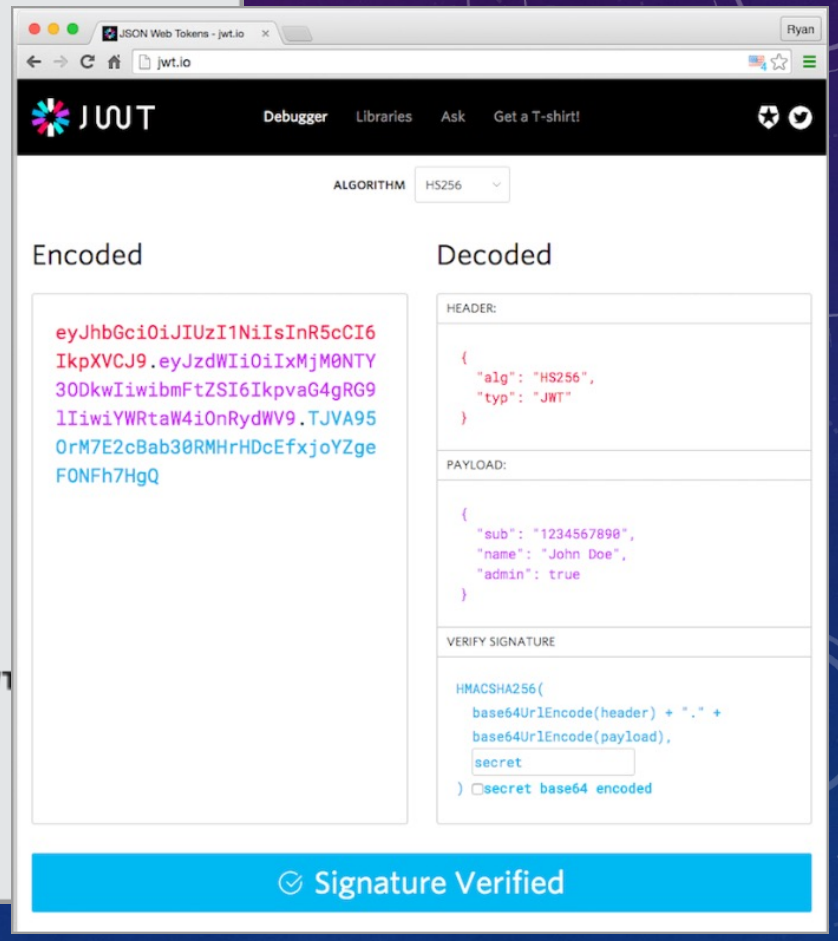
- **WebAuthn**

Web Authentication (WebAuthn) is a web standard published by the World Wide Web Consortium (W3C). WebAuthn is a core component of the FIDO2 Project under the guidance of the FIDO Alliance.

Source: https://auth0.com/docs/get-started/identity-fundamentals/identity-and-access-management

JWT Auth Flow





SAMANTHA VISITS A BANK IN THE METAVERSE

- How do you ID this person visiting the Kiosk in Decentraland – gamer tag?
- Are they a person, an AI, or an IoT device? We certainly cannot identify them by their facial or external appearance
- All Identification in virtual worlds then comes down to system-to-system interfaces and the subject (entity) needs to prove that they are who they claim they are.
- How do you ensure an unchangeable identity for digital entities? SBTs or Soul Bound Tokens could be one way

Soulbound Tokens (SBTs) are digital identity tokens that represent the traits, features, and achievements that make up a person or entity. SBTs are issued by “Souls,” which represent blockchain accounts or wallets, and cannot be transferred [Binance Academy]

A visit to the J.P. Morgan lounge in Decentraland.

HOW WOULD YOU IDENTIFY SAMANTHA?

- In movie Her, Theodore Twombly falls in love with a computer OS named Samantha. What is the identity of Samantha, an AI?
- She has no physical attributes, there is no national, cultural or religious and her personality traits are defined by the computer code and keep evolving based on learning patterns.
- Perhaps something like a Soul Bound Token can be assigned to each entity which cannot be altered even by AI? But then Samantha does not have any soul – does she?
- Personas and avatars are basically digital objects/programs which are rendered on devices. As such, each such digital object will need to embed an immutable identity tag for that entity to interact with the ecosystem.

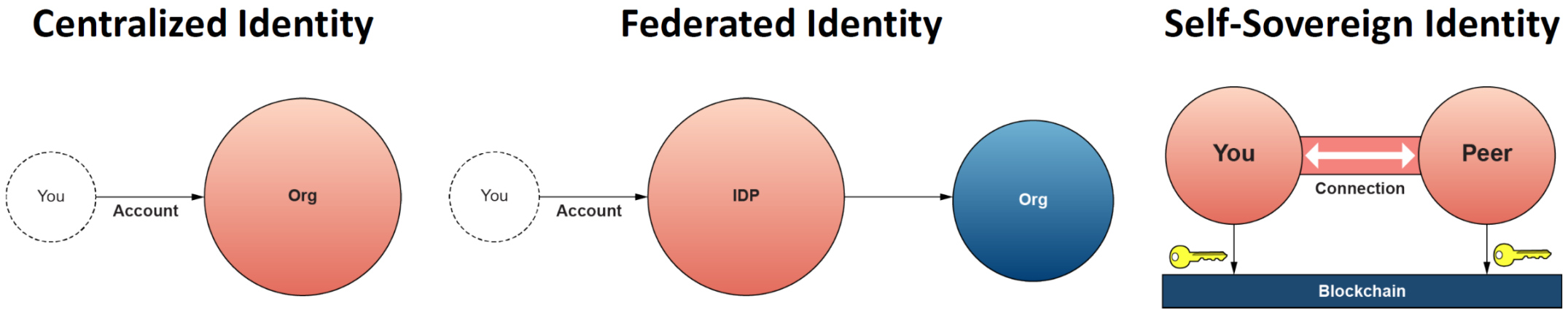
Who assigns these IDs? Enter DI/SSI

Courtesy: Peter Steiner, NY Times July 1993

WORLD ECONOMIC FORUM

DIGITAL IDENTITY

Self-sovereign identity: the future of personal data ownership?



The three models of digital identity. Image: Self-Sovereign Identity.

Decentralized Identity

Key Tenets of Decentralized Identity (Self Sovereign Identity)

- Digital Wallets and Agents
- Verifiable Credentials
- DIDs (Decentralized Identifiers)
- Registries (could be blockchains or other trustable, append-only databases)
- Governance Systems

- **What is decentralized identity?**

Decentralized identity, also referred to as self-sovereign identity, is an open-standards based identity framework that uses digital identifiers and verifiable credentials that are self-owned, independent, and enable trusted data exchange. It aims to protect privacy and secure online interactions using blockchains, distributed ledger technology, and private/public key cryptography.

- **What are verifiable credentials?**

In the decentralized identity approach, verifiable credentials are identity claims, or attestations, like proof of a workplace or student ID, official memberships, or other information from any trusted issuer. People access and control their verifiable credentials using a secure, encrypted digital wallet stored locally on a smart device.

- **What are Wallets and Agents?**

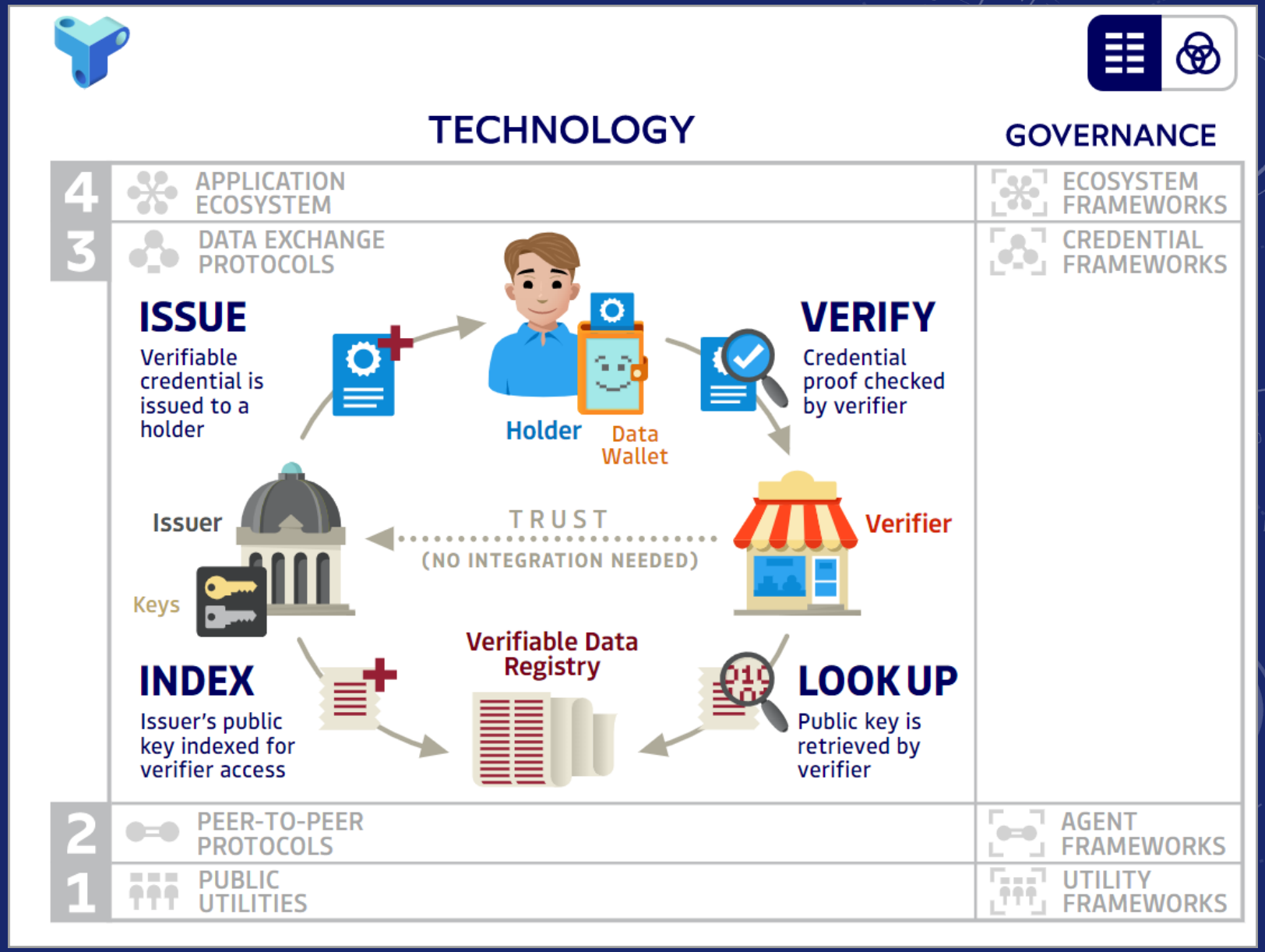
A digital wallet, in the context of self-sovereign identity, is a software application and encrypted database that stores credentials, keys, and other secrets necessary for self-sovereign identity. For simplicity's sake, at Trinsic, we call it all a "wallet" although, in more technical circles, you'll find the term "agent" used for the application that routes messages and decrypts the wallet, and "wallet" used for the storage layer of the agent [Trinsic].

https://rufftimo.medium.com/when-explaining-ssi-start-with-the-wallet-bee5d2af6696

Trust Over IP

The Trust Over IP (ToIP) Foundation was launched in May 2020 with 27 original founding member organizations. It was gestated over the previous year as a confluence of multiple efforts in the digital identity, verifiable credential, blockchain technology, and secure communications spaces by people who saw the need to converge and create an interoperable architecture for decentralized digital trust. This culminated in a Linux Foundation paper called The ToIP Stack published in August 2019 and subsequently turned into a December 2019 article in a special edition of IEEE Communications Standards Magazine on decentralized digital identity.

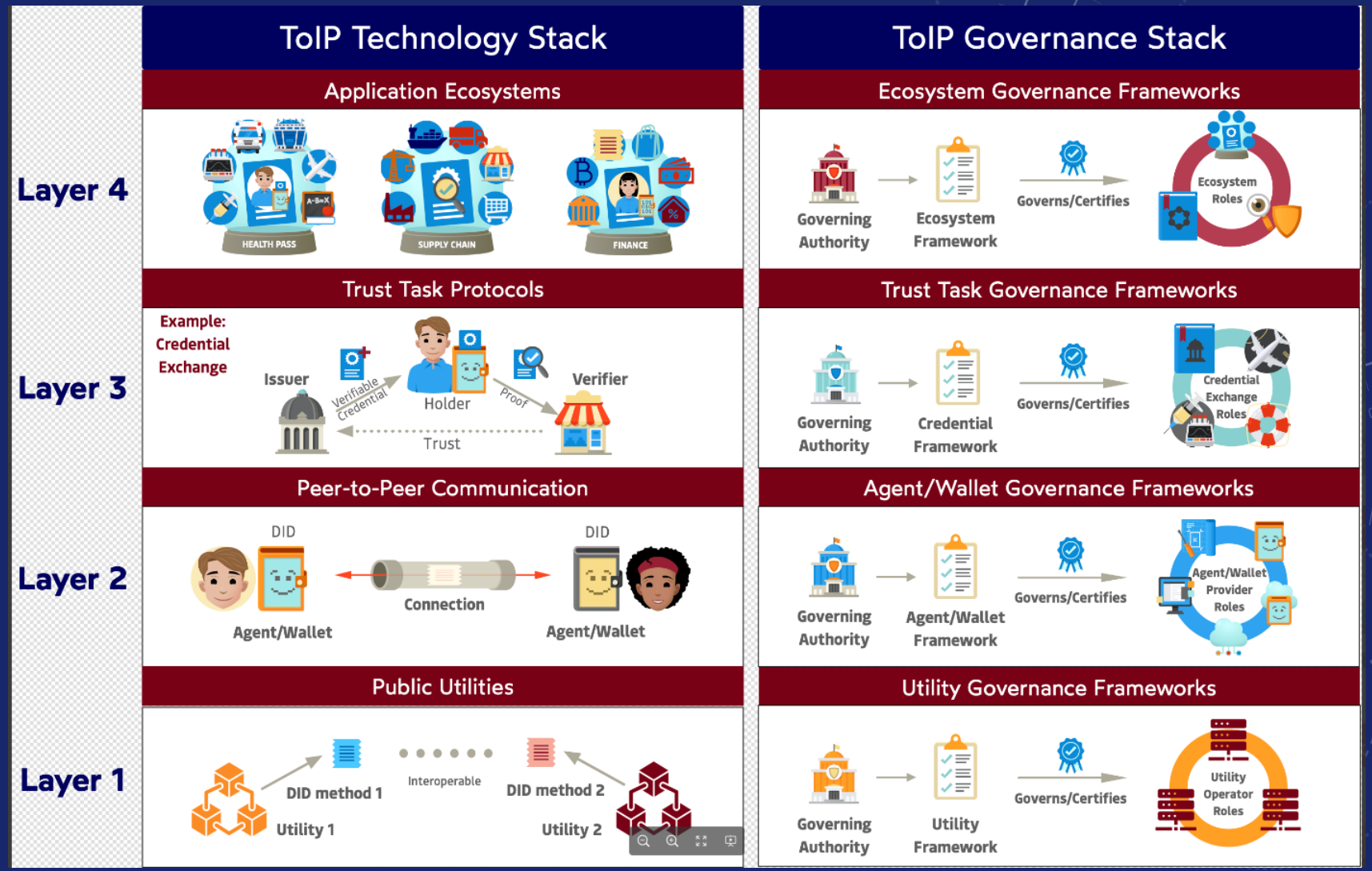
The mission of this Foundation is to simplify and standardize how trust1 is established over a digital network or using digital tools (whether online or disconnected). The goal is to create a safe and private space for all digital interactions—whether between individuals, businesses, governments, or any type of "thing" we might digitally interact with.2 The primary tool for achieving this objective is a "stack" roughly analogous to the TCP/IP stack that powers the Internet. However, this stack is not just technology, rather it combines cryptographic verifiability at the machine layers with human accountability at the legal, business, and social layers.



Source: https://www.trustoverip.org

TOIP DUAL STACK

- Tech Stack
  - Public Utilities
  - Peer to Peer Communication
  - Trust Protocols
  - Application Ecosystems
- Governance Stack
  - Utility Governance
  - Agent/Wallet Governance
  - Trust Governance
  - Ecosystem Governance



Source: https://wiki.trustoverip.org/display/HOME/Introduction+to+ToIP

Identifying Entities in the Metaverse

Possible Ways to Identity Entities in the Metaverse

- Gamer or Avatar Tags (Each one of current virtual worlds such as Second Life, Microsoft Mesh, Meta's Horizon Worlds, etc. require a person to create a user ID which can have its own display tag (one person can create one more IDs)
    - This does not address entities spawned in the virtual space
        - AI generated characters such as Samantha in the movie "Her"
        - A child character born when two avatars decide to have a family in Second Life
        - IOT devices which could theoretically join as characters (can I have my raspberry-pi drone join the Metaverse as a flying bird?)
- Make each entity present a Verifiable Credential
    - This will require each spawned entity to be registered on some trust registry which is audited and governed
        - Where to register?
        - Blockchain
            - Public doesn't make sense due to PII data
            - Permissioned blockchains can be used (with channels for per missioning)
    - Can this become a pre-req for avatars to be identified (Twitter blue checkmark?)
    - Can the hosting ecosystem be held responsible for ensuring there are no UEs (Unidentifiable Entities) in their ecosystem?

Identifying Entities in the Metaverse

Decentralized Social Networks and Graphs

The key idea behind decentralized social networks is giving users the choice to exit from any application whilst maintaining their social connections

Three approaches to decentralized social networks (The Block Research)

- Farcaster — Sufficient Decentralization (minimum info on blockchains)
- Ave Lens - Decentralize social graph (middle ground)
- DeSo - Decentralize everything (very impractical)

The Player/User

Telemetry

- Account, Financial, Purchases Data
- Demographic User Data
- Geospatial, Location Data

Biometrics

- Physical/Biological Data
- Motion/Tracking & ID Data
- Behavioral/Actions Data
- Attentional/HeatMap Data
- Voice Content/ID Data

Biometrics in XR

User Data Rights, Ownership, & Data Privacy are one of the greatest challenges of the 21st century. Not sale of rights, but protection of rights.

We must start with the assumption that the user owns their own data not own to sell but own to lock identity and keep it private. Start with a default of NOT SALE, and only grudgingly let people sell parts of their data, or the race is lost before it is started.

Fix this in XR BEFORE we reach any future attempt at the metaverse

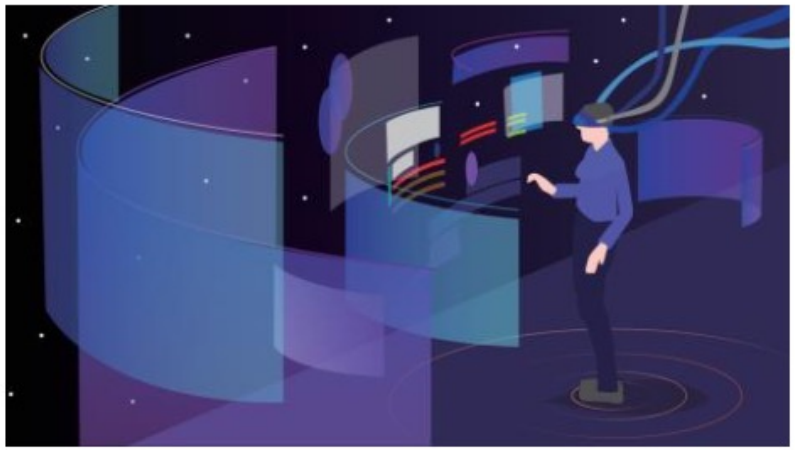
PAYMENTS IN THE METAVERSE

- Payments in the real world
  - Cash / Check / Cards
  - ACH
  - Wires
  - Digital Payments (such as Venmo, PayPal, Alipay, WeChat, Paytm, etc.)
  - Crypto Payments

PAYMENTS IN THE METAVERSE

- Payments in virtual worlds
  - Most payments are made via platforms or marketplaces
  - Direct avatar-to-avatar payments are not generally allowed (for example, Tilia manages payments for Second Life and other Virtual Worlds)
  - Micro payments are not economically efficient in virtual worlds due to lack of payment rails
  - Staying compliant with Regulations while allowing payments and money transfer is a major hurdle for most virtual worlds
  - Generally speaking. everything in the virtual worlds, includes a 30% platform fee

Yet again, Identity takes center place when it comes to payments



JP Morgan invests in Second Life's payment platform Tilia

19 October 2022 6 2 1

JP Morgan has made a strategic investment in Tilia, the payments platform initially built to power the economy of online virtual world Second Life.

Source: https://www.finextra.com/newsarticle/41162/jp-morgan-invests-in-second-lifes-payment-platform-tilia

Data Privacy

- There are numerous privacy issues with our PII (Personal Identifiable Information) in our current systems.
- What started as convenience has now become a major security issue for individuals, companies and nations.
- Decentralized Identity models suggest no personal data should be kept on public databases (not even encrypted since today's encryption may not be quantum-safe in next 10 years)
- Open Questions Remain:
  - How much correlation between IDs is okay?
  - Can we let entities to be fully anonymous in the Metaverse?
  - How do you enforce accountability and personal responsibility while ensuring data privacy in virtual worlds?

Passwords

- Regular Internet users have an average of 85 passwords for all their accounts. (Cnet, 2020)
- The most used password in the world remains **123456** followed by **123456789**, **qwerty**, **password**, and **12345**. (Cybernews, 2021)
- 80% of all hacking incidents are caused by stolen and reused login information. (Verizon, 2020)

Phishing

- As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the U.S. FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime. (FBI Internet Crime Complaint Centre, 2021)
- Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months). (Tessian, 2021)

Data Breaches

- There were 1,767 publicly reported data breaches in the first six months of 2021, which exposed a total of 18.8 billion records. (Risk Based Security, 2021)
- Over 90% of all healthcare organizations reported at least one security breach in the last three years. 61% acknowledged they don't have effective mechanisms to maintain proper cybersecurity. (Frost Radar, 2020)
- In 2020 the average cost of a corporate data breach was $3.86 million. (Dice.com, 2020)

Summary

This brief session was meant to instill a sense of complexities involved in getting the concept of Identity right as we delve into an unknown – the Metaverse, which is expected to be a mesh of a multitude of virtual worlds and perhaps some intersection with the real world.

Please consider following three key takeaways from this session:

- Identity in our physical world is mostly based on appearance and biometrics (including DNAs in some cases) and are controlled by central authorities or organizations serving as IdPs
- Identity in Digital space is primarily based on proving that the subject has possession of a secret. While digital IDs are still mostly centralized (or clustered using SSO and Federation), SSI is slowly getting adopted in multiple regions (prime examples: Sovrin, IDunion, ION).
- Identity in the Metaverse will need to be decentralized to allow subjects to prevent current issues surrounding centralized censorship and hoarding of PII. While one can expect to stay pseudonymous in the Metaverse (using game tags, multiple DIDs and Zero Knowledge Proofs), one should not expect to remain totally anonymous.

In Summary, while entities (read avatars & personas) can stay pseudonymous but each entity in the Metaverse will need to offer proof of humanity by being linked to a real human who can be held accountable in the real world for their actions via decentralized governance systems (yet to be defined for yet to come Metaverse)