Blockchain Technology (Week 5)
Blockchain Identity Project (S&W)

Name: Vannchannida ANG
Class: FDE C6 (Afternoon)

Blockchain Identity Project (Sovrin)

Sovrin, a decentralized global public utility for self-sovereign identity, was built on a distributed ledger technology (DLT) and aims to return control of digital identity to individuals, moving away from the current model where corporations and governments act as centralized identity providers. At its core, Sovrin enables the creation of verifiable credentials that are secured using cryptographic, privacy-preserving, and interoperable.

Sovrin Strengths

1. **Foundational Focus on Self-Sovereign Identity (SSI) Principles**

Based on the Sovrin White Paper explains how Sovrin was built from the ground up to follow the main ideas of SSI. This includes the existence where users live their own lives and aren't just a data collectors' target. Users also have ultimate control over their identities and personal data. They must explicitly consent for their data to be used. In addition to that, users have the right to access their own data and be able to retrieve it if held by a third party. This philosophical dedication is a big strength because it makes sure that the architecture was designed to give users power, not to take data from them.

2. **Tokenized Model**

Slightly different from the other blockchain models, Sovrin doesn't use a cryptocurrency for speculation or to pay for general network transactions like gas fees. The Sovrin Token (SOV) is a "utility minimized token" with one primary, elegant function to prevent Sybil attacks and spam by requiring a minimal and refundable token deposit for writing certain transactions to the ledger.

3. **Advanced Cryptographic Privacy Features**

Sovrin leverages cutting-edge cryptography to maximize privacy. It also goes far beyond simple pseudonymity It has Zero-Knowledge Proofs (ZKPs) that allows users to prove they possess a certain credential without revealing the underlying data.

4. **High Degree of Interoperability via Standards**

This project was built on and actively contributes to open, global W3C standards, primarily Decentralized Identifier (DIDs) and Verifiable Credentials that ensure the identities and credentials be used across other compatible SSI networks and ecosystems.

Sovrin Weaknesses

1. **Centralization and Decentralization paradox**

This is like a problem of “who guards the guards” which is the biggest criticism of Sovrin is its “permissioned” nature. Relying on a group of trusted Stewards creates a new kind of club. What happens if it becomes too exclusive and doesn’t let new members in? Or the Stewards disagree on a major decision, causing a gridlock? Or even a government pressures the Stewards to censor certain users? This is a centralization paradox; in trying to create a decentralized system, Sovrin introduced a small group of powerful players. In addition, the success of the network depends entirely on the Sovrin Foundation’s ability to keep this group honest, diverse, and decentralized.

2. **Legal and Liability Ambiguities**

While the technology is smart, it also throws a wrench into our current legal system, which simply isn't built for this new model of identity. Think about a simple case of fraud: if someone uses a fake digital diploma to get a job, who's left holding the bag? Is it the university that issued it, the employee who presented it, or the stewards who maintain the network? Our old rules for liability don't have a clear answer for a system where responsibility is so spread out. And it's not just about fakes; what about taking a credential back? If a driver's license is suspended, revoking it isn't as simple as hitting 'delete' in one central DMV database. The system has to ensure that every verifier, everywhere, knows

that the credential is no longer valid in near real-time—a daunting technical and logistical challenge on a global scale.

3. **User Experience and Key Management**

This system puts the users in full control, but that also means the entire security of their digital identity boils down to them safeguarding one thing, which is the private key. It requires a huge amount of responsibility; if you lose the key, you don't just lose the account, but you lose the entire digital identity forever. There's no customer service to call or "forget password" link. It's a level of technical complexity and permanent risk that most people aren't prepared for. This leads them to be one of the biggest hurdles to mainstream adoption

4. **Competitions and Market Fragmentation**

Sovrin is not the only player in the SSI space. It faces competition from other blockchain-based identity projects (e.g., uPort, Civic), corporate-led initiatives (e.g., Microsoft's ION on Bitcoin, IBM's offerings), and consortium models (e.g., Decentralized Identity Foundation). These risks create silos of trust that undermine the goal of a universal, interoperable identity system.

Reference:

https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf