**Project Design Phase-I**

**Solution Architecture**

|  |  |
| --- | --- |
| Date | 30 october 2023 |
| Team ID | NM2023TMID01608 |
| Project Name | Ethereum Decentralized identity smart contract |
| Maximum Marks | 4 marks |

**Solution Architecture:**

Creating a decentralized identity (DID) solution on the Ethereumblockchain involves several components, including smart contracts and off-chain services. The goals of a decentralized identity (DID) project on the Ethereumblockchain can vary depending on the specific use case and the stakeholders involved. However, some common goals for such a project include:

**1**.**Self-Sovereign Identity**: The primary goal of a DID project is to give individuals or entities control over their own identities. Users should have the ability to create, manage, and share their identity information as they see fit.

**2.Privacy and Security**: Ensuring the privacy and security of identity information is a key objective. Users should be able to share only the necessary information and have confidence in the security of their digital identity.

**3. Interoperability**: DIDs should be interoperable with other decentralized identity systems and adhere to recognized standards, such as the W3C DID standards and DID methods, to facilitate compatibility and data portability.

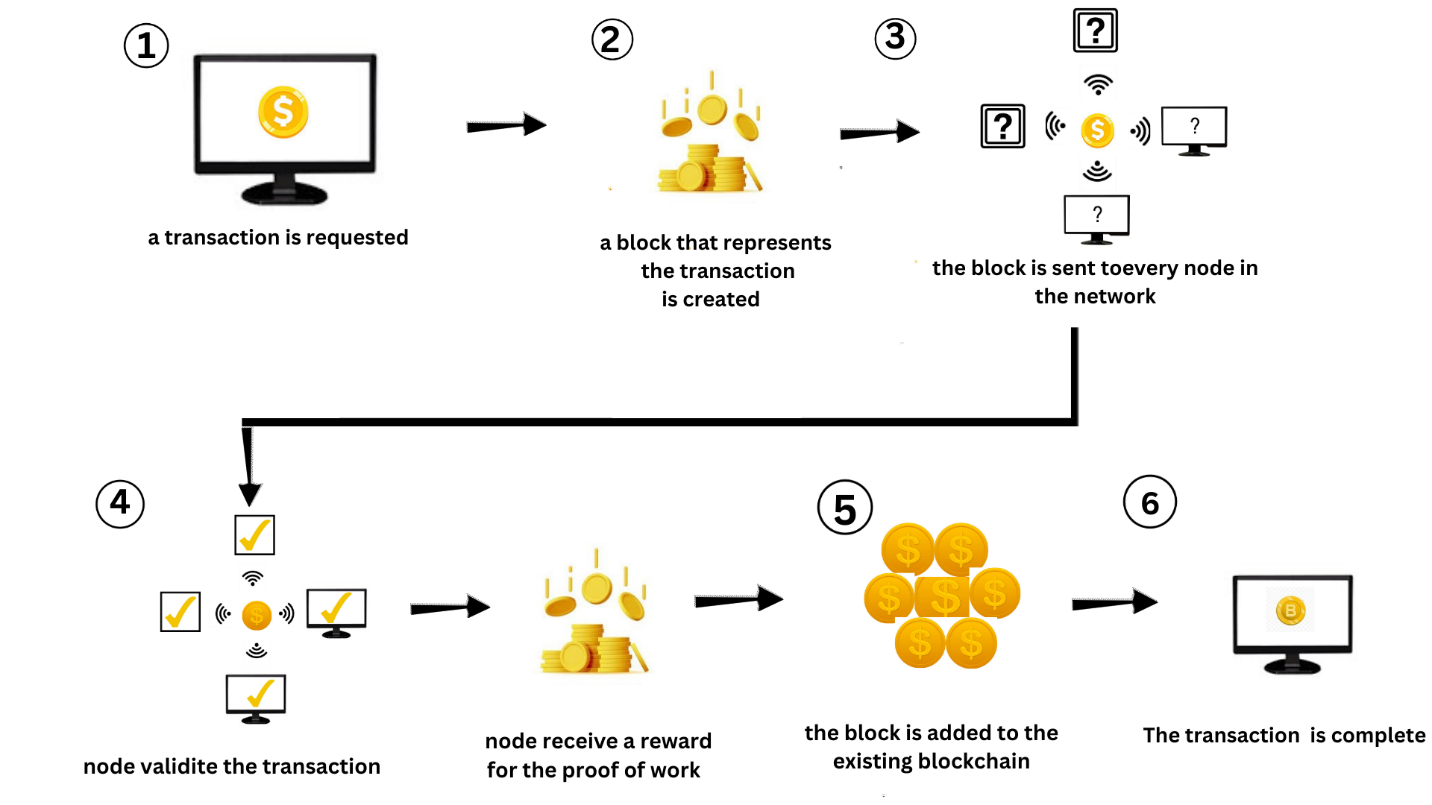
**4. Security and Auditing**: Security is paramount in a DID solution. Implement robust security practices, conduct security audits, and ensure proper access controls.

**5. Scalability**: Consider the scalability of the Ethereum network and use layer-2 solutions if necessary to handle a large number of DIDs and credentials efficiently.

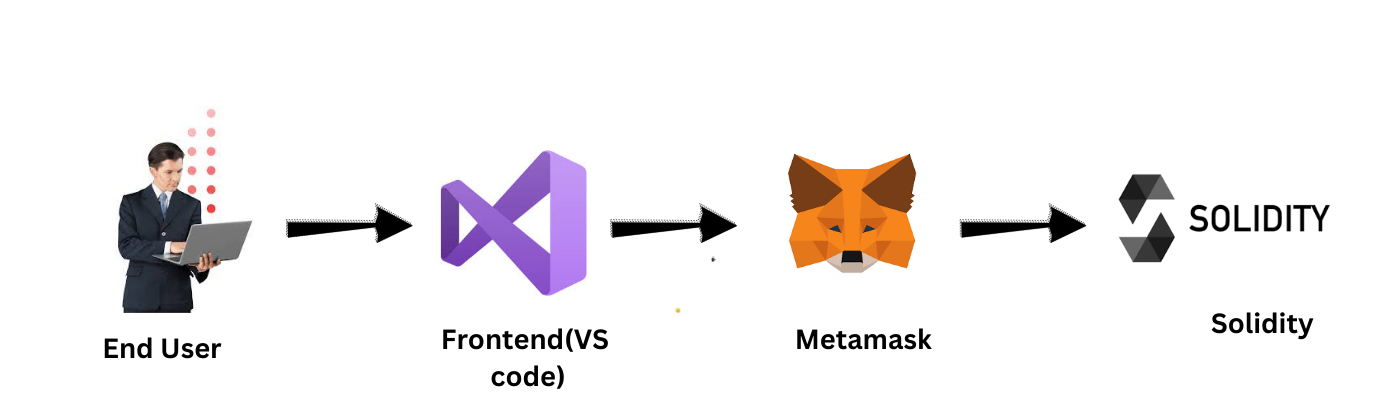
6. **End-to-End Verification**: The system enables end-to-end verification of identity information, enhancing the overall Top of Form

**Solution Architecture Daigram**

**Technical Architecture**

****

**Technical Stack**



**Step 1: Transaction Requested**

* A user initiates a transaction, which could involve sending cryptocurrency, recording data, or executing a smart contract.

**Step 2: Block Creation**

* The transaction is grouped with other pending transactions to form a new block.
* This block is created by a miner or node in the network.

**Step 3: Block Sent to Nodes**

* The newly created block is broadcast to every node in the blockchain network, ensuring network-wide awareness.

**Step 4: Node Validation**

* Each node in the network validates the transaction within the block.
* Validation includes checking criteria such as sender's balance and adherence to network rules.

**Step 5: Node Reward**

* In networks using Proof of Work (PoW) or similar consensus mechanisms, the node successfully validating the block is rewarded.
* Rewards typically come in the form of cryptocurrency (e.g., Bitcoin), incentivizing node participation.

**Step 6: Block Added to Blockchain**

* The validated block, containing the transaction, is added to the existing blockchain.
* This process extends the blockchain's history and is permanent.

**Step 7: Transaction Completed**

* With inclusion in a validated block, the transaction is considered completed.
* It becomes a secure, unalterable part of the blockchain's history.