PRIVACY-PRESERVING CONSENSUS PROTOCOL BASED ON SOCIAL CAPITAL

Bc. Juraj Mariani supervisor: doc. Ing. Ivan Homoliak Ph.D.







What is Social Capital and why do we use it?

Definition:

- Human capital + attention economy + social influence metrics
- scarce resource, replacing hardware (PoW) or stake (PoS)
- consensus power mechanism,
- SC is easier to amass than \$ or HW

System Overview:

- social capital
- content creators = validators & block proposers
- influence = consensus power

Types of Social Capital:

- Passive Unallocated SC
- Active Allocated and automatically staked SC
 - Effective Active SC & scaled to balance influence
- Limited Each user has a fixed amount of social capital

Incentive Mechanism

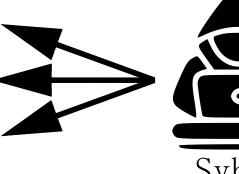
- Encouraging users to endorse
- Creators offer exclusive, follower-only content
- Followers who prove engagement (e.g., viewing content) receive native token rewards

Identity verification

- Sybil entity protection (user with more than one account)
- one-account-per-person policy
- Why? A single user could generate limitless social capital

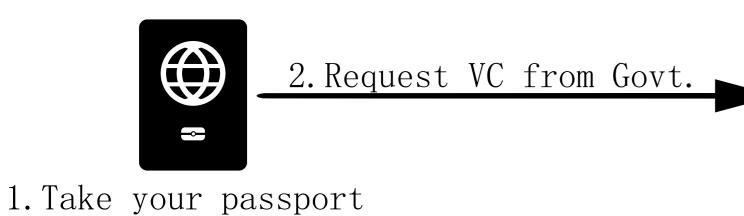
{Account: 1, SC: X} {Account: 2, SC: X}

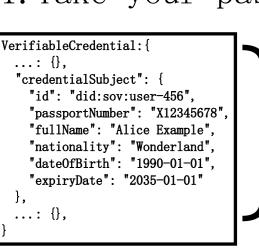
{Account: 3, SC: X}

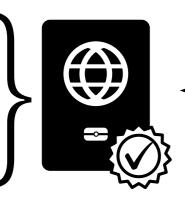




guide to our social capital blockchain Step 1: Register with your local government

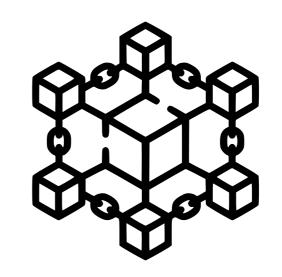


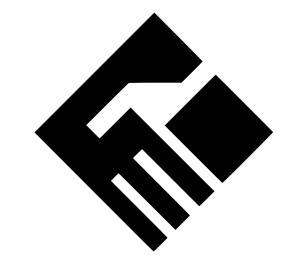




3. Receive Virtual Identity

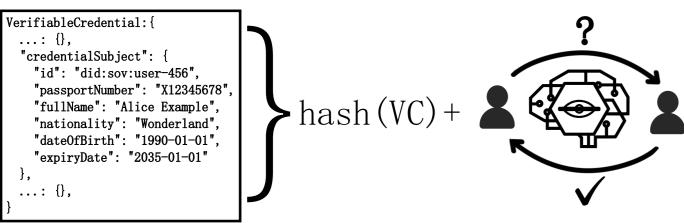
Step 3: Identity verified



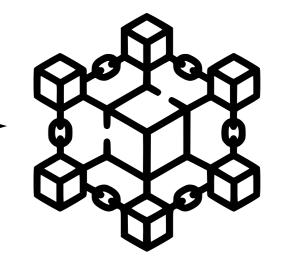


You can now interact with the blockchain, earn and distribute Tokens and endorse creators or produce content!

Step 2: Verify your on-chain identity

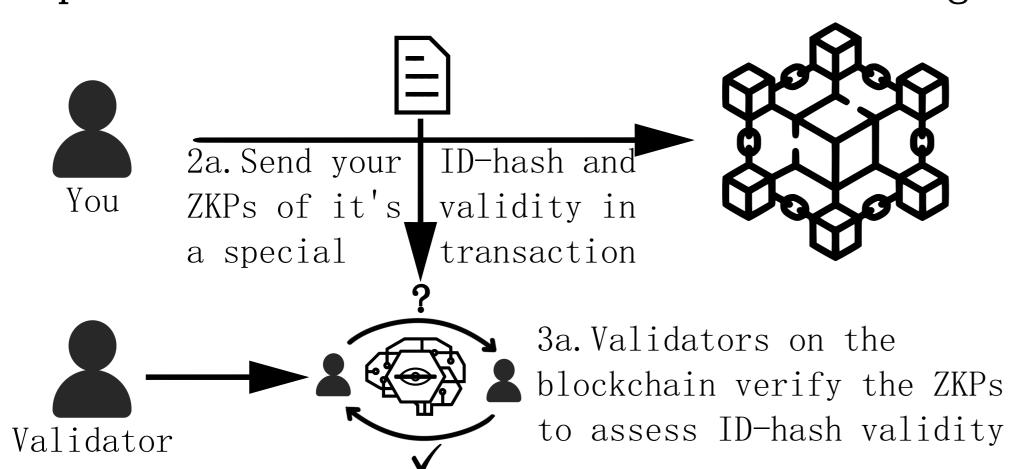


2. Access Social Capital Blockchain



1. Take your VC and create an ID-hash and Zero-knowledge proof that you generated the ID-hash correctly

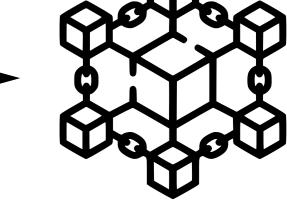
Step 2 Alternative A: ZKP on-chain storage



Step 2 Alternative B: IDP chain ZKP valid.



hash(VC) 2b. Send your ID-hash in a special transaction



3b. Send ZKP to a separate IDP blockchain, providing decentralized identity verification

