Decentralized verification infrastructure for documents anchored to blockchain
Contents

• What is Blockchain

• Digital credentials

• Zero knowledge proofs

• Data decoupling

• Verification of credentials
What is a blockchain

- blockchain is the result of a consensus protocol based on proof of work
- represented as a distributed database
- the point of a blockchain is not to store data but to ensure mutually distrusting parties are all in agreement.
  - public vs. private discussion: it is clear that a private blockchain is a misnomer
Characteristics of a blockchain

• Immutable
  • write only *(data cannot be altered or removed!)*
  • open access

• Distributed
  • no central authority

• Only transaction records
  • cryptographic hashes
  • public keys
Digital credentials

• Traditionally issued on paper
  • relatively easy to falsify
  • cannot be revoked
  • need to be verified -> entire industry based around verification
  • can be lost/destroyed (only one original)

• Early 21st century digitalization craze
  • credentials issued digitally
  • require authentication infrastructure
  • large online repositories of data are attractive targets
Zero knowledge proofs

• Zero knowledge proof
  • method by which one party A, can prove to another party B, that they know information X
  • achieved through cryptographic hashing

• To put in real perspective
  • without knowing a credential’s contents, the hash stored on the blockchain can be used to prove that it hasn’t been altered
  • person is issued a credential
  • proof is stored in a central repository
  • issuer’s copy is kept in an offline storage
Where is the blockchain

- One or more proofs are anchored to a transaction on a blockchain

- Benefits
  - records continue to exist even if the issuer seizes to exist
  - ensures non-repudiation
  - cross national repository
  - immutability of records
Data decoupling

• Blockchain does not guarantee the authenticity of the issuer, only the immutability of the record
  • garbage in, garbage out

• Accreditation of the issuers
  • out of scope

• Format/standard agnostic
  • ensures faster adoption
  • mitigates technological obsolescence
Verification infrastructure

• The “cost” of verification needs to be minimal

• Cost can be defined as:
  • complexity of software implementation
  • ease of inclusion into an existing CMS
  • many new systems end up as abandoned code repositories due to high complexity of implementation

• Need for fewer resources for verification
  • helpdesk, account management, hosting…
  • cheap hardware
Verification infrastructure

• Can work offline
  • example: Bitcoin transactions transmitted periodically by satellites

• Stakeholders that can have nodes
  • HEIs
  • Governmental agencies
  • Employers / recruitment agencies
Does it make sense?

• Yes
  • decentralization is always a good thing
  • records are preserved if institutions seize to exist
  • an integral part of the principles of self sovereignty
  • puts the individual before the institution

• No
  • cultural, sociological and legal difficulties
  • cost of development to change a system that has worked for centuries
  • institutions don’t like to share
  • resistance to change
  • if it works, don’t fix it
    • but does it?
Questions?