Blockchain for finance and banks

Year : 2023-2024

Prepared by : Mrs. LOUDINI Souad

Master : Distributed Information Systems Engineering and Security

Chapter 03:

Blockchain as identity verification

1. *Accounting and auditing*

❖ Definition of Accounting and auditing

- Accounting and auditing are two interrelated concepts that stem from the same context of financial information. These functions are essential for the effective operation of an organization, with each playing a distinct yet complementary role in ensuring the accuracy and reliability of financial information.

- accounting is the process of recording and organizing financial transactions, while auditing is the process of evaluating and ensuring the accuracy and reliability of financial statements

- Auditing and accounting form the backbone of robust financial management, fostering trust and accountability within organizations and the broader financial ecosystem.

❖ This table summarizes the difference between Accounting and Auditing :

Feature	Accounting	Auditing
• Purpose	- Accounting is the process of recording, summarizing, and presenting financial transactions and statements, determining a company's financial position, profitability, and performance	- Auditing is the process of verifying the accuracy and completeness of financial statements, aiming to add credibility to the company's financial reports and ensure compliance with various regulatory standards
• Timing	- Ongoing and continuous as part of daily business operations.	- Typically conducted periodically, often annually, to verify financial statements.
• Preparation	- Executed by internal accountants within the organization.	- Carried out by external auditors, independent of the organization And often requested by regulatory authorities.
• Confidentiality and Integrity	- Accountants maintain the confidentiality of financial information, ensuring that it is accurate and up-to-date	- Auditors also maintain confidentiality, but their primary focus is on evaluating the credibility of financial statements

Read more

Blockchain in Accounting and Auditing

- blockchain is poised to transform traditional accounting practices, offering a robust solution that addresses longstanding challenges and sets new standards for transparency and efficiency in the financial ecosystem.

- Blockchain could fundamentally change the auditing process. As a complete record of transactions is stored on a blockchain, auditors will no longer need to request, and wait for trading parties to provide, data and documents. In addition, blockchain will surpass the traditional audit sampling process, and allow continuous audits for any “on-chain” transactions in any specific period. The adoption of blockchain will free up resources that were previously expended on evidence collection and verification.

Read more

❖ This table summarizes the key benefits of blockchain for accounting

Current accounting challenges	Value driver	Blockchain benefits
• Manual documents	- Operational simplification/efficiency	- Digitize documents, increase efficiency, reduce costs, reduce human error, automate reconciliation.
• Time-consuming process	- Transaction settlement time reduction	- Blockchain-powered smart contract enables contracts to execute automatically once pre-set conditions are met and facilitates real-time transactions.
• Lack of mechanism to track transactions from different ledgers	- Counterpart risk reduction	- Agreements are codified and executed in a shared, immutable environment, forming an audit trail.

Read more

❖ This table summarizes the key benefits of blockchain for accounting

Current accounting challenges	Value driver	Blockchain benefits
• Prone to fraud	- Fraud minimization	- Blockchain provides transparency, visibility, provenance, and immutable records, which enhances security. Any suspicious fund transfer will be observed and detected in real-time.
• Regulatory complexity, costly to organizations	- Regulatory efficiency improvement	- Provides faster and more accurate reporting by automating compliance processes through a smart contract.

❖ This table summarizes the key benefits of blockchain for auditing

Current auditing challenges	Value driver	Blockchain benefits
• The challenge **in auditing transactions** is how to obtain enough evidence to achieve audit objectives when auditors cannot examine every item within an account balance or class of transactions due to limited sampling	- Supervision of all transactions	- Provides auditors with the ability to supervise all transactions, reducing the need for sampling.
• Conventional auditing approaches often rely on manual sampling, static data analysis, and a focus on historical transactions. These limitations can hinder auditors' ability to effectively address the complexities of modern environments .	- Changing Traditional Control Understanding	- Blockchain technology provides auditors with a more comprehensive view of companies, prompting the exploration of new audit models.
• **Delay** in the audit process until the conclusion of the reporting period	- Real-Time Auditing	- Establishes a real-time audit framework, enabling immediate assessment of financial activities.

2. Funding

Introduction

- In the modern, interconnected world, identity has emerged as a critical element in every aspect of our lives, particularly in the digital realm. As individuals, organizations, and devices interact and engage in transactions online, verifying and managing their identities has become paramount to ensuring secure, trustworthy, and efficient interactions. Identity is the first step in any transaction between two or more parties. It is the foundation upon which trust and confidence are built. Without a reliable way to verify the identity of each party involved in a transaction, there is a risk of fraud, abuse, and other malicious activity.

- Traditionally, identity verification has relied on physical documents like passports, ID cards, and birth certificates. While these methods have served us well for many years, they are becoming increasingly insufficient in the face of the rapidly evolving digital landscape.

Definition

- A digital identity is the information and data that identifies an individual in the digital world. In other words: an electronic representation of an individual often used to access online services, make purchases, and interact with others on digital platforms.A digital identity can include personal information as well as a person's online behavior.

- The key components that comprise the digital identity:

• Personal Information	This includes your name, address, date of birth, and other identifying information.
• Digital Credentials	These are electronic documents that verify your identity, such as a passport or driver's license.
• Biometric Identifiers	These are unique physical or behavioral characteristics that can be used to identify you, such as fingerprints or facial recognition.
• Digital Behavior	This is the data that is generated by your online activity, such as your browsing history, search queries, and social media posts.

Life cycle

- **Registration:** Capturing and recording key identity attributes of a person who claims a certain identity. This may include biographical data (e.g., name, date of birth, gender, address, email), biometrics (e.g., fingerprints, iris scan), and the other attributes.

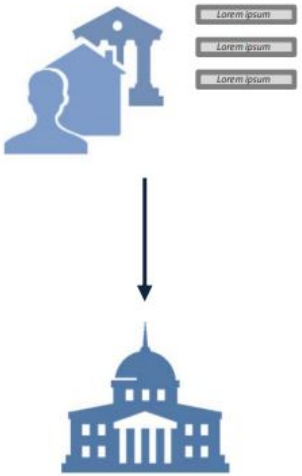
- **Validation & Issuance:** Identity is validated by checking the presented attributes against existing data. Then, the registered identity goes through an issuance/credentialing process before it can be used. For an identity to be considered digital, the credentials or certificates (e.g., birth certificate, passport) issued must be electronic, in the sense that they store and communicate data electronically.

- **Usage:** After users have been registered and credentialed, it is possible to use their digital identities to access public or private services. For instance, citizens may use their eID number to pay their taxes through an online portal, while bank customers can use smart debit cards or mobile financial services. In order to access services, the user must be authenticated using one or more factors, for example password or fingerprint.

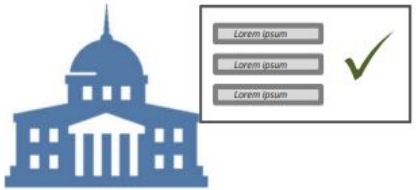
Figure

THE STRUCTURE OF IDENTITY SYSTEMS

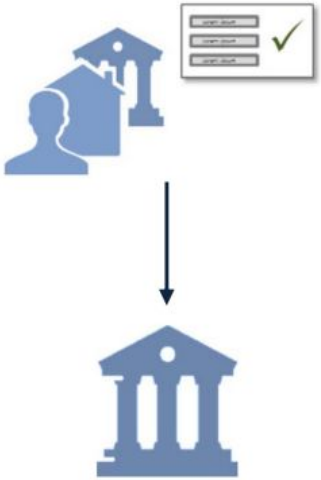
1. *The user presents a set of attributes to a third party*



2. *The third party verifies the attributes and attaches its attestation to the attributes, becoming an identity provider for the user*



3. *The user then uses the credential from the identity provider in transactions with relying parties*



Limitations in digital identity

❖ Here are some of the key challenges organizations face in managing digital identities:

- **Data quality:** Identity data is disparate, difficult to find and often inaccurate.

- **Data protection:** Standards differ from country to country,and compliance is difficult and costly to manage, increasing the risk of non-compliance and potential legal issues

- **Implementation:** Significant investments have been made in these schemes globally; any change would be highly disruptive.

Blockchain-based Digital Identity

Using blockchain or distributed ledger technology (DLT), digital identity issues can be straightforwardly addressed by introducing a new way of managing identities. It enables direct data sharing among network entities without intermediaries and possesses key features that have potential benefits for identity systems:

- ➔ **Low transaction cost:** By eliminating intermediaries, distributed ledgers reduce the overhead costs associated with traditional identity verification and management processes. This makes it more cost-effective for individuals and organizations to manage their identities and interact with each other securely.

- ➔ **Immutability:** The tamper-proof nature of blockchain ensures that once identity data is recorded on the ledger, it cannot be altered or deleted without the consensus of the network participants. This immutability safeguards identity data from unauthorized modifications and ensures its long-term integrity.

- ➔ **Convenience:** Blockchain-based identity systems allow individuals to manage their identities from any device. This accessibility empowers individuals to control their identity data and interact with service providers seamlessly, regardless of their location or connectivity.

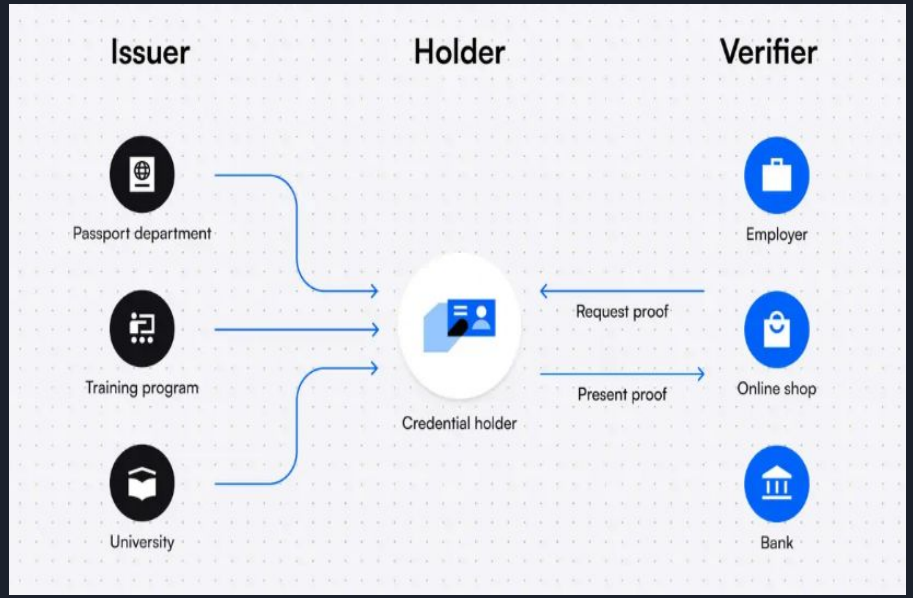
self-sovereign identity (SSI)

self-sovereign identity technology allows people to self-manage their digital identities without depending on third-party providers to store and manage the data. Currently, Self-Sovereign Identity is used interchangeably with the term decentralized identity.

There are three main participants in the SSI system:

- **Holder:** Someone who creates their decentralized identifier with a digital wallet app and receives Verifiable Credentials.
- **Issuer:** Party with the authority to issue Verifiable Credentials.
- **Verifier:** Party checking the credential.

The interactions between the holder, issuer, and verifier is sometimes called "the trust triangle." Every time information is requested by a verifier, the holder chooses whether to allow access to their data.

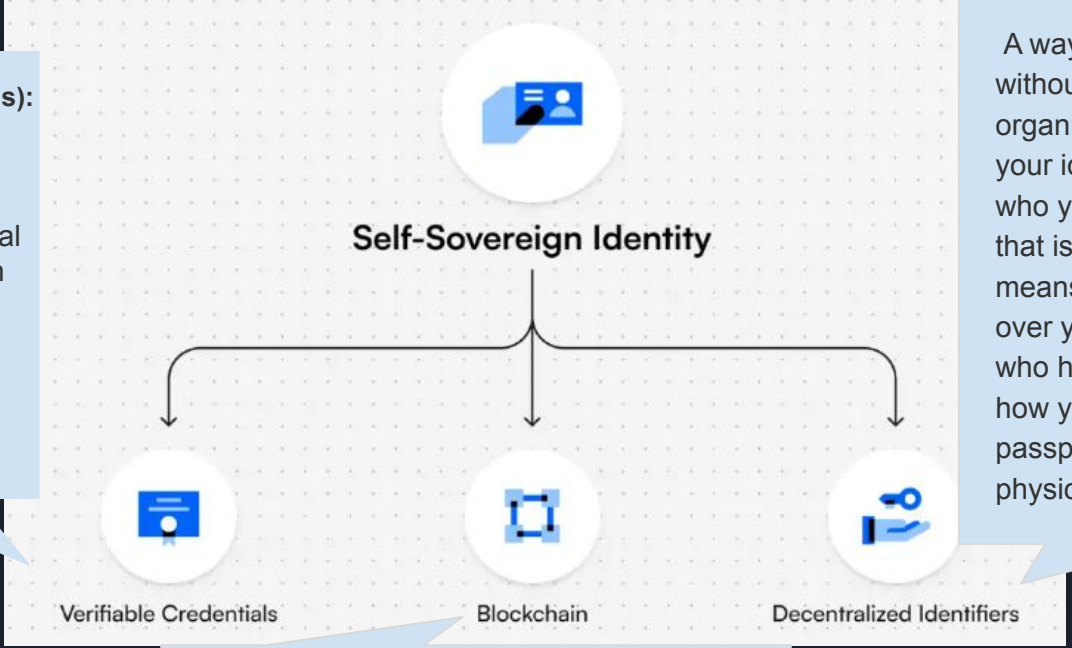


figure

❖ Key Components of SSI :

3.Verifiable Credentials (VCs):

Digital cryptographically-secure versions of paper and digital credentials that people can present to verifiers.



2.Decentralized Identifiers (DIDs):

A way to identify yourself online without relying on a centralized organization or company to verify your identity. Instead, you can prove who you are using a unique code that is stored on a blockchain. This means that you have more control over your personal information and who has access to it. It's similar to how you use a driver's license or passport to prove your identity in the physical world.

1.Blockchain:

A decentralized database that is shared among computers in the blockchain network that records information in a way that makes it very difficult to change, hack, or cheat the system.

Digital identity : Use cases

❖ Worldcoin :

- Worldcoin aims to become the world's largest digital identity and financial network.
- It will give ownership to everyone, no matter where they live or their background.
- By leveraging **unique iris scans** and decentralized protocols, Worldcoin envisions a future where individuals possess autonomous control over their digital identity and financial data, facilitating trust and seamless participation in the global digital marketplace.
- Worldcoin will provide universal access to the global economy.

here