A Blockchain Solution for Digital Identity Management for Refugees

Dr. B. Adrian Dina

Udacity:
Blockchain Developer
20 July 2024

Project Overview

Introduction: Refugees often face significant challenges in

- proving their identity and
- integrating into new communities

due to a lack of reliable identification documents.

We propose: A blockchain-based digital identity management system that provide a secure, immutable, and portable solution to address these issues.

Traditional Approaches

The traditional approach: We consider the schematic representation of refugee reception in Germany; we restrict on the first two steps of the actual registration process:

1. Arrival and First Contact:
   - After entering German territory, refugees must make contact with the authorities; this can be done at border posts, police stations, or directly at reception centers.
   - Afterwards, refugees are transported to an initial reception center called "Erstaufnahmeeinrichtung".
2. Reception and Identification:
   - At the reception center, personal data is recorded, including fingerprints and photographs.
   - After verifying the refugee's identity, they undergo a medical examination.

Some Challenges with Traditional Approaches

Some challenges regarding the traditional approach in the second step, Reception and Identification:

- Individuals arrive without proper documentation; some may have lost their documents, while others may intentionally discard them to obscure their origins.
- This can complicate efforts to ascertain the true identity and background of applicants, which is crucial for security and asylum determination purposes.

Our Blockchain Solution (1)

New Approach: We propose a blockchain-based digital identity management system (BBDIMS) that can provide a secure, immutable and portable solution to address these issues.

Arrival and First Contact:

- Upon first contact, authorities use a mobile app connected to the blockchain system to create a preliminary digital identity for the refugee; a unique identifier (given by a hashed version of initial biometric data) is generated and recorded on the blockchain, ensuring that the refugee's identity can be tracked securely from the outset.

Our Blockchain Solution (2)

Reception and Identification:

- Upon arrival at the reception center, detailed biometric data (fingerprints, photographs) are securely recorded using the blockchain system; this data is hashed and stored on-chain, with actual biometric files stored off-chain in a secure, distributed file system (e.g., IPFS). The blockchain ledger records the hash references.
- Smart contracts manage the identity verification process, ensuring that data is immutable and only accessible to authorized entities.

Our Blockchain Solution (3)

Reception and Identification:

- The blockchain system verifies the refugee's identity by cross-referencing the newly recorded biometric data with existing records on the blockchain, ensuring no duplication or fraud.
- Once identity is verified, a smart contract triggers the next steps, including medical examination; medical examination results are securely recorded and linked to the refugee's digital identity on the blockchain. This ensures that medical records are tamper-proof and can be accessed by authorized medical personnel only.

Our Blockchain Solution (4)

Some challenges related to our steps of consideration:

- Ensuring immediate and reliable access to the blockchain system for all border posts and police stations, which may have varying levels of technology infrastructure.
- Ensuring the accurate and secure collection of biometric data in a potentially high-stress environment.
- Managing potential duplicates and ensuring accurate identity verification across different locations and systems.
- Balancing transparency and accessibility of medical records with the need to maintain data privacy and comply with regulations.

Existing Solutions (1)

Question: What are the (major) problems in the current system(s)?

Arrival and First Contact:

- Inefficiencies and Delays;
- Lack of Immediate Tracking;
- Data Fragmentation;

Existing Solutions (2)

Reception and Identification:

- Recording Personal Data;
- Identity Verification and Medical Examination;

Blockchain: Hyperledger Fabric

Blockchain: Hyperledger Fabric (HF).

Consensus Mechanisms: Practical Byzantine Fault Tolerance (PBFT) and Raft.

Relevant parameters for our use case:

- Decentralization; medium - suitable for controlled environments.
- Performance; high - over 2000 tps.
- Transaction Throughput; very high, suitable for high-volume applications.
- Scalability; high - supports growing usage efficiently.

Blockchain: Hyperledger Fabric

Relevant parameters for our use case:

- Privacy and Security; high - robust privacy features and access controls.
- Integration and Flexibility; high - modular and flexible architecture.
- Compliance with Regulations; high - strong support for data protection regulations.
- Ease of Implementation; moderate - requires moderate expertise for deployment.
- Cost Efficiency; moderate - higher setup and maintenance costs.
- User Experience; high - user-friendly interfaces and systems.

Estimated Number of Transactions

Question: How fast the system needs to process transactions to meet demands (and still work well) as usage grows?

Activity	Frequency per Refugee	Total Transactions (Annually)
Initial Registration	1	100,000
Identity Verification	10	1,000,000
Data Updates	5	500,000
Access Logs	20	2,000,000
Total Annual Transactions	-	3,600,000
Total Monthly Transactions	-	300,000
Total Daily Transactions	-	9,860
Transactions per Second (tps)	-	0.114

Tabelle: System req. for an estimated number of refugees of 100,000 p.y.

Hyperledger Fabric Capabilities

Parameter	Requirement	Hyperledger Fabric Capability
Estimated Daily Transactions	9,860	high
Estimated tps	0.114	> 2000
Scalability and Performance	adequate	high

Conclusion:

- Given the extremely high transaction throughput of Hyperledger Fabric, the system can theoretically handle up to:

$$1,728,000,000$$

refugees per day (which is unrealistic for real-world scenarios).

- It shows that Hyperledger Fabric's capacity far exceeds typical and even extreme refugee numbers, ensuring that the system will not collapse under normal or even high-demand conditions.

Alternative blockchains

We considered the following (alternative) chains:

Criteria	Hyperledger Fabric	Quorum	Corda
Performance	high	high	medium
Transaction Throughput in tps	> 200	> 2000	170
Scalability	high	high	medium
Privacy and Security	high	high	very high
Integration and Flexibility	high	high	high
Compliance with Regulations	high	high	high
Ease of Implementation	moderate	moderate	moderate
Cost Efficiency	moderate	moderate	high
User Experience	high	high	moderate
Consensus Approach	Practical Byzantine Fault Tolerance, Raft	Raft, Istanbul BFT	Notary (Raft, BFT)

Summary: While Quorum and Corda have their strengths in privacy, security, and specific enterprise applications, Hyperledger Fabric stands out due to its:

- High transaction throughput and performance;
- Modular and scalable architecture;
- Strong compliance with regulatory standards.

Technical Implementation (1)

Let's focus on the technical implementation.

Overview:

- The high-level architecture will consist of multiple layers and components, with specific functions residing on the blockchain to ensure security, transparency, and efficiency.
- The architecture will also include off-chain components for data storage and processing that do not require the blockchain's immutability and decentralization.

Technical Implementation (2)

On-Chain Components:

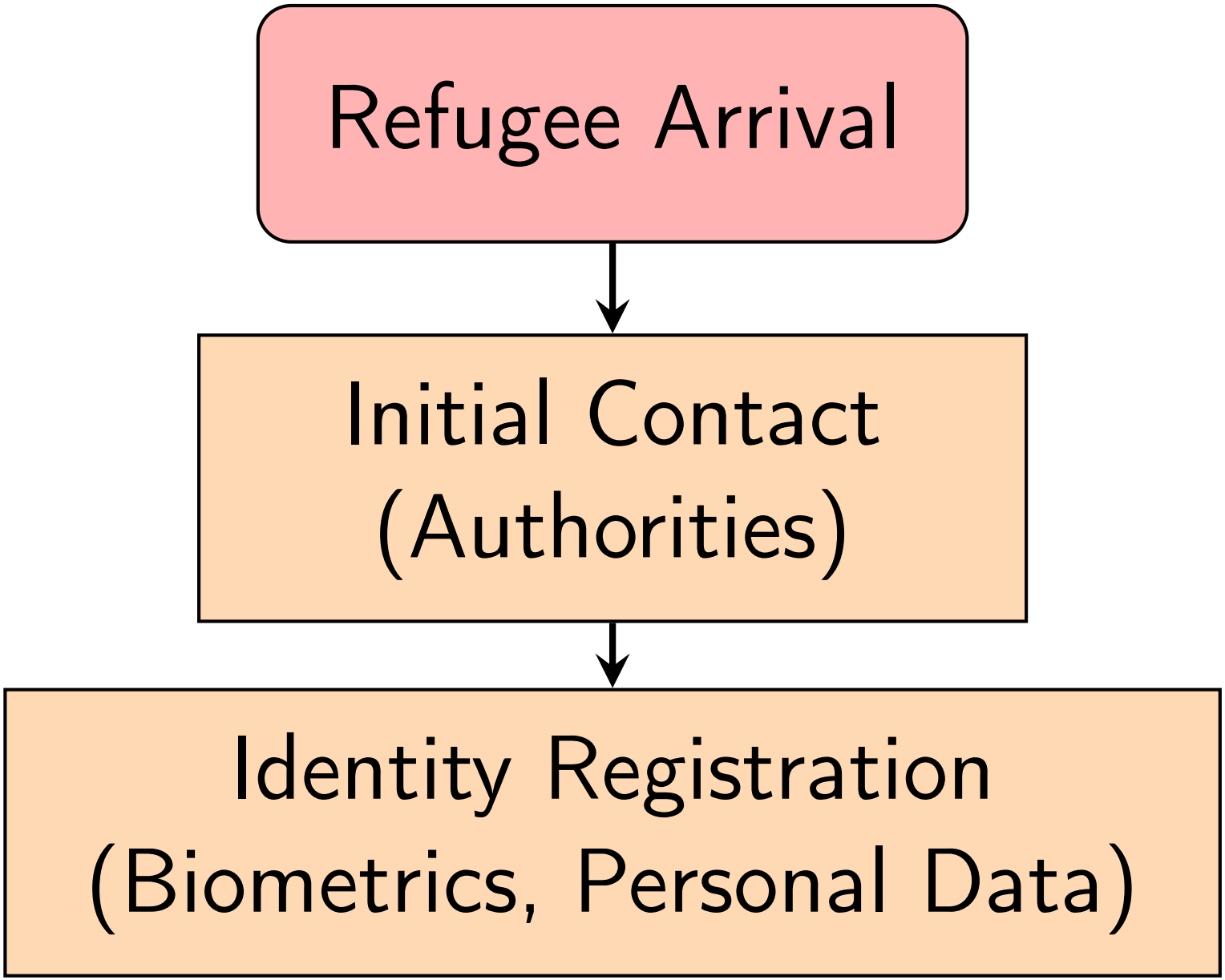
- Digital Identity Management:
  - Identity Creation and Registration;
  - Identity Verification;
- Access Control and Permissions:
  - Smart Contracts for Access Control;
- Transaction Logging:
  - Immutable Logs;

Technical Implementation (3)

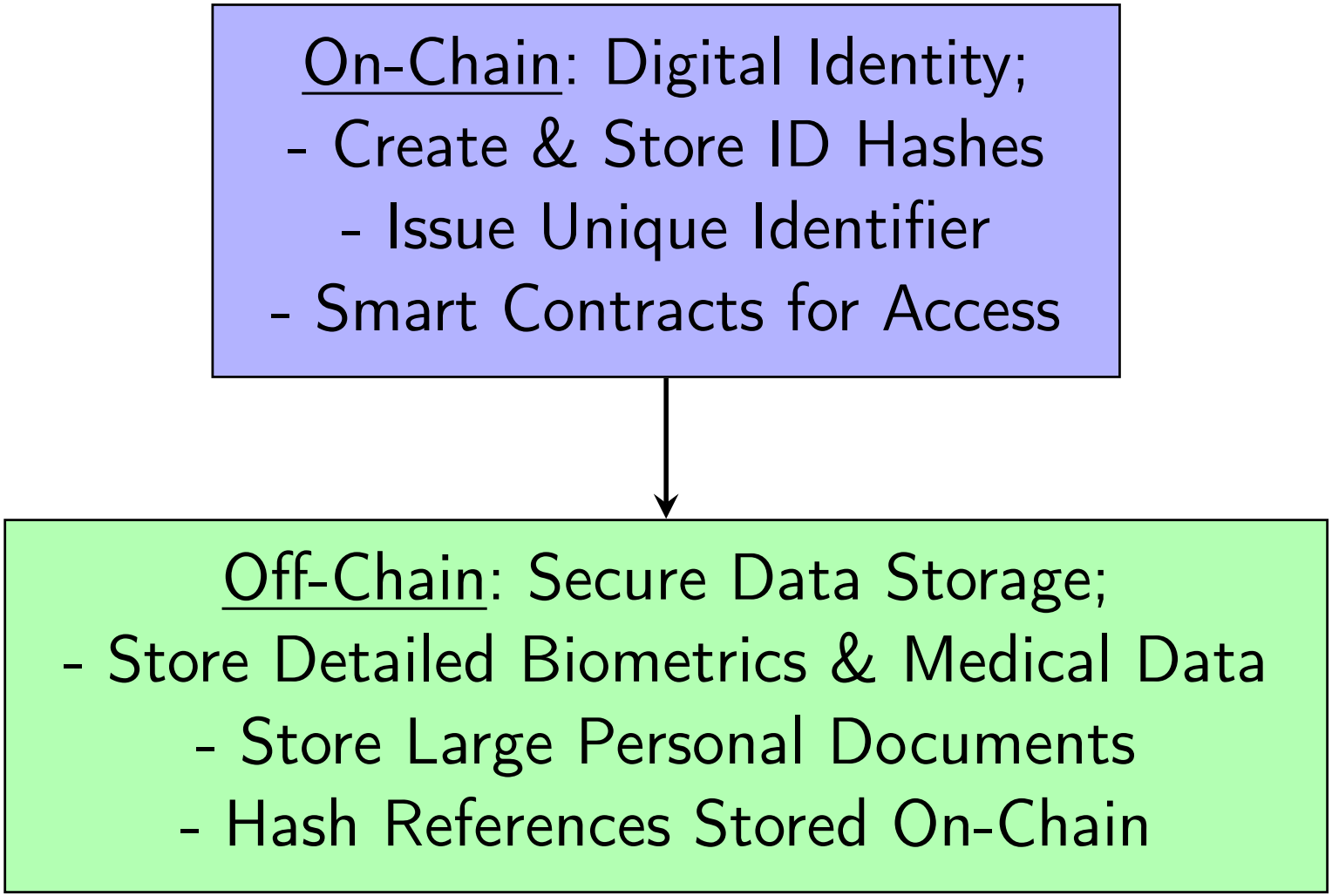
Off-Chain Components:

- Data Storage:
  - Secure Off-Chain Storage;
- Application Layer:
  - User Interfaces;
  - API Gateway;
- Middleware:
  - Integration Layer;

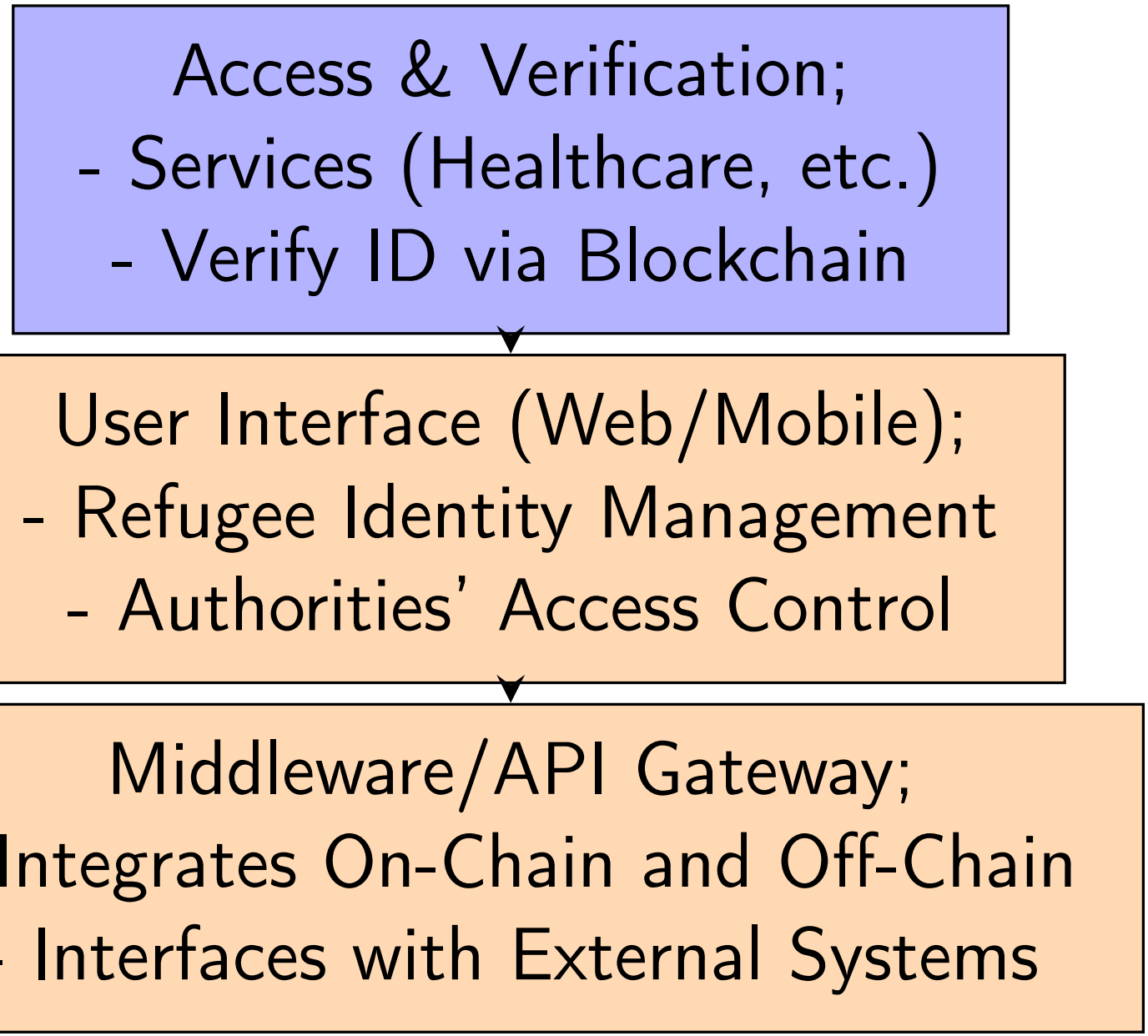
Architecture Diagram (1)



Architecture Diagram (2)



Architecture Diagram (3)



Architecture Challenges (1)

We present the two major challenges for our solution.

Data Security and Privacy:

- Challenge: Protecting sensitive personal and biometric data from unauthorized access and breaches.
- Addressing the Challenge:
  - Encryption;
  - Access Controls;
  - Regular Audits;

Architecture Challenges (2)

Adoption Incentives:

- Challenge: Encouraging stakeholders (government agencies, NGOs, refugees) to adopt and trust the new system.
- Addressing the Challenge:
  - Pilot Programs;
  - Stakeholder Engagement;
  - Incentives;

Alternatives to Complement Blockchain Aspects

Question: What alternatives could complement the blockchain aspects?

1. Distributed Storage Solutions:
   - Example; InterPlanetary File System (IPFS).
   - Function; store large files and sensitive data off-chain while using the blockchain to store hash references, ensuring data integrity and availability without overloading the blockchain.
2. Federated Identity Systems:
   - Example; Self-Sovereign Identity (SSI) Frameworks.
   - Function; allow refugees to manage their identities and control access to their personal data, enhancing privacy and user autonomy.
3. Cloud-Based Infrastructure:
   - Example; Amazon Web Services (AWS), Microsoft Azure.
   - Function; provide scalable and compliant infrastructure for off-chain components, such as secure data storage and API gateways.

Literature:

- https://www.hyperledger.org/projects/fabric
- https://goquorum.readthedocs.io
- https://corda.net
- Scholar GPT

Thank you for listening!