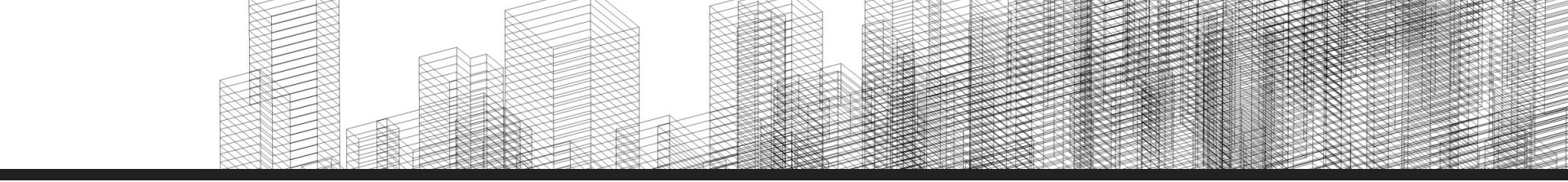
- BAVEBI -
Blockchain-based Attendance Validation Exploiting Biometrics Information

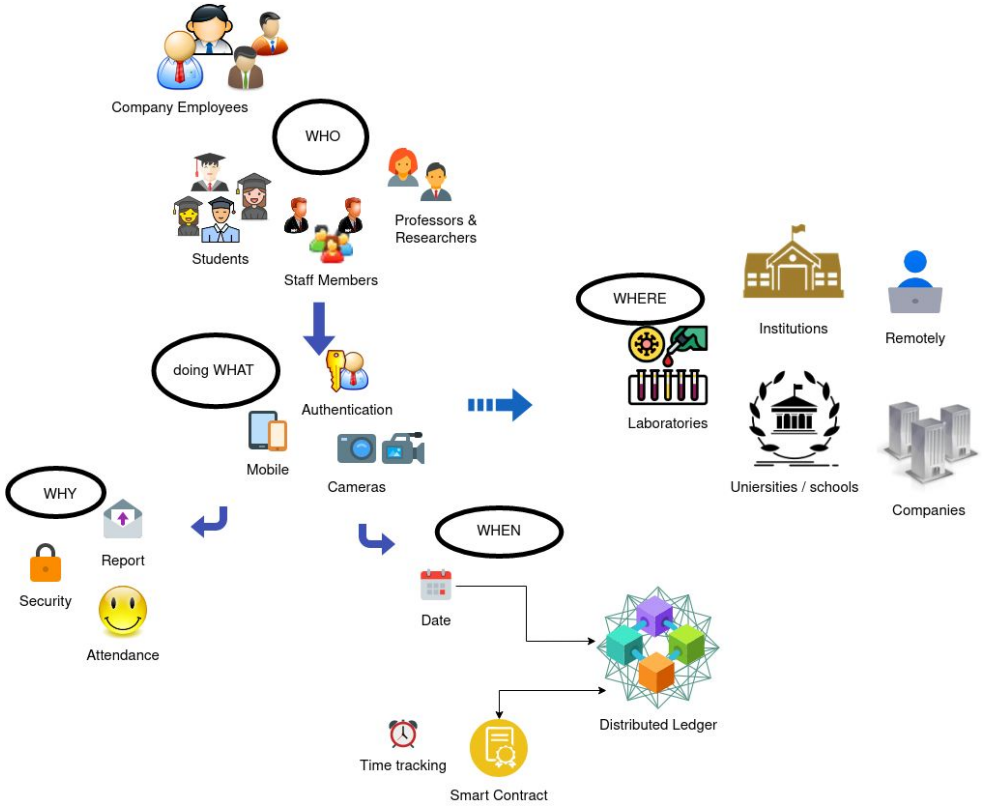
Ph.D. Michele Scarlato
Applicant for research position at Korean Culture Technology Institute (KCTI)



Presentation content

1. Description of the BAVEBI overall architecture.
2. Technical analysis of the three main phases:
   a. Storage of the biometrical information into the blockchain.
   b. Authentication employing Smartphone or Cameras.
   c. Execution of the Smart Contract to perform measurements.
3. A brief discussion of possible use case scenarios.
4. A short literature review of Blockchain-based Identity Management (BBIM) systems.

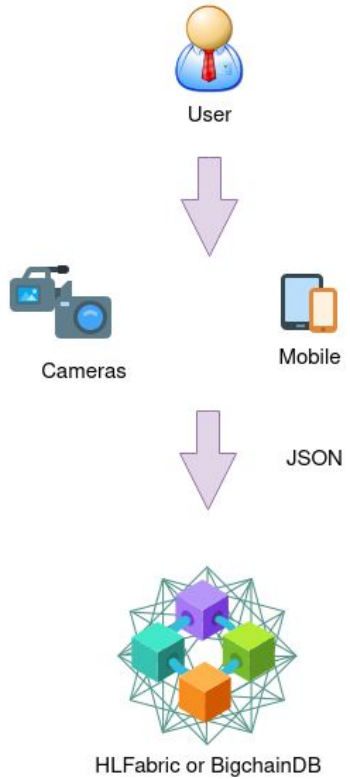
BAVEBI - a Blockchain-based Identity Management (BBIM) system for Attendance Validation Exploiting Biometrics Information.



Phase 1: storage of the biometrical information into the blockchain

1. Biometrical information - such as:
   a. picture -> Facial recognition.

   It can be stored in JSON format.
2. Permissioned blockchain such as Hyperledger Fabric and BigchainDB adopt an underlying layer of distributed NO-SQL databases, enabling JSON storage and query.
   a. HL Fabric : LevelDB and CouchDB
   b. BigchainDB: MongoDB.
3. Inserting users' biometric information into the blockchain increases authentication security. Blockchain vs. distributed databases provides data immutability and adds further authentication through cryptography keys.



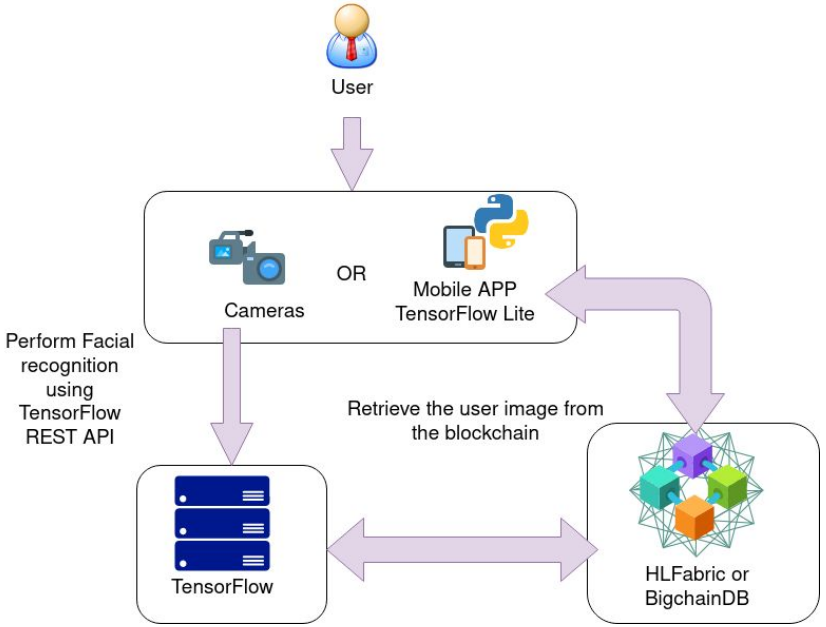
Phase 2: Authentication using Smartphone or Cameras - Facial Recognition

Facial Recognition (FR) algorithms require intensive resource consumption. A possible approach to perform it on a mobile phone is using TensorFlow Lite.

Performing FR using IP Cameras, or CCTV, requires a TensorFlow deployment on one or more server(s), using its REST APIs.

Both approaches rely on the dataset provided by the blockchain to match the user against the picture stored during the registration phase.

TensorFlow (server or mobile app) will parse the JSON retrieved from the blockchain, convert it into the original image, and execute FR.

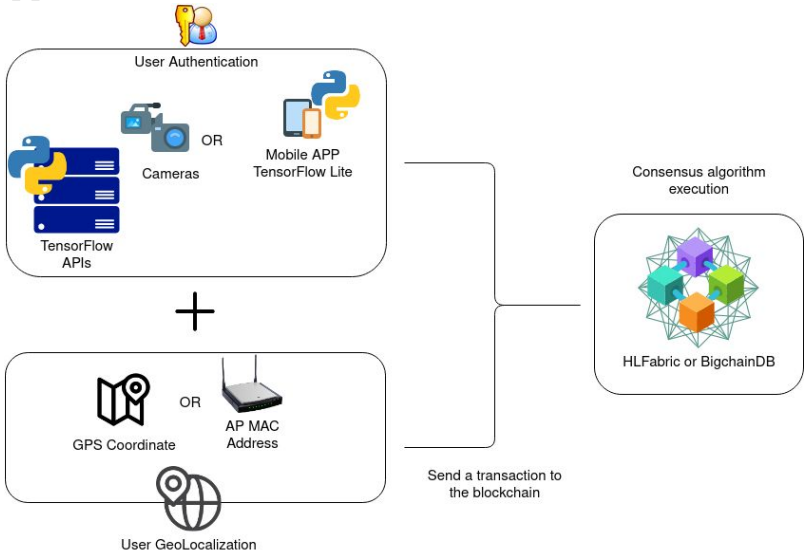


Phase 2: GeoLocalization using GPS information or Wireless Access Point MAC Addresses - and block creation.

GPS information or AP MAC address would guarantee the User presence within a specific area.
The more accurate will be inserted as metadata into a JSON and an authentication token generated by TensorFlow.

This JSON will be sent over the blockchain network as a new **transaction**.
The blockchain nodes will execute the **consensus algorithm**, *Tendermint* in BigchainDB, *Crash Fault Tolerance*(CFT) for HLFabric.

After the transaction approval, a **new block** will be added to the chain.



Phase 3: Smart Contract(SC)'s execution.

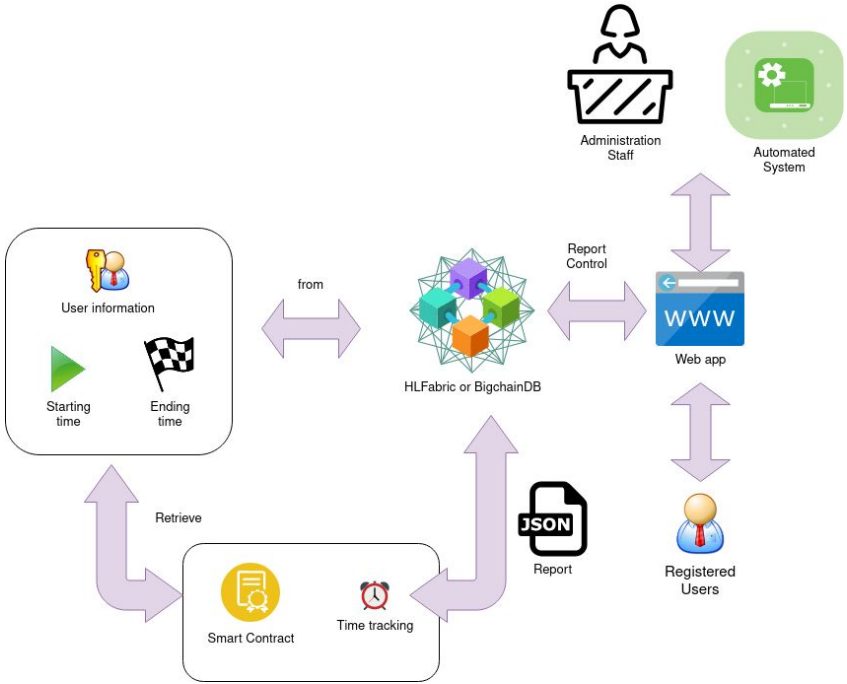
Once the user performs the logout, the SC will generate a report certifying the user's time at a particular location/event.

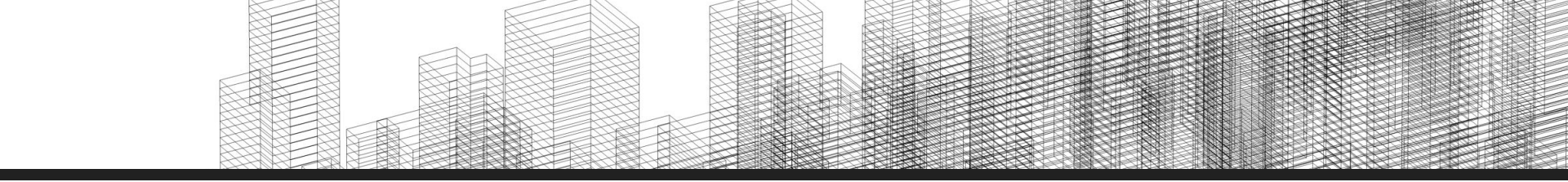
This report could be inserted as a JSON transaction and inserted in a new block after the nodes achieved consensus.

Administrative staff (or an automated system) and registered users can perform report control through a web app that interfaces to the blockchain.

HLFabric permits **channels** where data can be seen only by those subscribed to preserve the user's privacy.

BigchainDB does *not* offer a *native* functionality that prevents authenticated users from seeing only their data.
Implementing **cryptography with a key shared** between user and administration (or the automated system) would achieve this.



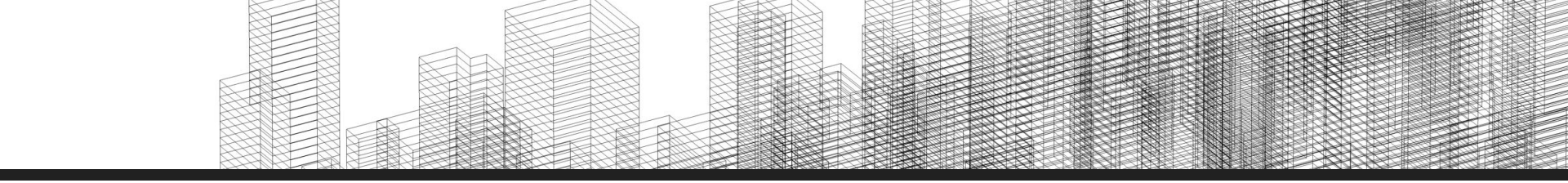


Phase 3: Smart Contract - how to implement it.

HyperLedger Fabric, which has a business logic, uses **Chaincode** (a form of Smart Contract), a program written in Go, Java, that implements an interface to the underlying db layer. A Python SDK is also available.

BigchainDB does not have business logic resulting in a con.
An critical pro is provided by the underlying distributed layer of MongoDB's, that thanks to the adoption of indexes offer better performances while querying JSON data with respect to LevelDB and CouchDB.

Business logic can be created ad-hoc for this specific application, e.g., creating a **web application** in JavaScript or Python performing the role of the *smart contract* (drivers for both languages are available and currently maintained).



Possible use cases.

Academic:

- **Universities**,
- **Schools** and **colleges**.

Will prevent tedious tasks such as collecting the *presences in class* or using *time trackers* during working time.

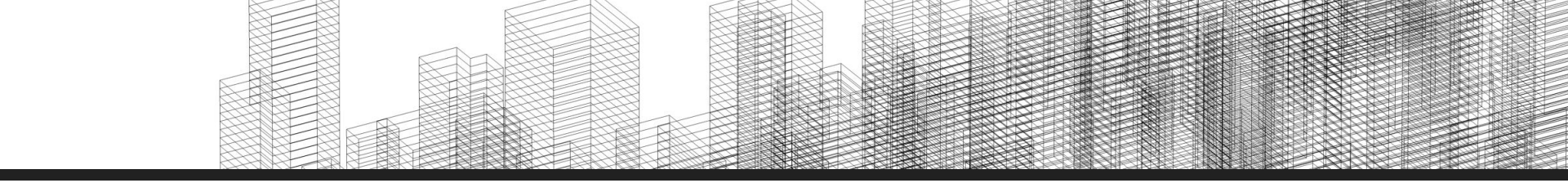
Corporations and companies:

- big **corporations** with several locations,
- small/medium **companies** that want to avoid the use of badges.

Both cases would benefit from the *augmented mobility* of their employees, using a safer *distributed authentication system*.

A short literature review of blockchain based biometric identity management systems

Ref	Authors	Source code	Implemented	Biometric type	Privacy	Use case
1	Bing Xu et al.	No	No	not specified	Biometric encryption	Foodchain
2	Ismatov et al.	No	Yes	FR	not addressed	BBIM - User attendance
3	Bing Xu et al.	No	No	FR/fingerprint	Biometric encryption	Intelligent Vehicles - VANET
4	Páez et al.	No	Yes	Iris/fingerprint	not addressed	BBIM
5	Sarier ND	No	Yes,partially	not specified	Brands - GDPR compliant	Industrial IoT Identity Management
6	Sarier ND	No	Yes	fingerprint	GDPR compliant	Blockchain based Identity Management (BBIM)
7	Dinesh et al.	No	schema	not specified	hashing approach	BBIM



References

[1] Xu, Bing, Tobechukwu Agbele, and Richard Jiang. "Biometric blockchain: A better solution for the security and trust of food logistics." IOP Conference Series: Materials Science and Engineering. Vol. 646. No. 1. IOP Publishing, 2019.

[2] Ismatov, Akobir, Vanessa Garza Enriquez, and Madhusudan Singh. "FaceHub: Facial Recognition Data Management in Blockchain." Blockchain Technology for IoT Applications (2021): 135.

[3] Xu, Bing, Tobechukwu Agbele, and Richard Jiang. "Biometric Blockchain: A Secure Solution for Intelligent Vehicle Data Sharing." Deep Biometrics. Springer, Cham, 2020. 245-256.

[4] Páez, Rafael, et al. "An Architecture for Biometric Electronic Identification Document System Based on Blockchain." Future Internet 12.1 (2020): 10.

[5] Sarier, Neyire Deniz. "Efficient biometric-based identity management on the Blockchain for smart industrial applications." Pervasive and Mobile Computing 71 (2021): 101322.

[6] Sarier, Neyire Deniz. "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management." Computers & Security 105 (2021): 102243.

[7] Dinesh, Amara Devendra, et al. "A Durable Biometric Authentication Scheme via Blockchain." 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). IEEE, 2021.