Biometric authentication is based on the initial acquisition
of a template associated with one or more of the user’s biomet-
ric features and the comparison of subsequent acquisitions of
the same biometric features with the initial template [1]. From
the biometric authentication paradigm itself, two fundamental
and opposed requirements naturally arise:

i) Template protection: biometric characteristics, in addition
to being credentials, and thus confidential, are also per-
sonal data, so they must be protected even better than
common passwords [2].

ii) Authentication portability: after initial enrolling in one
place or device, users would like to port their biometric
authentication to other systems and devices as well,
without necessarily having to repeat the initial enrollment.

A commonly adopted solution to enable biometric authenti-
cation on different systems without having to repeat the initial
enrollment step is to rely on a single device performing bio-
metric authentication (e.g., a smartphone with face, fingerprint,
or iris recognition), associated with a single sign-on
system
(e.g. operated by some identity provider) that allows successful
authentication, once executed, to be transferred across various
services. Although this approach is very effective and widely
used today, it relies on a single device able of performing
biometric authentication, and this is a limitation in terms of
security and scalability of the system.

Blockchain and distributed ledger technology (DLT) repre-
sent an important innovation and provide a decentralized
digital infrastructure characterized by the absence of single
points of failure. We propose a solution to implement a
decentralized biometric authentication system that leverages
the blockchain technology. The main advantage over classic,
centralized biometric authentication systems is that of allowing
each user, after an initial enrollment phase, to be authenticated
from any device participating in the network, rather than only
from the one to which he or she initially registered. The
main challenge to achieve this is the public nature of the
data stored in the blockchain, which is not compatible with
the sensitive nature of biometric data. To overcome such an
issue, we leverage fuzzy commitment schemes allowing to
perform biometric authentication in the encrypted domain.
This, along with a public blockchain and a suitable smart
contract, allows us to design a set of protocols able to achieve
the desired target. Few previous studies to date have looked
at the the integration of biometrics and blockchain [3]–[5],
but the proposed solutions do not achieve the same levels of
scalability and security that the solution we propose is able to
achieve, mainly because of the use of fuzzy commitments.

The system we propose, which is schematically described
in Fig. 1, exploits a public blockchain (like Ethereum), a
managing smart contract (SC) and two types of nodes: en-
rollment centers (ECs) and authentication centers (ACs). Each
EC can register one or more authentication centres (ACs) by
writing their blockchain addresses into an AC list maintained
by the SC. Each EC is also responsible for the enrollment
of users by registering their blockchain addresses along with
their biometric templates (in the encrypted domain, through
fuzzy hashing) into a user list maintained by the SC. Biometric
authentication of any enrolled user can then be performed by
any AC through the protocol we propose, the main steps of
which are described next.

A. Initial setup

The system is setup by some initiating body (e.g., a govern-
mental institution), which, however, does not become a central
authority of the system itself, which has a decentralized nature.
Such an initial setup is performed by deploying the SC onto a
public blockchain and including one or more initial ECs into
the SC list. The SC provides a payable function that allows
new data to be written into the blockchain and some non-
payable functions used to retrieve data from the blockchain.
The payable function can be invoked only by ECs, which are
responsible for the enrollment of end users and ACs. The latter
are limited blockchain nodes responsible for performing users’
authentication based on data retrieved from the blockchain.

B. Registration stage

The registration stage allows new ACs and ECs to be
incorporated into the system. In fact, by invoking the SC, an
existing EC is responsible for storing onto the blockchain the
addresses and the data of new ACs. Each newly registered AC
is provided with read-only permissions by the SC. As a special
case of registration, an EC can provide write permissions to the
registered node, which is then elevated to the same hierarchical
level of the EC, thus becoming in effect a new EC.
C. Enrollment stage

This stage is a modified version of the enrollment stage in the fuzzy commitment scheme (FCS) [6] to suit the interaction with the blockchain. Enrollment can be performed by any EC, and starts by generating a random key $K$ when a new user requires to be enrolled into the system. From the key $K$, a codeword $C$ is generated using linear encoding through an Error Correcting Code (ECC). The codeword $C$ is then XORed with the user’s biometric features $x$ extracted from the acquisition of some biometric data $b$, to generate the offset $\delta$. At the end of the enrollment stage, the offset $\delta$ along with the hash of the key $h(K)$ are stored onto the blockchain for each biometric feature associated to the user ID.

D. Authentication stage

This stage allows any user enrolled into the system to be authenticated from any AC, and it consists in a modified version of the fuzzy commitment scheme (FCS) verification stage [6] to suit the interaction with the blockchain. The user requiring to be authenticated communicates his/her ID to the AC, along with some new biometric feature acquisition $x'$. The AC retrieves the corresponding values of $\delta$ and $h(K)$ from the blockchain. The biometric feature $x'$ is then XORed with the offset $\delta$ to generate a noisy codeword $C'$, which is given as input the ECC decoder. If the ECC decoder is able to compensate the noise affecting $C'$ (which occurs when the new biometric acquisition is close to the original one), the original codeword $C$ is retrieved, which is then demapped into the correct key $K$. By comparing the digest of the latter with the value of $h(K)$ retrieved from the blockchain, the AC decides whether the user authentication is successful or not.

E. Revocation stage

According to GDPR and data protection best practices, each users must be granted the right to be forgotten from the system. In the framework we propose, this right can be enforced by any EC. In fact, any EC can invoke a payable function of the SC that erases the user record from the list of enrolled users. Despite ACs will no longer be able to retrieve data concerning revoked users and thus perform their authentication, their registration data will still be stored within past transactions. However, these data are stored in encrypted form, according to the fuzzy commitment paradigm, and no personal data of revoked users can be retrieved from them.

More details concerning each one of the above stages that constitute the system we propose will be provided in the presentation, along with a detailed security analysis.

REFERENCES