Private Digital Identity on Blockchain

Tom Hamer, Kerry Taylor, Kee Siong Ng, Alwen Tiu

College of Engineering and Computer Science, The Australian National University,
Canberra ACT 0200, Australia
tomhamer@live.com, kerry.taylor@anu.edu.au, keesiong.ng@anu.edu.au
alwen.tiu@anu.edu.au

Abstract. For many identification systems, including those in government, finance and healthcare, it is critical that at most one identity exists for each human individual within a given system. Many existing approaches identify individuals through an exchange of verifiable documents attesting to basic identification information. However, the same basic information is collected for identification in almost every system, meaning that persons are linkable across different identity systems and are not in control of how their identity is used. We propose Unique Self-Sovereign Identity, (USI), combining Cancelable Biometrics [6] and W3C Verifiable Claims [8] to achieve privacy preserving and non-linkable identification, with guarantees against double enrolment with any system. Because our protocol is based on biometrics, it permits individuals to enrol without official identification documents. Our protocol can be used in a wide range of situations, offering data security for large organisations, access to basic services for over one billion people who lack official identifying documents, and personal identity control for all individuals.

Keywords: Verifiable Claims · Blockchain · Cancelable Biometrics · Homomorphic Signature

1 Introduction

1.1 Motivation

One fundamental aspect of many human identification systems is that for each individual, no more than one identity exists [1]. This is often due to an unfair advantage that can be gained by a malicious individual having two identities, for example, they may be able to fraudulently access additional credit at a bank [2]. However, preventing malicious double enrolment is difficult. Many existing approaches uniquely identify individuals through an exchange of verifiable documents and basic identification information [3]. However, these traditional identification methods have a number of fundamental drawbacks:

1. Through organisations storing basic identity attributes such as name, birthdate and address, individuals can be linked across multiple independent uses of their identity, without consent.

2. When organisations requiring identity verification store a large amount of information about each individual for identification purposes, it makes the

system vulnerable to attacks, as it is easy for a hacker who obtains access to the internal records to learn many details about each individual. Worse still, basic attributes such as address cannot easily be cancelled or changed and so a fresh identity is very hard to establish.

3. Over 1 billion individuals worldwide lack a form of officially recognised identity such as a passport [4], which makes it very difficult to enrol with service providers–such as banks, which need to uniquely identify individuals.

We propose a decentralised, privacy-preserving identity system which can identify individuals through a bijective mapping from individuals to identifiers used in a specific organisational context. It is designed to give individuals control over their own identity and shared information but to give organisations a guarantee of uniqueness. To our knowledge, such a privacy preserving biometric identification system does not exist in the literature.

1.2 Related Work

Biometrics are a useful tool in identification of individuals because biometric signatures, such as fingerprints, are unique to each human [5]. Further, they do not depend on an individual needing to hold official identity documents. Cancelable biometrics have been created as a method to protect biometric signatures; rather than storing the full biometric in identification databases, biometrics are non-invertibly transformed to obfuscate the original biometric signature [6], and only the obfuscated version is stored. However, one problem with current cancelable biometric protocols is that the individual must trust the organisation receiving their biometric signature to correctly transform and securely manage the biometric signatures.

Homomorphic signatures allow a verifier to prove that a calculation has been done correctly without having to access the underlying data [7]. We propose utilising homomorphic signatures as a proof mechanism to allow the individual to obfuscate their own biometric signature on their personal device through applying a specific non-invertable transformation that is requested by the organisation wanting to identify the individual. The authors are unaware of previous research proposing the use of homomorphic signatures to prove the validity of cancelable biometrics. For the first time, we propose that the combination of these techniques enables self-sovereign identity.

The W3C, an international standards organization, has introduced Distributed Identifiers (DIDs) and Verifiable Claims. DIDs are linked to DID documents, which store mechanisms used to authenticate the DID, service endpoints, and other claims [8]. Using DIDs, the W3C aims to create a standard for individuals and organizations to control their own identity. W3C Verifiable Claims are a mechanism to express credentials on the Web in way that is cryptographically secure, privacy respecting, and machine-verifiable [9]. The Sovrin foundation has used DID and Verifiable claims to create a Blockchain based Identity System [10], which enables distributed management of public keys and revocation of verifiable claims. Similarly, we propose to facilitate transfer of obfuscated biometrics using Blockchain-based verifiable claims.

Self-sovereign identity can be defined as “the concept of individuals or organizations having sole ownership of their digital and analogue identities, and control over how their personal data is shared and used” [11]. A number of organisations including The Sovrin Foundation [10], Civic Ledger [13] and uPort [14] have recently launched of self-sovereign identity protocols. The Sovrin Foundation has been involved in the development of ID2020 which aims to create an open and human-centric approach to identity [12]. They suggest benefits including no physical papers and the convenience of biometric authentication. Other attempts, such as Civic ledger’s solution, depend on the individual holding official identity documents such as passports to enrol with their system, which is problematic for displaced persons and others.

No self-sovereign identity schemes are currently available which offer non-linkability of individually-controlled identities. Where existing protocols offer the capacity to use biometric signatures, they do not allow individuals to non-invertably transform their biometric signature before it is sent, and therefore do not protect the privacy of personal biometrics.

We propose the concept of Unique Self-Sovereign Identity, or USI. USI means that an individual can have at most one identity in a particular context, but identities cannot be linked between contexts without permission from the individual. Therefore, individuals can be uniquely identified but still have control over their personal identifying data.

2 Solution Sketch

2.1 Our USI protocol

We define three key roles:
Individual: a human who wants to be identified by a Service Provider.
Service Provider: an organisation requiring its individual users to complete identity verification for access to services. The service provider commits to requiring a specific variety of biometric for all of its users.
Trusted Organisation: an organisation within the trust network of both a service provider and an individual. Service providers trust these organisations to ensure that the biometric signatures are accurate and individuals trust these organisations to destroy their biometric signature immediately after use. Trusted organisations maintain public keys for each variety of biometric signature they sign, meaning that service providers are able to verify that the biometric signature is of the variety they require.

In our protocol, each individual is identified for each service provider by a cancelable (non-invertibly transformed) version of their biometric signature. To achieve this non-invertibility, we use a Partial Discrete Fourier Transform for non-linkable biometrics [6]. We extend existing cancelable biometric schemes so that the service provider never has access to the complete biometric signature of each individual. To enable this, we use fully homomorphic signatures [7] to prove the validity and correctness of a biometric signature which is already

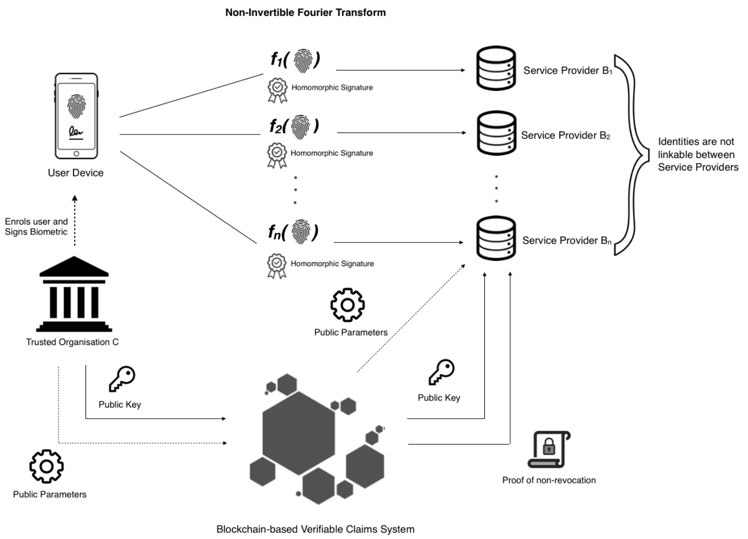

Fig. 1: Our USI Protocol showing the interactions between an Individual represented by a User Device, a Trusted Organisation, and several Service Providers

non-invertibly transformed by the individual before it is sent. Finally, the solution uses a Blockchain W3C standard Verifiable claims system [10], where our homomorphic signature acts as the proof mechanism, meaning that individual biometric signatures can be revoked when needed, and requiring that the public key of the Trusted Organisation is publicly available. Our protocol does not address authentication, that can employ conventional means such as username and password. Our protocol is as follows (see figure 1).

1. The individual enrols for an identity with a trusted organisation C of their choice (see Algorithm 1). C collects finger print and vein scans, ensuring that the biometrics are collected accurately and are truly the biometrics of the individual. The assurance process will be determined by C's own policy, but will probably include human supervision. The individual stores the biometrics together with a corresponding signature which is provided by C. C must not store the biometrics–and is trusted not to by the individual. C has its public key available on the Blockchain Verifiable Claims system. C adds required randomly generated public parameters for homomorphic signature verification to the ledger, and adds the signature for the biometric to a public revocation register, attesting to the validity of the biometric.

2. The individual wants to enrol with a service provider B_i and B_i requires proof that they have not enrolled previously with B_i. To check, B_i requests an P-DFT transform [6] with the trusted organisation's specific parameters, from the individual. These parameters are derived using the public key of B_i and are therefore not used by any other organisation requiring identity verification.

The individual computes the result of the transformation and sends it to B_i, with a fully homomorphic signature under that P-DFT, along with the name of trusted organisation C for lookup in the Blockchain Verifiable Claims Public Key register. Verifying that the calculation was done correctly does not require the individual to send the initial signature from C or the individual's raw biometric.

3. Service provider B_i looks up trusted organisation C's public key on-chain and verifies the homomorphic signature against the transformed biometrics sent by the individual, the public parameters, and the public key of C (see Algorithm 2). If it holds as valid, and the proof of non-revocation holds, then B_i checks all current biometric vectors in its database for any vectors within a thresholded similarity of the provided biometric. If it finds no matches, then B_i has verified that the individual has not previously enrolled.

Algorithm 1 Trusted Organisation Creates Verifiable Claim for Individual to Store

```
procedure VCGEN($pk, device$)
    $bVec \leftarrow$ retrieve($device$) //retrieve processed biometric vector for individual
    from trusted organisation's external device
    $l \leftarrow$ length of $bVec$
    $V \leftarrow$ randomly generate $l$ public parameters
    $x \leftarrow \mathrm{Sign}_{sk}(bVec)$//trusted organisation homomorphically signs the biometric
    vector using its secret key
    writeToChain($V$) //write the public parameters $V$ onto the Blockchain
    $claim \leftarrow$ generate a verifiable claim from trusted organisation's metadata [9]
    $claim.proof \leftarrow$ generate a proof property from signature $x$
    addToNonRevocationRegister($claim$) //add the claim to a public non-
    revocation register
    cleanup() //critically, trusted organisation must delete $bVec$, the user's raw
    biometric vector
    return $claim$
```

2.2 Features of our USI System

Self-sovereignty: The identity holder has complete control over storage and use of their identity. This is provided through the use of verifiable claims, and the homomorphic proof mechanism, which allows individuals to reliably store their own biometric signature [9],[7].

Privacy and Non-linkability: The verifier, who receives a non-invertibly transformed version of the biometric is unable to reverse the transformation and discover the individual's actual biometric signature. Provided that the transformations have different parameters, cross matching of biometrics is impossible. These privacy and non-linkability features are provided by definition through cancelable biometrics [5]. Further work is required on the non-linkability of the proof mechanism as it is in some cases possible for proofs to be linked via the

Algorithm 2 Service Provider Enrols Individual

```
procedure AddNewUser($p_i$, biometricVariety, similarityThreshold) //$p_i$ is unique to each service provider
    $claimPres \leftarrow$ request verifiable claim for P-DFT biometric transform from user with parameters $p_i$
    $sig \leftarrow claimPres.proof.proofValue$ // extract the transformed biometric from the claim presentation [9]
    $transbVec \leftarrow claimPres.credentialSubject.transformedBiometric$ // extract the proof from the verifiable claim presentation [9]
    $V, pk \leftarrow$ retrieve(biometricVariety) //get public parameters V and trusted organisation's public key for the biometric type$pk$ from Blockchain
    if not $\text{valid}_{pk}(V, sig, transbVec)$ or isRevoked($claimPres$) then
        //if the homomorphic signature does not hold, or the claim has been revoked
        return false
    for transformedBiometric in database do
        if $transbVec$.isSimilar, similarityThreshold($transformedBiometric$) then
            return false //if a similar biometric exists already then reject.
    addNewUserToDb($transbVec$) //save transformed biometric
    return true //success
```

public parameters. This issue may be rectified either through Gorbunov's multi-data signing scheme [7] or by having the trusted organisation issue a number of public parameters to each individual, and each one could be used to establish an unlinkable identity.

Unique Identification: An individual can create as many signed biometrics or identities as they like and enrol with any trusted organisation. The transformation will always map them back to the same identifier, with an error rate that is dependant on the quality of the matching algorithm and the number of individuals in the system. This is irrespective of the trusted organisation and is a result of biometric classification algorithms. The error rate arises from the imprecise nature of biometric feature extraction. Note that each Service Provider must require the same variety of biometric from all of their clients, or unique identification is impossible. [5].

Decentralisation: The trusted organisations do not have to communicate or be in consensus for the **Unique Identification** property to hold. This is enabled through Blockchain technology, which allows public keys and parameters to be stored without a central authority [10].

Biometrically Derived: Biometrics are used, meaning that the system does not depend on individuals holding previous identity documents in order to enrol.

3 Conclusion

We describe a USI identity system which is capable of addressing number of significant current challenges in identity management. A key area for further work is improving the performance of biometric identification. The error rate could prove to be an obstacle due to the compounding of errors in biometric identification systems [15]. The need to trust the trusted organisation's management of biometric data is a potential drawback of our protocol that could be addressed by legal or social mechanisms. Personal enrolment with the trusted organisation potentially exposes information about identity that could be exploited. However, we believe that this system could be feasible for distributed and privacy preserving identification at large scale. Future work includes a reference implementation and security analysis.

References

1. UNHCR.: UNHCR Resettlement Handbook. UNHCR - the UN Refugee Agency, Geneva (2011)
2. Saunders, K., Zucker, B.: Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. In: International Review of Law, Computers & Technology 1999, 2, pp 183–192. Routledge (1999).
3. Moyano, J. P., Ross, O.: KYC Optimization Using Distributed Ledger Technology. Business & Information Systems Engineering, 59(6), pp 411-423. (2017).
4. Kour, G. & Saabne, R.: Global Identification Challenge by the Numbers. http://id4d.worldbank.org/global-dataset/visualization. Accessed 30 July 2019.
5. Punithavathi, P., Subbiah, G., 2017. Can Cancelable Biometrics Preserve Privacy? Biometric Technology Today, 2017(7), pp 8–11.
6. Yang, W. et al.: A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recognition, Volume 78, pp 242–251. (2018)
7. Gorbunov, S., Vaikuntanathan, V., Wichs, D: Leveled Fully Homomorphic Signatures from Standard Lattices. In: STOC'15 Proceedings of the forty-seventh annual ACM symposium on Theory of Computing, pp 469–477. ACM, New York, NY, USA (2015)
8. Reed, D. et al.: 2019. DID Spec. https://w3c-ccg.github.io/did-spec/. Accessed 30 July 2019.
9. Sporny, M. et al.: Verifiable Credentials Data Model, https://www.w3.org/TR/vc-data-model/. Accessed 30 July 2019.
10. Sovrin.: Sovrin Protocol and Token White Paper. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf Accessed 30 July 2019.
11. Metadium.: Introduction to Self-Sovereign Identity and Its 10 Guiding Principles. https://medium.com/metadium/introduction-to-self-sovereign-identity-and-its-10-guiding-principles-97c1ba603872. Accessed 30 July 2019.
12. Leong, C.: ID2020: Digital Identity. https://www.accenture.com/us-en/insight-blockchain-id2020. Accessed 30 July 2019.
13. Civic Technologies.: Civic Whitepaper. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf. Accessed 30 July 2019.
14. Dunphy, P., Petitcolas, F.: A First Look at Identity Management Schemes on the Blockchain. https://arxiv.org/pdf/1801.03294.pdf. Accessed 30 July 2019.
15. Pato, J. N., Millett, L. I.: Biometric Recognition: Challenges and Opportunities. Washington, DC: The National Academies Press. (2010)