# Chapter 11
# The Biometric Signature as a Blockchain Application


**Ahmet Koltuksuz**

## 11.1 The Definition and the Function of a Signature

A signature is a person's name or a nickname handwritten by himself or by herself as a proof of intent and identity for the authorship of the contents of a document. Traditionally, the primary function of a signature has been to create a binding in between a person and a record by perpetually attaching a person's uniquely identifiable handwritten sign as direct evidence that the document that is in part or in whole belongs to that person.

Therefore, the peculiarities of a given signature to fulfill this traditional function are that it should be authentic, unique, unforgeable, undeniable, unalterable, and not reusable and must be created in such a way that it cannot be repudiated.

The determination of the genuineness of the signature has been a problem for centuries. Even today, when a signature drawn by a person's handwriting with the use of a pen, which in such a case is known as the wet signature, is in question in court, many measures must be taken by the forensic laboratories of law enforcement bodies to determine whether the signature is authentic or not. All the metrics and endeavors related to a wet signature are bundled together under the science of graphology.

In the history of humankind, every century has witnessed some technological advancements like that of the invention of the wheel, a clock, steam engines, electricity, and electrical motors until the twentieth century. All these technological improvements have changed societies and their lifestyles tremendously, however, without much affecting the belonging proving methodologies. The signature, produced as a handwritten wet signature for proof of belonging, has always been around

A. Koltuksuz (✉)
Yasar University, Izmir, Turkey
e-mail: ahmet.koltuksuz@yasar.edu.tr



T. Choudhury et al. (eds.), *Blockchain Applications in IoT Ecosystem*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-65691-1_11

for hundreds of years, that is, until the era of Information and Communication Technologies (ICTs).

The Internet, a direct result of the ICTs, has changed humankind unprecedentedly and thus very much deserved to be defined as a game-changer. Thus, the concept of a traditional handwritten wet signature has witnessed quite a few new forms that are altogether different in structure and generation than the classical one the very first time many centuries after. So, the game both for the production and forensics of signature has changed radically.

## 11.2 A Brief Literature Review on Digital Signatures

The digital signature is a protocol-level application of an asymmetrical cryptosystem. It is the direct result of a combination of both the hash functions and the asymmetrical encryption. In contrast to a symmetrical cryptosystem, in which there is only one key utilized for both processes of encryption and decryption, there are two separate keys involved for each operation in asymmetrical cryptosystems.

The idea belonged to Merkle [1] and Diffie and Hellman [2]. The methodology put forward by these researchers declared that the keys should be created in pairs and be utilized one by one for the processes of encryption and decryption. Moreover, in mathematical terms, it should be intractable to generate one key from the other. The encryption key which belongs to the receiver is publicly known and thus employed by anybody in the process of sending a message to that specific receiver. That way, the encryption key was renamed as the public key.

On the other hand, the legitimate receiver is the only possessor of the decryption key. Thus, as in the renaming of the encryption key, the decryption key is renamed as the secret key. Today, by this renaming convention, the cryptographic system is designated as the public key cryptography (PKC) and the related hardware and software infrastructure as the public key infrastructure (PKI).

The Institute of Electrical and Electronics Engineers (IEEE) standardized PKC as P1363-2000 [3].

While PKC is one compound of the digital signature, the hash functions are the other. A mathematical hash function of h is given as:

$$H = h(m) \tag{11.1}$$

where h is the hash function, m is the variable length message, and H is the fixed length hash value of the message. The hash value for the message can also be termed as the message digest, as the fingerprint, or as the digital fingerprint of the message. The peculiarities of a hash function are as follows: (i) the hash value should be computed in P time for any given message of m; (ii) the hash function should be a one-way function, that is, it must be computationally intractable; and (iii) there should only be one hash value for any given message which means that the hash function should be collision-free.

**Table 11.1** An algorithm in pseudocode for the creation of a digital signature

| Step number | Pseudocode |
|---|---|
| **1** | **start** |
| **2** | **read the plaintext as the message (m)** |
| **3** | **apply SHA function to (m) to obtain the 512bit hash value (H)** |
| **4** | **apply PKC to encrypt the (H) with sender's SECRET key to obtain the digital signature (DS)** |
| **5** | **append (DS) to the end of (m) to sign the message** |
| **6** | **end** |

Secure Hash Algorithms (SHA) have been standardized by the US National Institute for Standards and Technology (NIST), and they produce H values with 160, 256, 384, and 512 bits, respectively [4].

### *11.2.1 Conventional Digital Signatures*

When combined with a hashing function, as mentioned above, one of the marvelous outcomes of asymmetrical cryptosystems is a digital signature. Whether one chooses either the RSA or elliptic curve or ElGamal cryptosystem as the PKC, the digital signature can be created and be added to the document after a couple of steps. The algorithm for digital signature creation is given in Table 11.1.

Currently, one can obtain a digital signature either by having the asymmetrical keys stored on a flash memory to be utilized through the USB port of a computer or having these keys on a SIM card of a mobile phone, which in that case it is called as the mobile signature. However, each of these technologies heavily underlines a hardware dependency; thus, user reluctance has always been an issue for those systems.

### *11.2.2 Server Signing*

Nevertheless, there is one alternative way of digital signing known as the server signing, which runs with asymmetrical keys that are stored on a networked server, and the digital signature is created by that server whenever there is a demand by the signee.

Server signing is founded upon the EU regulation on "electronic identification and trust services for electronic transactions" known as eIDAS [5]. eIDAS might be considered as one of the underlying framework regulations for server signing standard CEN/TS 41924 [6]. The server signing option frees the users form hardware dependencies. However, it is not free from the complexities of the networking hardware and software.

Although a digital signature thus obtained is mathematically proven to be secure, it is nevertheless not so easy to utilize by the signees, and unfortunately, underlying computing intractabilities are susceptible to quantum computing attacks, which seems to be the new revolutionizing technological breakthrough in the days to come along with IoT.

## 11.3 The Biometric Signature

Biometric authentication can be done in many ways, such as retina, voice, palm, or fingerprint recognition. Along with these, behavioral biometric verification can be used very effectively. A biometric signature is a behavioral biometric recognition that can be done by one's actual handwriting signature on – say – a tablet computer or on a cell phone using a digital pen (a stylus). Since a very conventional way of handwriting does it, it is of no surprise to find the fast acceptance of biometric signatures by banks, hospitals, companies, and various government departments all throughout the world, hence the ISO's standard 19794/7, "Biometric data interchange formats-Part 7: Signature/sign time series data" on biometric signatures [7].

The popularity of biometric signatures is continuously increasing. Recently, Páez et al. proposed an architecture for a biometric electronic document identification implemented on blockchain for enhanced security measures [8]. While Delgado-Mohatar discusses blockchain technologies for storing data in biometric templates [9], Tolosana et al. discuss the biometric signature application on smartphones not with a stylus but with an actual finger touch [10]. Moreover, Bibi et al. delineate the offline and online biometric signature verification systems by taxonomical classification models [11].

The biometric signature consists of three steps that are capturing the image, extracting the signature specific features, and comparing the signature with that of the master signature recorded earlier, respectively. After capturing the handwritten signature on a tablet or a mobile phone, 20 different features on each point of the signature (usually a signature consists of 300–350 points depending on how large the signature is) are extracted for signature recognition. Here are the typical features extracted: the normalized x coordinate, the normalized y coordinate, the pressure of the pen, the altitude angle, the azimuth angle, velocity in x coordinate, velocity in y coordinate, the absolute speed, x coordinate acceleration, y coordinate acceleration, absolute acceleration, tangential acceleration, press derivation, sine of the $\alpha$, cos of the $\alpha$, the $\alpha$-angle between the absolute $\alpha(t)$ velocity vector and the x axis, derivation of $\alpha$ angle, sine of the $\alpha'(t)$, cos of the $\alpha'(t)$, and the angle between two adjacent line segments at each coordinate [12–14]. Figure 11.1 depicts a captured signature image with point number 0, and Table 11.2 shows the extracted 20 features from point number 0.

Once the extraction of these 20 different features from every 300–350 points of the handwritten biometric signature is done, then this data set ($20 \times 350 = 7000$


**Fig. 11.1** A captured signature. Arrow shows point 0

**Table 11.2** Extracted 20 features from point number 0

| Feature name | Description | Feature value |
|---|---|---|
| x(t) | The normalized x coordinate | −2.0417045316174507 |
| y(t) | The normalized y coordinate | 0.8904726440681375 |
| p(t) | The pressure | −0.12352253310985135 |
| altitude(t) | The altitude angle | −0.7705902233032206 |
| azimuth(t) | The azimuth angle | 0.19341427835884628 |
| $v_x(t)$ | Velocity in x coordinate | 0.2578478834273576 |
| $v_y(t)$ | Velocity in y coordinate | −0.2321773958415317 |
| v | The absolute speed | 2.047146860798148 |
| $a_x(t)$ | x coordinate acceleration | 0.1153587798695471 |
| $a_y(t)$ | y coordinate acceleration | −0.21780126610015516 |
| a(t) | The absolute acceleration | −0.64522618184873 |
| $a_t(t)$ | Tangential acceleration | −0.05318895898172835 |
| $p'(t)$ | Press derivation | 0.993728388123432 |
| α(t) | The angle between the absolute Velocity vector and the x axis | −0.3296822027324172 |
| sinα(t) | Sine of the α | −0.3296843007139452 |
| cosα(t) | Cosine of the α | 0.15743419748851212 |
| $\alpha'(t)$ | Derivation of α angle | 0.0026385951811272353 |
| $\sin\alpha'(t)$ | Sine of the $\alpha'(t)$ | 0.0026385951811272353 |
| $\cos\alpha'(t)$ | Cosine of the $\alpha'(t)$ | 0.0026385951811272353 |
| β(t) | The angle between two adjacent line segments at each coordinate | 0.002739030665447192 |

specific data item in total) is dynamically compared with the original master handwritten signature data of the user which was obtained earlier. The dynamic comparing process creates a threshold value. Once and if the comparison threshold value is in the acceptance interval, then the biometric signature can be accepted, hence no forgery. Figure 11.2 shows a comparison of a genuine signature against a fraud by selected features.

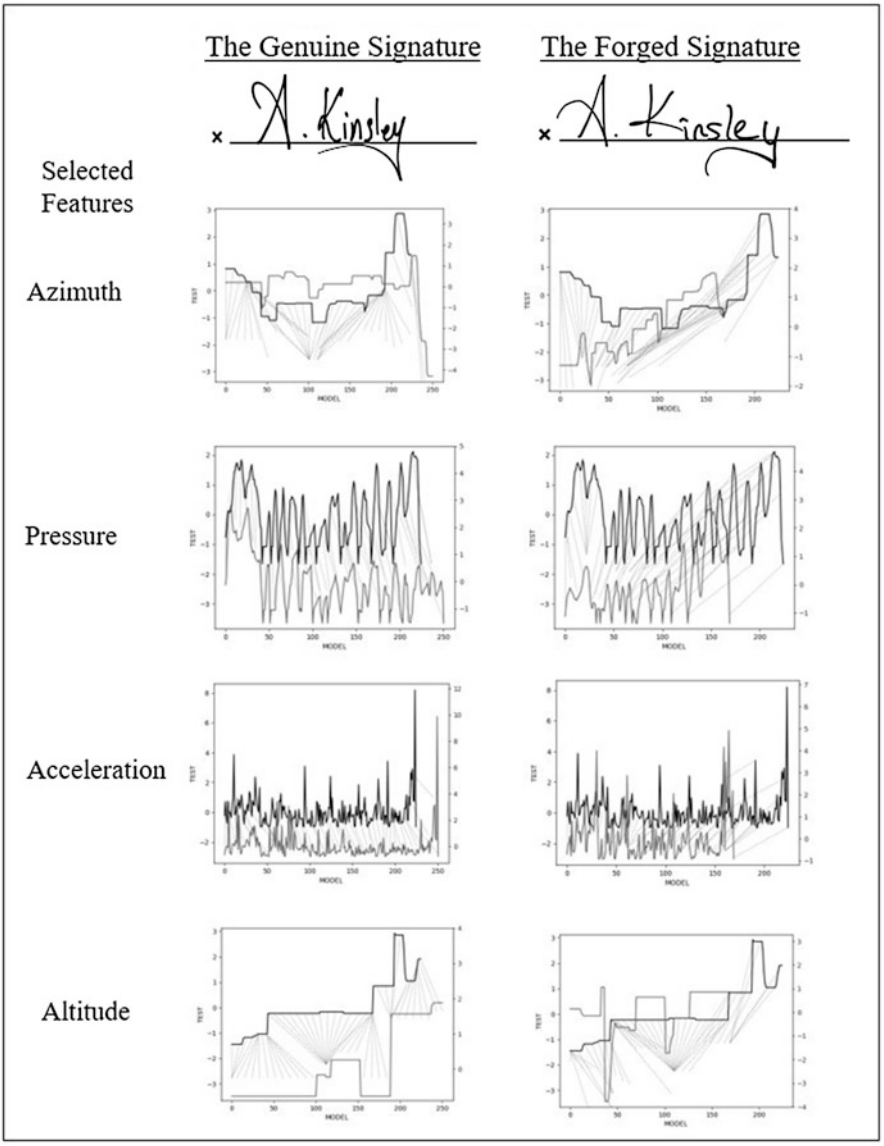


**Fig. 11.2** The comparison of genuine and forged signatures by selected features only

## 11.4 The Biometric Signature on a Blockchain

Hardware dependency has always been a significant issue for conventional digital signing. Even though server signing was kind of an answer to that unsettled question, it has not without its networking issues. On the other hand, computational

intractability, which provides the security and reliability for all these asymmetrical cryptosystem protocols, is due to our current computational model.

The advancements in the science of physics and engineering make it possible that quantum computing will be in use in a decade or so. If this will be the case, the conventional asymmetrical cryptosystems will be useless. Thus, digital signing methodologies as we know them today will be pushed aside.

While handwritten signing on a touch-sensitive screen like that of a tablet and/or a mobile phone is natural, hence the frequent and rapid acceptance by the industry, the data which is composed of the signee's signature image should still be kept under tight security. Therefore, all the information reflected as the extracted features from the points of the image must be stored along with the image of the signature itself.

The idea of utilizing the conventional cryptographic protocols to provide security for biometric data is by no means the only alternative due to the issues mentioned above.

What we propose is to have all that biometric information added to a blockchain. With a new hashing algorithm that will be developed as a quantum computing resistant, the blockchain will be one of the safest solutions to come.

As detailed in Sect. 11.3, the biometric info in the form of extracted features from all the points of the signature image provides the base for comparison. However, there must be at least five authentic signature images obtained from the signee to develop the genuine signature base with all extracted features to be kept in a blockchain. Table 11.3 shows the basic model for a blockchain.

**Table 11.3** A blockchain entry for a biometric signature genuine base

| Data Structure in a Blockchain |
|---|
| **{**<br>**"data": {**<br>**"client": "2020",**<br>**"threshold": 2.316184737819842,**<br>**"signatures": {**<br>**"s1": {350 items…}**<br>**"s2": {350 items…}**<br>**"s3": {350 items…}**<br>**"s4": {350 items…}**<br>**"s5": {350 items…}**<br>**},**<br>**}**<br>**"prev_hash":**<br>**"d498df3a5b9e4935cf965da99b2e2dbb64e876453479a05fb1c0801df3126a7**<br>**5",**<br>**"timestamp": 1594906588.52126,**<br>**"proof": 32,**<br>**"index": "16"**<br>} |

**Table 11.4** A blockchain entry for the extracted features of the first point of the first signature

| Data Structure of First Points of First Signature |
|---|
| **"signatures": {** |
| **"s1": {** |
| **"0": {** |
| **"x": -1.988754379338032,** |
| **"y": 0.4511260131208926,** |
| **"p": -0.7661117399152955,** |
| **"ax": -0.08439360522909167,** |
| **"ay": 0.6915132498531755,** |
| **"vx": 0.06674528445182873,** |
| **"vy": 0.1399171613281847,** |
| **"altitude": -1.4444335626533926,** |
| **"azimuth": 0.8187890660248799,** |
| **"v": 1.9903431712158168,** |
| **"a": -0.2087518489067404,** |
| **"att": 0.026736406092351797,** |
| **"dvp": 0.4651733290018387,** |
| **"alfa": -0.2052921036689894,** |
| **"sina": -0.20529230586040206,** |
| **"cosa": 0.3752404477999517,** |
| **"deva": 0.11523422497388082,** |
| **"devsina": 0.11523422497388082,** |
| **"devcosa": 0.11523422497388082,** |
| **"beta": -0.00020099889827516584** |
| **},** |

Each block includes extracted features from all points of five genuine signatures along with client, threshold, previous hash, and timestamp info. Table 11.4 indicates the extracted features of the first point of the first signature.

All the details of a transaction must also be added to the block. Table 11.5 depicts the transaction details as kept in blockchain. Note that the latitude and longitude info along with the time info also stored in blockchain for the increased reliability of the whole transaction.

## 11.5 Conclusion: The Biometrix Project

The idea of storing the biometric information on blockchain was realized in a project called Biometrix. The issues in signing and the related biometric solutions along with a blockchain implementation outlined above were addressed in the Biometrix project. The detailed information concerning the application of Biometrix can be accessed in GitHub [15].

**Table 11.5** Transaction information on blockchain

Transaction Information Data Structure


```
{
   "transaction-id": "B90CFE6E-CCD6-46A1-84BE-1CE5B861F1DE",
   "client-id": "2020",
   "end-user-id": "taylanakbas@bx.com",
   "document-id": "2C700091-D9C6-4266-ABA3-D60A07FF03B0",
   "timestamp": "16-07-2020 16:37:50",
   "signature": {
      "0": {
         "x": -2.0417045316174507,
         "y": 0.8904726440681375,
         …
         …
         …
      }
      "1": {
         "x": -2.0221943900950627,
         "y": 0.8639206844542605,
         …
         …
         …
      }
      …
      …
      …
   },
   "score": "2.301189502775008",
   "threshold": "2.316184737819842",
   "difference": "-0.015",
   "transaction-result": "Genuine",
   "latitude": 38.44594114808755,
   "longitude": 27.202107367501608
}
```


## References


1. R.C. Merkle, Secure communications over insecure channels. Commun. ACM **21**(4), 294–299 (1978)
2. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
3. IEEE Homepage., https://standards.ieee.org/standard/1363-2000.html. last accessed 16 July 2020
4. Secure Hash Standard (SHA), *Federal Information Processing Standards (FIPS) Publication 180–4* (2015). https://doi.org/10.6028/NIST.FIPS.180-4. August 2015

5. eIDAS: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
6. EN 419241-1:2018: *Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements*. 15-Jul-2018
7. ISO/IEC 19794/7, *Biometric Data Interchange Formats-Part 7: Signature/Sign Time Series Data* (2007)
8. R. Páez, M. Pérez, G. Ramírez, J. Montes, L. Bouvarel, An architecture for biometric electronic identification document system based on blockchain. Future Internet **12**, 10 (2020)
9. O. Delgado-Mohatar, J. Fierrez, R. Tolosana, R. Vera-Rodriguez, *Blockchain Meets Biometrics: Concepts, Application to Template Protection, and Trends* (2020). https://arXiv.org/2003.09262 [cs.CV]
10. R. Tolosana, R. Vera-Rodriguez, R. Guest, J. Fierrez, J. Ortega-Garcia, Exploiting complexity in pen- and touch-based signature biometrics. Int. J. Doc. Anal. Recognit. (IJDAR) **23**, 129–141 (2020). https://doi.org/10.1007/s10032-020-00351-3
11. K. Bibi, S. Naz, A. Rehman, Biometric signature authentication using machine learning techniques: Current trends, challenges, and opportunities. Multimed. Tools Appl. **79**, 289–340 (2020). https://doi.org/10.1007/s11042-019-08022-0
12. O. Hurtada-Miguel, *Online Signature Verification Algorithms and Development of Signature International Standards*. Ph.D. Thesis, Universidad Carlos III de Madrid, September (2011)
13. T.Q. Ton, T. Pham Tung, Online signature verification using dynamic time wrapping and extended regression. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **4**(5), 1854 (2015 May)
14. T. Giorgino, Computing and visualizing dynamic time warping alignments in R: The dtw package. J. Stat. Softw. **31**(7), 1–24 (2009). https://doi.org/10.18637/jss.v031.i07
15. T. Akbaş, *Biometrix- BIOMETRIX – Artificial Intelligence Assisted Biometric Signature on Block Chain* (Engineering Graduation Project, Yasar University, Department of Computer Engineering, Izmir, 2020) https://github.com/taylanakbas/Biometrix