PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(3)2020

Managing Gender Change Information on Immutable Blockchain in Context of GDPR

[1]Ali Shahaab, [2]Ross Maude [1]Chaminda Hewage, [1]Imtiaz Khan
[1]Cardiff Metropolitan University, United Kingdom
[2]Companies House, United Kingdom

Correspondence: ashahaab@cardiffmet.ac.uk

Received: 30 September 2019 **Accepted**: 25 November 2019 **Published**: 6 January 2020

Abstract

The transgender community faces serious socio-economic predicaments due to the discrepancy that its members face between their current gender expression and the assigned gender identity at birth. Even though, a considerable amount of work has been done to protect their basic human rights such as security, equality and social acceptance; trans people are still large victims of hate-related crimes. With general data protection regulation (GDPR) and other data protection laws and policies in place, now it is ever more important to protect the confidentiality of gender change information as well as to establish technical solutions that can prevent from inferring any sense of gender change from historical data. In this context, distributed ledger technologies such as blockchain present great opportunities for information integrity, security, privacy and access. However, at the same time provenance information extracted from immutable blockchain can be exploited to infer gender change. Addressing this paradox here, we propose recommendations for managing gender change information in the blockchain environment in the context of the present socio-political, legislative and technical challenges associated with gender change.

Keywords: *blockchain, distributed ledger technology, personal information on blockchain, immutability, public sector, gender change, GDPR*

JEL Classifications: *D02, D71, H11, P16, P48, P5*

1. Introduction

1.1. Transgenders and social injustice

Sweileh [1] analyzed 5772 peer-reviewed documents published between the year 1900 and 2017 from 80 different countries in order to quantify and map keywords used in relation to transgender health. The term "HIV" obviously ranked the top keyword used, but interestingly the second and third top keywords were "mental health" and "discrimination". Figure 1a shows the network of these keywords and clearly indicates that transgender health is not only related to physical health but to other mental and social issues also. In fact several studies have argued that mental health issues faced by transgender people are due to discrimination, victimisation, cultural intolerance, social stigma and violence [2]–[4].

According to the definition of the Government Equalities Office (GEO; this is the official UK government's unit responsible for work on policy relating to women, transgender equality and sexual orientation). "Trans" is a general term for people whose gender is different from the gender assigned to them at birth. For example, a trans man is someone that transitioned from woman to man. [5] Accurate data for trans people living in the UK are not available, as it is not asked in the census and no statistically significant research has ever been conducted in this context. However, it is estimated that there are 200,000 to 500,000 trans people living in the UK [5]. Trans people are exposed to widespread social stigma, abuse, harassment and discrimination. Gender change has severe social, economical and political consequences for these subjects, and in some cases it can be life-threatening, even in free societies like US (Figure 1b) [6] and UK (Figure 1c) [7].

Beyond statistics, the following quotes from victims of identity-related hate crimes underpin the general attitude of the society towards trans people:

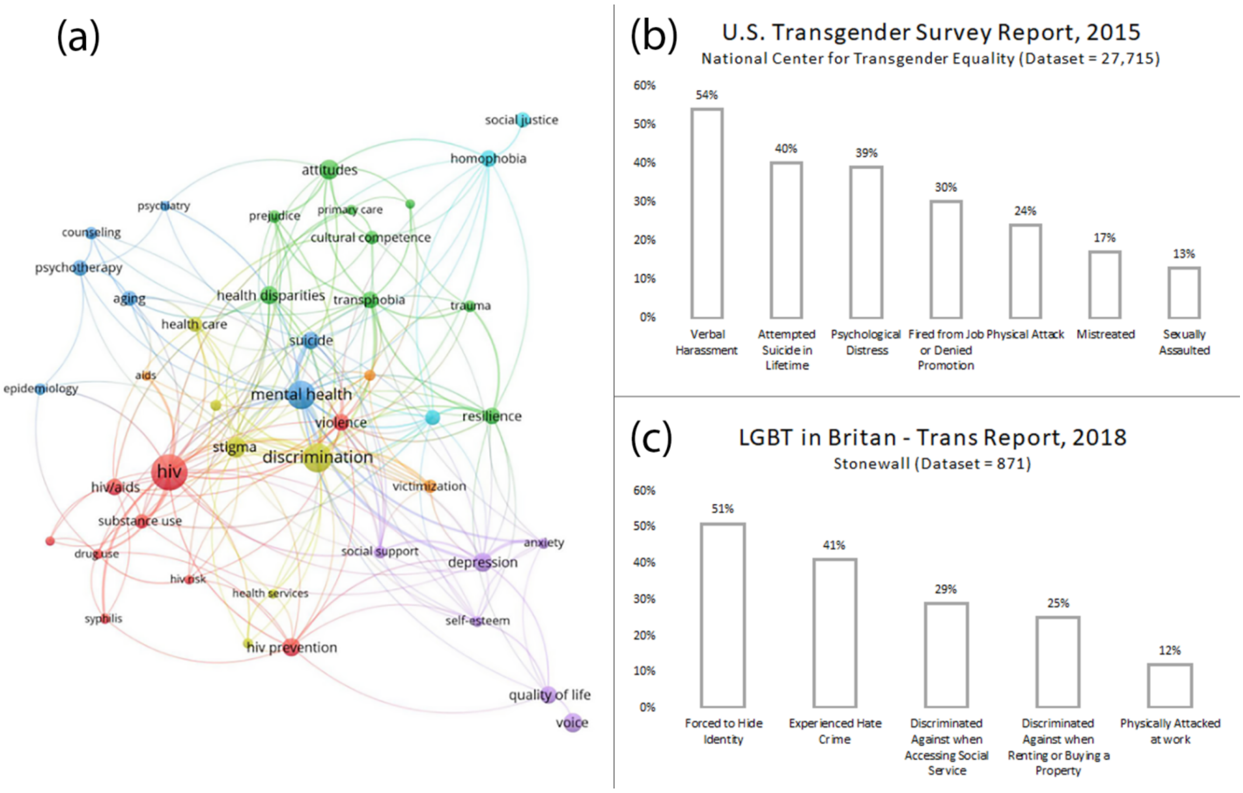

Figure 1: (a) Inter-relationship of different health-related keywords extracted and analyzed from 5772 peer reviewed articles by Sweileh [1] (The figure was reproduced under the creative commons licence). Different experiences that transgender people face in (b) USA and in (c) UK.

I am a trans man and I have been stalked for over two years now from an unknown person. During this time, I have received anonymous threatening letters. I've had two letters containing razor blades, one which contained a toxic substance which burnt my hands, face and eye. I have been beaten up three times. —James, 47 (South East England, UK) [7]

I was raped. Police kept referring to me as 'she' and 'female' and using my birth name. The doctor they brought to examine me made me uncomfortable and continued calling me female. —Angus, 24 (Scotland, UK) [7].

To understand the sheer scale of the problem, we would like the reader to take into account the fact that the physical, emotional, sexual and verbal abuse of trans people is so common that it has been given a name "trans bashing." Also, a dynamic list of unlawfully killed transgender people is being maintained on Wikipedia [8].

Considering the consequences and the severity of the matter, it is utterly important that the information about gender change is dealt with highest confidentiality and no unauthorised person is ever be able to infer about the gender change. Section 22 of the Gender Recognition Act (GRA) declares the revelation of gender change request without the explicit permission of a trans person as a criminal offence [9]. However, revealing anonymised data or in accordance with the GRA-defined criteria is acceptable.

1.2. Gender in the context of personal data

Gender is an attribute of "personal data." The Information Commission Office (ICO) [10] and the Organization for Economic Cooperation and Development (OECD) [11] defines personal data as "information that relates to an identified or identifiable individual." Personal data could be as simple as a subject's name or email address, or it could include other identifiers such as browser cookies, IP address or location data. In short, any information that could possibly result in the identification of a subject, directly or indirectly, is personal data. Introduced in May 2018, the general data protection regulation (GDPR) [12] requires data controllers (entity that determines the reason and the need for the processing of personal information) and data processors (entity that processes personal data on behalf of the controller) to take strict measures in securing fair usage of personal data. Sexual orientation is considered as a special category of personal data under GDPR, and sensitive data under the Data Protection Act (DPA) 1998. Data controllers need explicit consent from the data owner for data processing. Encrypted data (pseudonymised) or hashes of deterministic datasets are also considered personal data under GDPR. For example, one can easily compare the hash (a deterministic message digest that can be used to store the cryptographic proof of the data instead of the raw data itself) of the subject's gender attribute to devise if the subject is a male or female and a subject's date of birth can be revealed by iterating over a very low subset of possible outcomes (gender will only take two and date of birth in dd/mm/yyyy format will take less than 50,000 attempts). Adding random noise to the data before hashing results in a non-deterministic hash, hence deeming the data as not personal anymore.

Chen and Zhao have discussed seven phases of personal data – generation, transfer, usage, sharing, storage, archival and destruction [13]. There are several security and privacy challenges associated with each step of the lifecycle. The subject has the right to know what information is collected on them, how it is stored and managed, how the integrity of the data is guaranteed, storage and usage of data and finally how it is destroyed once it is no longer used [13]. Data controllers and processors are required to take all the necessary steps in protecting personal data in all steps of the data lifecycle.

1.3. Potentiality of the blockchain technology

Computer scientists and information security experts continuously propose different methodologies and frameworks for secure sharing and protection of personal data collected on the subjects. Distributed ledger technologies (DLTs), such as blockchain, have also attracted a wide spectrum of researchers for secure dissemination of valuable information and as a tamper-proof medium for the storage of personal information. Blockchain basically is a global distributed digital ledger or database system where the updated copy of the ledger is available to all participants (also known as nodes) at all time. Blockchain is also a "trustless" system where instead of a trusted third party (e.g. banks and government organizations), trust on each transaction is asserted by general consensus within the participants in a democratic, competitive and incentivized manner. Once validated, each transaction is recorded on the ledger in an immutable fashion, and the updated copy of the ledger is available to all participants on a real time basis. In addition to the nodes maintaining the blockchain network, the state and history of the ledger can be accessed by anyone (public DLTs) or restricted to only a few (private DLTs) through blockchain explorers.

Cryptographic capability of the blockchain ensures security and privacy, and with smart contract technology, a data usage control mechanism – commonly known as "disclosure without exposure" can be established within the blockchain network [14], where data owners can define the level, duration and authorities using their data. It is the latter capability that provides blockchain unique advantage over traditional database management systems by empowering data owners to determine which aspect of their personal information can be exposed to whom and for how long – a debatable issue of GDPR commonly known as the "right to be forgotten" (RTBF) [15]. Despite this empowerment, the immutable block of information and the ability to extract provenance information from the chain can be a liability for trans people, because anyone with the right access on the blockchain can trace and detect any gender change by comparing the current gender attribute value with the past value.

Addressing the technical complexity of blockchain in relation to the reality of GDPR and the contemporary social stigma and insecurity of trans people, here we aim to investigate the suitability of blockchain for storing and sharing the personal data of trans people. This article is set as follows: Section 2 discusses related work in the space of handling personal data on the blockchain and we discuss our recommendations in Section 3 about how gender change should be managed as part of personal data on the blockchain. We end the article with our conclusion and prospective future work in section 4.

2. Related work

We found several articles discussing the techniques around sharing, storing and managing personal data on the blockchain but we have not come across any piece of literature discussing the challenges associated with the change in gender. Here we present some of the common techniques of handling personal data on the blockchain.

a. Blockchain and medical data

Medrec [16], a blockchain-based system to handle electronic medical records (EMRs), aims to provide users with an immutable log and access to their EMRs. Personal data are stored on patients' smartphones and service providers' databases. Access to the data is managed through permissioned setup of the Ethereum [17] blockchain. No personal data are put on the blockchain, but a 'DNS-like' link is created between the already established identity and the Ethereum address. Cryptographic hash of the data is stored on the blockchain to ensure data integrity while data are kept off-chain. Smart contracts are used to manage access permissions to the externally stored patient data. [16] A service provider such as GP can update patient records and notify observers about the update, and a patient can at any time revoke permissions to their data. The query string for data retrieval is affixed to the hash of data subsets for tamper evidence. Even though, no personal information is put on the blockchain, this fixed query string can indicate a gender change in the gender data set.

b. Blockchain and personal data

CareerChain [18], a platform to host jobseekers profile, also uses a private instance of the Ethereum blockchain. The subject's data are encrypted using private keys and stored on an interplanetary file system (IPFS) [19], and the address to the latest profile is stored in a smart contract, where access is controlled by the subject. [18] assumes that RTBF is preserved as the subject can delete their private key, making the data unreadable and hash meaningless. However, the subject cannot exercise their RTBF if they lose their private key, compromising their personal details forever.

Engima [20] protocol stores the data off-chain and pointers to the data are stored in distributed hash tables (DHTs), which are distributed across several nodes. Access control is governed by the blockchain, and computations on the data are performed using multi-party computation (MPC), without revealing the complete data to any of the nodes. Even though Engima guarantees private computation on the blockchain, it does not secure the raw data, making it possible for someone to change the data. This change can be easily identified as the data pointers will change with the data modification.

Hossein et al. has proposed a blockchain-based solution for Internet of Things (IoT) devices**.** Their approach is similar to [16] such that the data layer is separated from the access layer, having access control on a blockchain and data resides in an off-chain centralised storage such as a cloud or decentralised storage such as DHTs or IPFS [21]. Chang et al. also suggest storing personal data in off-chain storages and storing a hash on the blockchain for authenticity and verification purposes [22]. Nazaré et al. uses a similar approach for certificate verification. The hash of the certificate containing the subject's personal details is placed on the blockchain and requires the verifier to have access to the original document and knowledge of the location of the hash on the blockchain [23]. This approach requires a new hash to be posted onto the blockchain if any personal details are changed for the user. Observers may notice the change and may also be able to decipher the change if they have previously had the original document for verification purposes.

c. Blockchain for data integrity

Ancile [24] also puts the hash of the data and the pointers on the blockchain while storing the data in traditional databases. Its purpose is to guarantee data integrity, as underlying data can be changed or removed. However, the issue of an identity update is not addressed as the network will be able to track the update to the existing record. Igor et al. propose the use of blockchain technology to ensure the integrity of files on the cloud. Hashes of the files are added on the blockchain as a reference of the change [25]. Though the authors do not deal directly with personal data, the files may contain personal data, indicating a change in personal data whenever a new hash is posted. Zyskind et al. propose the use of shared identity for data access and storage. Encrypted data are stored off the blockchain, and pointers (hash of data) to the data are stored on the blockchain [26]. Users remain anonymous while the service's profile can be verified on the blockchain.

d. Blockchain as identity service

Identity as a service-based blockchain focuses greatly on privacy. The goal of these blockchains is to allow the subject to prove their identity and relation to any verifier. Shocard [27] keeps the encrypted personal data on the user's device and posts the full record of signed hashes and a code (to prevent discovery) on to the blockchain. Verification involves the user presenting the raw data and the code for the verifier to be able to verify the data on the blockchain. The subject's identity is confirmed by other authorities when they verify its claim of identity. If any part of the identity changes, the subject has to get new certification for that part of the identity. For example, if the subject changes their address, new certification on the new address will be required but their other claims about age, gender, etc. will stay valid. Figure 2 shows the change of gender and attestation recorded with new timestamps on the blockchain.

Even though the solution is practical, it still poses a threat to the trans person as the certification's timestamps become a proof that the subject has changed gender at a later point. Figure 3 shows a subject sharing their identity credentials with different attestation dates, revealing a later change in gender.

Sovrin [28] allows interactions using distributed identifiers (DIDs), which are unique for each relation. The subject's data are kept in private ledgers, and claims about the identity can be kept private or public. The use of zero knowledge proofs (ZKPs) enables the subject to disclose the proofs for verification.

The challenge with the identity on blockchain schemes is that the subject needs to reveal (a) more than one verification to establish trust, (b) the timestamp of the verification so the verifier can see that the subject is sharing the valid claims, (c) claims regarding more than one attribute. Hence, for example, if a trans person is to reveal their date of birth and gender to a verifier, they will be able to spot the gender change because there will be more attestations on the date of birth than on a recent gender change.

3. Our recommendations

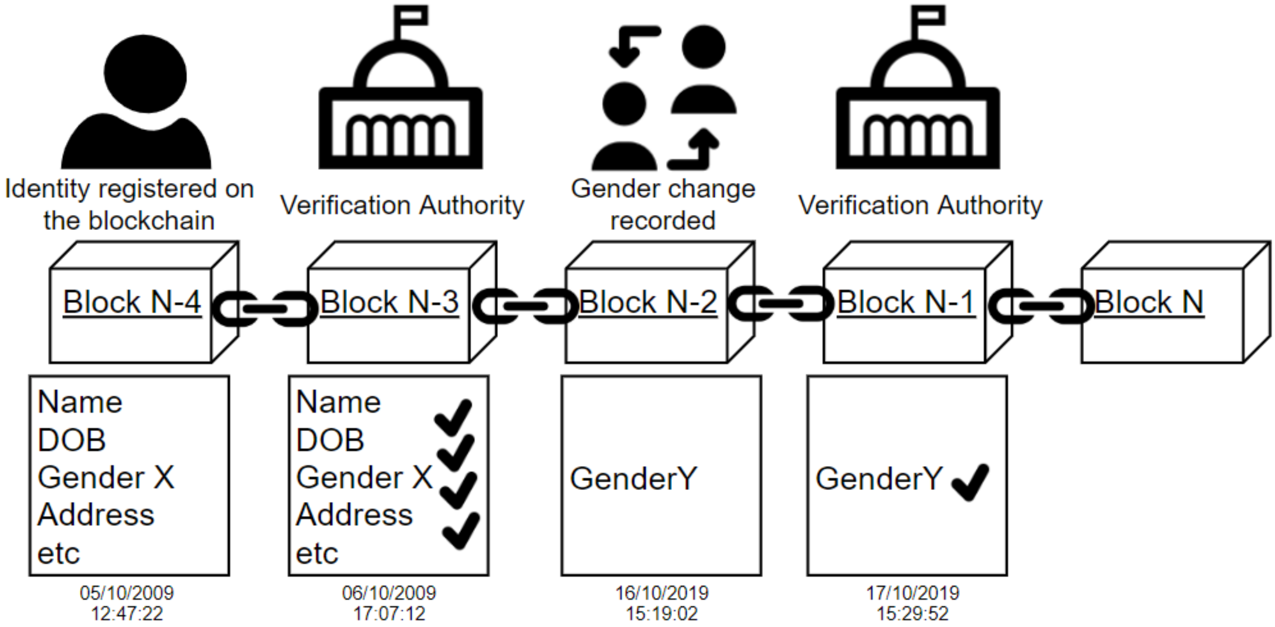

Figure 2: Establishing identity on the blockchain. Subject's identity attributes are verified by a verification authority and a verification claim to the blockchain. Any changes in the identity attributes yields the old claim to be invalid and new verification is required in order to establish trust. Each claim has a timestamp and possibly a validity period.

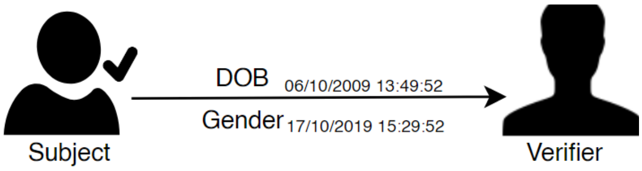

Figure 3: Subject revealing verification claims about their identity to a verifier. The timestamp of the claim can reveal a gender change to the verifier as it is obvious that gender change has a later verification from DOB. DOB may also have several more claims then gender.

Gender change is a delicate subject with severe consequences for the subject and also for the authority dealing with the information around gender change. The solution to obfuscating the change of personal data change, such as gender, on the blockchain must meet the following criteria:

a) On-chain activity should not de-anonymise the subject.
b) Change in gender should not be visible to unauthorised observers.
c) Any historical transactions should not reveal the previous gender but only show the recently acquired gender.
d) Gender change should not be revealed when accessing multiple personal identity attributes.
e) Any such solution should be future proof in both technological and legal perspectives.

We recommend the following approach to satisfy the aforementioned criteria.

a. On-chain activity should not de-anonymise the subject

"Identity" on the blockchain is only a random string (public key). However, identity can be exposed by the reuse of public keys. Bos et al. were able to identify several bitcoin account owners by analysing the repetition of public keys [29]. Supplementary data may also aid in ring fencing the subjects, for example, IP address or spending patterns. Anonymisation can be achieved by avoiding the reuse of public keys. It becomes difficult to deanonymise a subject if they are using a unique public key for every transaction across the network. For example, using the same public key if the subject's previous transactions revealed the subject's gender as male, then an observer may be able to infer the gender change if the new transactions reveal the subject as female. ZKPs [30] and homomorphic encryption [31] techniques should be deployed to obfuscate the details of transactions, such that the subject cannot be linked to the transaction.

b. Change in gender should not be visible to unauthorised observers

It is important that not only the personal information is secure but the change in personal information, such as gender, should also be kept private. As blockchain links the new transactions with the previous ones, it makes it difficult to "hide" the change from the observers. We suggest including an encrypted transaction belt in the transaction schema, which can only be decrypted with the symmetric keys shared with the authorities. All participants in the network will see the encrypted transaction belt with every transaction but will not be able to see what has changed, hence removing the "sense of change." Off-chain storage should be used for storing personal information and the hash pointer on the blockchain will only point to the latest transaction on the blockchain. Authorities will be able to decrypt the belt and see the change, such as the information about gender change. Key delegation [32] and rotation should be used to renew the symmetric keys. Role-based encryption and proxy re-encryption techniques can also be used to manage access to the encrypted transaction belt. We also recommend managing the detection of the change using a similar approach to [27]. Grouping of identity attributes for certain access levels can significantly obfuscate the detection of the change. Personal data can be graded into different levels and access can be managed based on the observer's clearance level. Smart contracts can be used to manage notifications for different observers. A member of the public may only be notified of a change, and credit referencing agencies can be on-boarded for notification of more detailed changes such as change of address, marital status or name. Law enforcement can be notified on the exact change that has taken place (Figure 4). As the access is managed by a smart contract on the blockchain, individuals can verify who can access what part of their identity, encouraging fair usage of the system.

c. Any historical transactions should not reveal the previous gender but only show the recently acquired gender

We conclude from section 2 that any personal details (gender included) should never be put on the blockchain but only a cryptographic proof should be put on the blockchain. As discussed in section 3b, the off-chain record of personal data will point to the most recent identity transaction. We therefore recommend that where possible, static personal data should not be stored as a part of the transaction but "looked-up" at the point of retrieval so that only the up-to-date information is retrieved. This approach will also aid the blockchain network to comply with the accuracy principle of GDPR [33].

d. Gender change should not be revealed when accessing multiple identity attributes

To satisfy this, we recommend that standards should be developed that allows sharing the claims about identity in such a way that it obfuscates any less common and severe change such as gender. Multiple attributes should be shared together in such a way that they do not compromise personal identification and privacy. Only recent timestamps should be accessible to the verifier so they cannot "sense" the change. For example, people move addresses quite frequently, so a subject sharing their claims for the last three residential durations with verification timestamps should be acceptable; however, a subject sharing their date of birth and gender claims with timestamps pose the risk of revealing the identity of the trans person. We conclude that timestamped information should not be shared for the somewhat

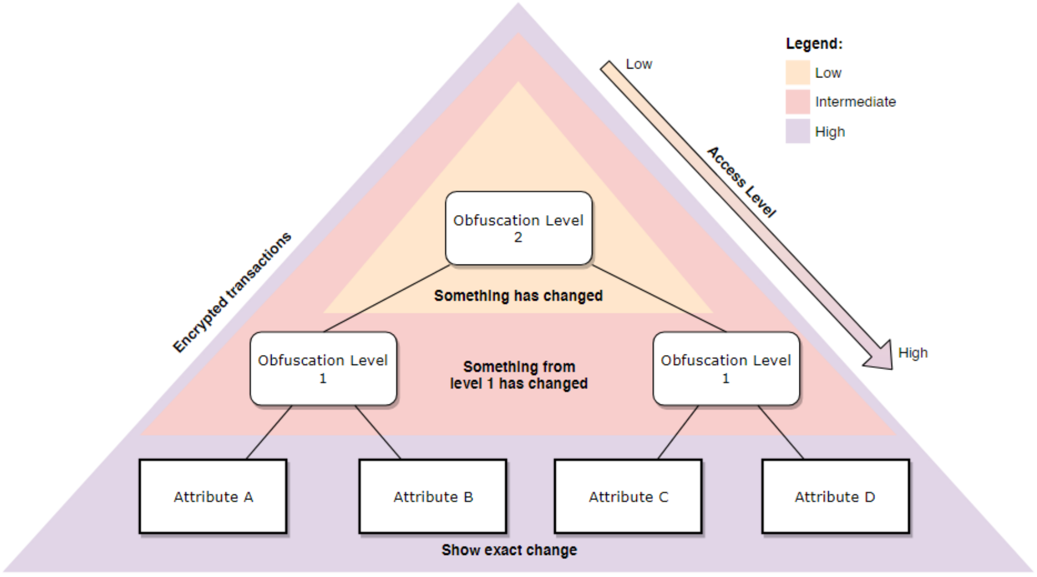

Figure 4: Different level of observers get a different level of view of the encrypted transaction. A Physician may get highest access and can see the change in gender, credit reference agency get intermediate access and can see a category change while any sort of details will be hidden from the public with visibility to undelaying data.

static personal information, but it can be shared for dynamic personal information.

e. Any such solution should be future proof in both technological and legal perspectives

These recommendations require foresight of the constantly changing socio-political landscape and evaluation of the continuous advancements in the technical space. The transparency versus privacy pendulum swings from one side to another with social awareness, technological change, media and recent events. Technical solutions must be flexible to adhere to the ever-changing socio-political landscape. Increased technical developments also lure threats to the cryptographic techniques used in the blockchain space. Bitcoin, Ethereum and several other blockchains rely on public key cryptography for transaction signing and funds locking. Advancements in quantum computing pose a serious threat to public key cryptography, and it is anticipated that commercially available quantum computers soon will be powerful enough to derive the private keys used to encrypt the personal information, making the subject vulnerable. Therefore any DLT/blockchain solution for personal information must ensure a safe migration towards the post-quantum era, and we should already be considering building systems using quantum-resistant cryptographic techniques [34].

4. Conclusion

DLTs such as blockchain are critical for establishing digital identity and protecting personal data online. No subset of personal data should be treated as "static," and personal data should never be uploaded to the immutable ledger. The revelation of an identity attribute such as gender change can have life-threatening consequences for trans people. This information must be protected and treated with confidentiality and must never leave any trail on the permanent blockchain. Gender change related information must be kept off-chain and declared in such a way that no unauthorised observer can detect the change in gender. New technological developments like homomorphic encryption, secure multi-party computation (SMPC), ZKPs and verifiable claims can significantly improve the odds of blockchain being a suitable technology stack for managing personal data. With the tightening of data protection laws around the world and classification of metadata of personal data such as encrypted data being classified as personal data, it may not be far that even the hash of the personal data is classified as personal data. Hence, we argue that gender-related information should never go on a blockchain. Only the commitment and a claim about the data should be put on the immutable ledger such as blockchain, and homomorphic encryption will also help in protecting and managing personal data.

Competing Interests:
None.

Ethical approval:
Not applicable.

Author's contribution:
AS, RM, CH and IK designed and coordinated this research and prepared the manuscript in its entirety.

Funding:
This research has been supported by Knowledge Economy Skills Scholarships (Scholarship # CMK219) a major pan-Wales operation supported by the European Social Funds through the Welsh Government. The scholarship was also partly funded by Companies House, UK.

Acknowledgements:
The authors acknowledge Mr Ben Lidgey for his continuous input on the subject and Mr Farhan Khan for his valuable feedback on the approach.

References:

[1] W. M. Sweileh, "Bibliometric analysis of peer-reviewed literature in transgender health (1900–2017)," *BMC Int. Health Hum. Rights*, vol. 18, no. 1, p. 16, 2018.

[2] K. D. Jaffee, D. A. Shires, and D. Stroumsa, "Discrimination and delayed health care among transgender women and men," *Med. Care*, vol. 54, no. 11, pp. 1010–1016, 2016.

[3] T. C. Carmel and L. Erickson-Schroth, "Mental health and the transgender population," *Psychiatr. Ann.*, vol. 46, no. 6, pp. 346–349, 2016.

[4] S. Page, J. Burgess, I. Davies-Abbott, D. Roberts, and J. Molderson, "Transgender, mental health, and older people: an appreciative approach towards working together," *Issues Ment. Health Nurs.*, vol. 37, no. 12, pp. 903–911, 2016.

[5] Government Equalities Office, "Trans People in the UK," 2018.

[6] S. E. James, J. L. Herman, Susan Rankin, M. Keisling, L. Mottet, and M. Anaf, "The Report of the US Transgender Survey," 2015.

[7] B. Chaka and G. Becca, "LGBT in Britain - Trans Report," 2017.

[8] Wikipedia. "List of unlawfully killed transgender people." [Online]. Available: https://en.wikipedia.org/wiki/List_of_unlawfully_killed_transgender_people. [Accessed 21. Apr 2019].

[9] *The Gender Recognition Act - Section 22*. United Kingdom: Statute Law Database, 2004.

[10] ICO, "What is personal data?," 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. [Accessed 12 Apr. 2019].

[11] "The OECD Privacy Framework 2013," 2013.

[12] The European Parliament and the Council of the European Union, *Regulation (EU) 2016/679 (GDPR).*

2016, pp. 1–88.

[13] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012.

[14] R. H. Campbell Rab, Thompson Gillian, Ferry Peter, "Distributed Ledger Technologies in Public Services," no. June, 2018.

[15] Information Commissioner's Office, "Right to erasure," 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/. [Accessed: 12-May-2019].

[16] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016.

[17] V. Buterin, "A next-generation smart contract and decentralized application platform," *Etherum*, no. January, pp. 1–36, 2014.

[18] R. Gibson, A. Evans, L. Tatarov, D. Mulder, and A. Dowdalls, "Careerchain Foundation Whitepaper," 感染症誌, vol. 91, pp. 399–404, 2017.

[19] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv Prepr.* arXiv1407.3561, 2014.

[20] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," pp. 1–14, 2015.

[21] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards Blockchain-based Auditable Storage and Sharing of IoT Data," pp. 25–30, 2017.

[22] H. Chang, G. Tortora, C. Esposito, K.-K. R. Choo, and A. De Santis, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, 2018.

[23] J. Nazaré, K. Hamilton, and P. Schmidt, "What we learned from designing an academic certificates system on the blockchain." [Online]. Available: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196. [Accessed 21 Feb. 2019].

[24] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, 2018.

[25] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, 2019, vol. 6, pp. 6855–6864.

[26] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. 2015 IEEE Secur. Priv. Work. SPW 2015*, pp. 180–184.

[27] ShoCard Inc., "ShoCard Shitepaper: Identity Management Verified Using the Blockchain," p. 20, 2017.

[28] W. Paper and S. Foundation, "Sovrin ™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust A White Paper from the Sovrin Foundation," no. January, 2018.

[29] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *International Conference on Financial Cryptography and Data Security*, 2014, pp. 157–175.

[30] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash Protocol Specification," pp. 1–53, 2017.

[31] C. Gentry and others, "Fully homomorphic encryption using ideal lattices.," in *Stoc*, 2009, vol. 9, no. 2009, pp. 169–178.

[32] M. Abdalla, E. Kiltz, and G. Neven, "Generalized key delegation for hierarchical identity-based encryption," in *Proc. European Symposium on Research in Computer Security*, 2007, pp. 139–154.

[33] "GDPR Principle (d): Accuracy," 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/. [Accessed: 24-Apr-2019].

[34] L. Chen *et al.*, "Report on Post-Quantum Cryptography," 2016.