Identity Management in the Age of Blockchain 3.0

Arthi Kanchana Manohar
Northumbria University
Newcastle Upon Tyne, UK
Arthi.manohar@northumbria.ac.uk

Jo Briggs
Northumbria University
Newcastle Upon Tyne, UK
jo.briggs@northumbria.ac.uk

Presented at the CHI 2018 Workshop on HCI for Blockchain: Studying, Critiquing, Designing and Envisioning Distributed Ledger Technologies.

Abstract

Since the invention of internet, Identity has become a significant aspect for nearly every interaction that occurs online. In this position paper, we demonstrate and discuss current limitations of centralised IdM systems by drawing from the cases of two of world's largest biometric ID systems: India's *Unique Identification System Aadhar* and China's Social Credit system *Sesame Credit*. This paper explores self-sovereign identity through innovative application from blockchain 3.0. We then identify some key characteristics of blockchain technologies to address the challenges centralised IdM services face and present opportunities for furthering HCI research around de-centralised IdM services to provoke workshop discussion.

Author Keywords

Identity Management, Blockchain, HCI, Trust, Distributed Ledger Technology.

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous; See http://acm.org/about/class/1998 for the full list of ACM classifiers. This section is required.

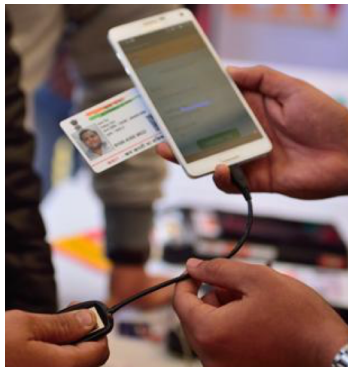

Figure 1: In this image, users' finger print is taken to verify their identity against their Aadhar biometric details. Aadhar details are also linked to their mobile number for re-verification. Image credit India TV News.

Introduction

IdM is a 'security discipline that enables the right individuals to access the right resources at the right times for the right reasons' [27]. Traditional IdM systems such as passports or driving licences are disconnected, expensive, cumbersome, time consuming to process, and trustless as the documents can be easily forged. These established ways of verifying one's identity are hindering digital innovation and limiting citizen experience. On the other hand, *online* IdM services, such as Facebook operate a federated identity system which can authenticate users' identity across services to determine whether or not they're allowed access. In comparison, *online* IdM systems are fast and cheap; yet they have also failed to evolve from the standard web forms that have been used to authenticate users' identity online over more than two decades! Further, it is relatively easy to fraudulently fill out an online form pretending to someone else. In the digital age, most online services do not provide Knowledge-Based Authentication that allows the user to prove his or her identity by providing shared security information to access the service.

Limitations and Failures: Centralised IdM Services:

In the recent years, we have seen the magnitude of personal identity leaks from organisations such as Equifax [17], Ebay [4], Yahoo [1] and Uber [4]. Such data leaks compromised millions of consumers' digital identities. Identity data leaks are particularly worrisome when they involve sensitive or financial data e.g. credit card details or, credit scores, date of birth etc. These centralised models of IdM services thus pose particular risks and threats – to both the company/organisation in the form of reputational and prospectively financial damage and increased mistrust in its service; and to citizen-consumers in compromising their sensitive data.

Unique Identification System (UIS) in India

In 2009, the Government of India introduced Aadhar ('foundation' in Hindi) as a voluntary identification system that provides all Indian residents with their own unique 12-digit number. As of 30th November 2017, Aadhaar is the world's largest biometric ID system with more than 1.19 billion enrolled members [24]. When residents register for Aadhar, their biometric details in the form of finger prints (see Figure 1), iris scan and personal photograph are obtained, along with demographical details such as date of birth and proof of address, which are verified through existing IdM e.g. passport and birth certificate [9].

Aadhar is an irreversible centralised identity system. It combines the details of a resident's passport, mobile number, bank account, PAN card (Permanente Account Number) and driving licence in an open-access database to which access can be acquired via a commercial service. At the time of writing (Jan 2018) Aadhar is said to soon become the all-purpose identification tool [24].

Since it was introduced in 2009, being enrolled with Aadhar has increasingly become necessary – or compulsory for all practical purposes. For example, without Aadhar a student cannot sit for a national exam; and any new mobile sim card requires Aadhar verification for its activation. Even the deceased required Aadhar to enable the release of a death certificate. And in the burgeoning space of Indian online dating – some websites including Lovevivah and TrulyMadly use Aadhar as mandatory, to verify users' is

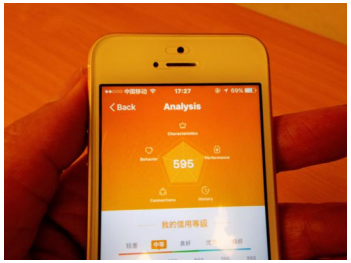

Figure 2: Alibaba's Sesame Credit interface showing how users are assigned numerical ratings based on various of financial factors (behaviour, characteristics, performance, history, connections). Image credit Nikkei Asian Review

now ubiquitous in India [23] and often impacts on the lives of Indians living abroad. This is all part of a higher level [5] which aims to make government services available electronically.

However, there are many disadvantages in such centralised identity database systems. First, users' identity information is insecure. Because of the poor data protection legislation and associated practice, personal data is often sold (outsourced) by companies and organisations for a small fee [14]. Second, the scale of such centralised identity databases could provide a tool for mass surveillance. Further, a significant drawback of incorporating biometric data is that this is non-salvageable – compromised once and it is compromised forever. Ahmad et al. [18] argues that biometric database links the information to the user, it cannot be reset or reproduced like unlike password when compromised. The 12 digit Aadhar identification number may link a user's bank details and mobile numbers—exposing a history of bank transactions, spending patterns, call history etc. Other information that can be relatively easily retrieved include a person's tax details or any recorded traffic violations or other legal transgressions— accessed with a query and payment of a small fee [22].

Social Credit System in China

The Social Credit System (SCS) Sesame Credit was piloted by the Chinese government from 2015 as an initiative for developing what amounts to a national reputation system. Eight technology companies have been granted permission to develop their own private credit scoring platforms one of which was launched by the Alibaba Group (www.alibabagroup.com). The SCS concerns 5 aspects of one's identity: users' online credit history, personal information, online social networks, behavioural habits and ability to pay off debts. The Chinese government aims to register all Chinese nationals by 2020 in a social ranking database. Using their app, the company ranks users by judging the type of products they buy online and their associated behaviour and the users are scored in a range between 300 and 850 (see Figure 2) by taking in account the above 5 aspects [13]. However, it is unclear if all 7 technology companies follow the same SCS process to provide the social credit scores for its users.

Sesame Credit connects users' financial, social, political, and legal credit ratings to synthesise into a personalised 'social trust score'. Individuals are ranked according to their social media interactions and online shopping history. Equally the score is informed on a wider variety of factors –whether they have received a ticket for a traffic offence or if they have unpaid taxes. In September 2016, the Chinese government legislated that users with high scores are now trusted to e.g. rent a car or a hotel room without paying a deposit; and even to move up the hospital waiting list for quicker treatment. Meanwhile those with lower scores are penalised as ineligible for public office or even social welfare payments; and no longer able to admit their child to a good school. The SCS appears to speak to the Chinese government's motivation around harvesting personal data on a large enough scale that it becomes a 'big data' resource for potential social control. As a means of mass surveillance it can privilege those who have earned higher 'scores' – thus promoting its particular values and channelling its limited resources to those who live by its rules. Some claim that the system replaces what in the west is verified by a simple credit card in what is still a cash based economy; and

"Someone who plays video games for 10 hours a day, for example, would be considered an idle person, and someone who frequently buys diapers would be considered as probably a parent, who on balance is more likely to have a sense of responsibility."

Li Yingyun, Sesame's technology director told Caixin, a Chinese magazine, in February 2015.

"If blockchain technology can be used to secure robust, self-sovereign digital identities around personal data, there's a real possibility that people in places with poor documents, registries and rules of law can establish trusted measures of their good reputation. This would allow them to assert who they are and access proof of their digital identity anywhere using a private key"

Dahan, 2016

that such a system is necessary for promoting trust between citizens. However, the Chinese companies tasked with running the SCS do not real their 'complex algorithms' that inform an individual's rating making it very difficult if impossible to repair a lower score.

As with Aadhar, Sesame Credit is being used in Chinese matchmaking, in a service called Baihe (Baihe.com) to promote its clients who have with good credit scores by giving them prominent spots on the company's website. And as with Aadhar, Sesame Credit was introduced to Chinese citizens as voluntary but has since become –in a practical sense – mandatory. In both these cases the services have effectively become compulsory by stealth without adequate investigation of the socio-technical and wider consequences.

Trust(less) services

Trust in centralised IdM services is uni-directional. Pasquale [21] refers to a 'one-way mirror' in his book 'The Black Box Society' where users are required to have trust in a serv ice, and to share their data. These services have no obligation or need to trust in their users; this is provided by evidence. Such centralised IdM systems can be thus be disruptive to users' welfare, and any lapse in the service's security poses multiple risks and threats.

Such centralised systems are of particular threat to 'vulnerable' groups, including women in a patriarchal Indian society. For instance, it is common for uneducated woman in India to lack valid personal documentation. Further for *any* woman her Aadhar must be first validated either by her husband or her father, while a child's Aadhar is linked to their father's as opposed to their mother's. China's SCS makes it very difficult for the users to restore their scores especially if they do not know how the algorithm works. Such centralised systems polarises those at the either end of the spectrum.

Blockchain and IdM

Crosby et al. [7] offer a simple definition of blockchain as a 1.0 is *currency*, deployed as cryptocurrencies such as Bitcoin, Ripple and Ethereum; blockchain 2.0 is *contracts* which represents financial applications as smart contracts and finally; blockchain 3.0 is the application of blockchain beyond the financial domain to e.g. civic systems, health, identity management, art and so on (refer Elsden et al. 2018 spreadsheet). The distributed trust model is a new way of managing identities and to establish trust among users, identity providers and relaying parties. While Nakamoto's blockchain (as blockchain 1.0) has been repurposed, across financial services, infrastructure, governance, identity management and much more, blockchain 2.0 technologies have the potential to empowers citizens and consumers to control their own identity and share between trusted entities with their full consent. According to Underwood [26] blockchain driven IdM services have the potential to change lives by providing 'unparalleled transparency' especially in developing countries to empowering people through 'recognised identity, asset ownership and financial inclusion'.

Dunphy and Petitcolas [11] have recently further classified blockchain based IdM into two main categories i. self-sovereign digital identities (e.g. Sovrin; Uport) and ii. Decentralised Trusted Identity

	Website	Description
Decentralised Trusted Identity		
ShO Card	https://shocard.com/	Sho Card provides IdM services through multifactor authentication through blockchain. Users can securely log into online services and devices without user ID and password.
ID2020	http://id2020.org/	Seeks to provide every child born after 2020 with a self-sovereign digital identity to reduce risks of human trafficking and to drive digital inclusion.
Trust Stamp	https://truststamp.net/	Trust Stamp uses social media and other publicly available data to verify identity and provide a unique trust score. Details of an individual's score are private and under their control; yet can easily be shared on another platform.
Bitnation	https://bitnation.co/	"The World's First Virtual Nation – A Blockchain Jurisdiction." A cryptographically secured public ledger distributed to all users that allows self-governance.
e-residency	https://e-resident.gov.ee/	A digital nation for global citizens, built by the Republic of Estonia. Government issued digital IDs available to access Estonian services such as company formation, banking, payment processing, and taxation.

	Website	Description
Self-Sovereign Digital Identities		
Sovrin	https://sovrin.org/	Self-Sovereign Identity (SSI) is an identity that is owned and controlled by an individual or organisation. No one else can read it, use it, turn it off, or take it away without its owner's explicit consent.
Blockstack	https://blockstack.org/	An open source blockchain application providing digital keys to enable users to own their identity. Users can sign in to apps locally without remote servers or identity providers.
Uport	https://www.uport.me/	The first identity system to enable self-sovereign identity, allowing the user to be in complete control of their identity and personal information.
Spidchain	www.spidchain.com	Spidchain uses blockchain to improve the digital identity management. The Blockchain allows the users high security level, with an easy and quick access, with significantly lower costs when compared with the current systems.

Table 1: Based on the survey available at Elsden et al [12].

(e.g. ShoCard). With regard to the former applications such as Sovrin, Uport and Spidchain offer self-sovereign identity through blockchain technology where the owner has control over what information they share without 'external administrative authority' [11]. Decentralised trusted Identity applications offer centralised service that provide identity proofing through existing identifications like passport and driving licence. The above-mentioned applications are few of applications offer 'privacy and trust', where interactions and transactions are secure by allowing authentication and verification only by 'consensus mechanism' within the 'permissioned network'.

Building on Dunphy and Petitcolas [11] we set out and extend entries available in the Elsden et al. 2018 database of blockchain applications as examples services offering IdM through secured with peer to peer interaction and storage of one's personal information which enables one to create a new digital identity – crucially allowing self-sovereign identity.

Is Blockchain a solution

Centralised online databases have proven time and again that people's personal information is exposed and extremely vulnerable. Could blockchain be the solution for the centralised IdM failures? Blockchain-based applications propose that users' personal information is safe, that the technology with proper application offers flexibility and better control over what information they share (e.g. revealing your age without having to show ones' passport or drivers licence). Swan [25] argues that blockchain technology still has many issues that need to be addressed, before individuals feels comfortable sharing their personal information in a 'decentralised manner'. Yet even such decentralised technology enables self-sovereign identity –bringing more control to the individual over managing personal information, and lowers the risk of 'joined up' cumulative identity theft.

Can online identity be self-sovereign? Can we securely manage our own personal data, sharing only what we want to share, so we do not have to put trust in other parties? We propose a potential solution which could combine of aspects of the decentralised technology/ transaction and centralised governance. This could be a flexible user-centric identity approach aiming to provide user-friendliness of authentication procedures, while at the same time ensuring strong authentication to service providers. As governments play a significant role in enabling and regulating the new digital identity ecosystem. While there are several unknowns about blockchain technology, we advocate for future research to address technical and privacy challenges for personal records. Buttarelli [6] argues that it is important that technologists and designers have to work closely to implement data protection law so the users share minimal information, contrary to the current practice where private companies and governments collect large amount of data sets and store them indefinitely. EU General Data Protection Regulation (www.eugdpr.org/), which includes the 'right to be forgotten', are difficult to regulate and new technologies can have aspects deigned in functions to support online privacy and safety. It is necessary that we as researchers, technologists, designers and also users to study and understand how to maximise the benefits of this technology to attain better development outcomes.

Acknowledgements

This research was funded by EPSRC grant EP/N02799X/1 (TAPESTRY: Trust, Authentication and

Privacy over a DeCentralised Social Registry) as part of the EPSRC Trust, Identity, Privacy and Security in the Digital Economy funding call.

References

1. BBC. 2017. *Yahoo 2013 data breach hit 'all three billion accounts'.* Retrieved January 28, 2018 from http://www.bbc.co.uk/news/business-41493494
2. BBC. Celia Hatton. 2016. *China 'social credit': Beijing sets up huge system.* Retrieved January 28, 2018 from http://www.bbc.co.uk/news/world-asia-china-34592186
3. BBC. Leo Keilon. 2014. *eBay makes users change their passwords after hack.* Retrieved January 28, 2018 from http://www.bbc.co.uk/news/technology-27503290
4. BBC. Dave Lee. 2017. *Uber concealed huge data breach.* Retrieved January 28, 2018 from http://www.bbc.co.uk/news/technology-42075306
5. Digital India. 2014. *A programme to transform India into digital empowered society and knowledge economy.* Press Information Bureau. *20 August 2014*.
6. Giovanni Buttarelli. 2017. *Privacy matters: updating human rights for the digital society. Health and Technology.* 7, 4. 325–328.
7. Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. 2015. *Blockchain Technology Beyond Bitcoin*. Sutardja Center for Entrepreneurship & Technology.
8. Mariana Dahan and Michel Casey. 2016. *Blockchain technology: Redefining trust for a global, digital economy.*
9. Shyam Divan. 2016. *India's Biometric Tsunami: Will it Sweep Away Privacy and Drown Civil Liberties?* Lawasia Intellectual Property and Technology Conference. Kuala Lumpur, Malaysia. Privacy and Surveillance Technology.
10. Pam Dixon. 2017. *A Failure to "Do No Harm" India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* Health and Technology. 7,4. 539–567.
11. Paul Dunphy, and Fabian A. P. Petitcolas. 2018. *A First Look at Identity Management Schemes on the Blockchain.* IEEE Security and Privacy Magazine special issue on "Blockchain Security and Privacy".
12. Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed and John Vines. 2018. *Making Sense of Blockchain Applications: A Typology for HCI.* CHI 2018, April 21–26, 2018, Montreal, QC, Canada. (to appear 2018)
13. Don Galeon and Brad Bergan. 2017. *China's "Social Credit System" Will Rate How Valuable You Are as a Human.* Futurism. Retrieved January 28, 2018 from https://futurism.com/china-social-credit-system-rate-human-value/
14. The Guardian. 2018. *Personal data of a billion Indians sold online for £6, report claims.* Retrieved January 28, 2018 from https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar
15. General Data Protection Regulation website www.eugdpr.org/
16. Salvatore Iaconesi. 2017. *The Financialization of Life. Startups & Venture Capital.* Retrieved January 30, 2018 from https://startupsventurecapital.com/the-financialization-of-life-a90fe2cb839f
17. Ron Miller. 2017. *Equifax data leak could involve 143 million consumers.* TechCrunch. Retrieved January 30, 2018 from https://techcrunch.com/2017/09/07/equifax-data-leak-could-involve-143-million-consumers/
18. Sharifah Mumtazah Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan. 2012.

Technical Issues and Challenges of Biometric Applications as Access Control Tools of Information Security. International Journal of Innovative Computing, Information and Control ICIC International. 8,11.

19. Santoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved January 30, 2018 from https://bitcoin.org/bitcoin.pdf
20. Clinton Nguyen. 2016. *China might use data to create a score for each citizen based on how trustworthy they are.* Business Insider. Retrieved January 30, 2018 from http://uk.businessinsider.com/china-social-credit-score-like-black-mirror-2016-10?r=US&IR=T
21. Frank Pasquale. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Harvard University Press.
22. Raja Siddharth Raju, Sukhdev Singh and Kiran Khatter. 2017. *Aadhaar Card: Challenges and Impact on Digital Transformation.* Retrieved January 30, 2018 from https://arxiv.org/ftp/arxiv/papers/1708/1708.05117.pdf
23. Manish Singh. 2017. *India's Aadhaar with biometric details of its billion citizens is making experts uncomfortable.* Mashable UK. Retrieved January 30, 2018 from https://mashable.com/2017/02/14/india-aadhaar-uidai-privacy-security-debate/#BH29Ghqm1OqK
24. Tathagata Satpathy. 2017. *The Aadhaar: "Evil" Embodied as Law.* Health and Technology. 7,4. 469–487. Retrieved January 30, 2018 from https://link.springer.com/article/10.1007/s12553-017-0203-5
25. Melanie Swan. 2015. *Blockchain Blueprint for a new economy.* O'Reilly.
26. Sarah Underwood. 2016. *Blockchain beyond bitcoin*. Communications of the ACM. 59,3. 15–17.

Authors' Bio

Arthi Manohar is a Design Research Fellow working on TAPESTRY project funded by the RCUK Digital Economy Programme at Northumbria University, UK. Arthi is developing and evaluating creative methods with emerging technologies such as blockchain and Distributed Ledger Technology. Her research interests are particularly concerned with the role of human values to change the way we engage with communities to help us be more creative, responsive and reflective by investigating the relationship between the social design and technology.

Jo Briggs is Co-Investigator of the TIPS TAPESTRY project and Associate Professor of Design at Northumbria University, UK. Briggs uses practice-led design approaches to explore complex and/or emergent digital-socio systems primarily across two interconnecting themes: design for digital engagement; and the design, use and 'disruptive' effects of peer-to-peer systems and platforms (e.g. crowdfunding, timebanking and now blockchain). Brigg's research is invariably multidisciplinary and/or cross-sectoral, including that situated 'in the wild'.