Blockchain and a Digital Identity System: Simply another mislead application of a popular technology

Rachael Robinson

December 14, 2016

Abstract

In today's world, there are many things that contribute to one's identity. A single person could have a multitude of numbers coming from multiple credit card numbers, a social security number, certificates, birth or otherwise, as well as other various pieces of documentation that verify their identity. These people can then use these to authenticate that they are who they claim they claim to be with the outside world. Unfortunately, as the volume and complexity of transactions as well as the possible repercussions increase, so does the need for digital identity. Currently, many developers and companies are looking to apply the popular blockchain technology as a solution to creating a secure digital identity system. While other systems utilize this technology, whether or not identity can also make use of a blockchain is questionable. Rather than immediately jump to apply popular technologies to current problems, developers and those investing in these solutions should question the use of these technologies and be mindful of the implications.

Introduction

The Need for Digital Identity

As a law of identity, no two people share an identity. This law allows people to then use these forms of identification, be that a number, a thumbprint, or other form, to create trust and ensure that they are who they claim to be. With many different forms of identification from multiple issuers and many more transactions occurring online, the future, as Australia Post CEO Ahmed Fahour, said, "is going to be a digital identity, so that when [a user] say[s] who [they] are, I can tell who [they] are."[1] This ability to authenticate users is an effort to create trust within the Internet. According to Bourass et al., digital identity comes down to a "set of descriptive data that reveals the identity of the user in the web."[2] While the current identity systems in place may appear to work well enough, identity fraud is rampant and the push for digital identity is still present.

According to the World Economic Forum and its *Blueprint for Digital Identity*, digital identity is a top priority due to multiple factors. First, there is an increase in the number of transactions occurring through digital channels.[3] Second, the complexity of these transactions, that is to say the complexities of the relationships between entities, is increasing.[4] Third, "regulators are demanding increased transparency around transactions."[5] That is to say that the regulatory requirements are becoming more stringent and companies must find a way to comply.[6] And lastly, "bad actors in financial systems are increasing [their sophistication] in the technology and tools that they use to conduct illicit activity, increasing their ability to quickly cause financial and reputational damage by exploiting weak identity systems."[7] In other words, those committing identity theft and fraud are finding ways to attack weak systems and are growing stronger. Due to these four points and more, many companies are investing in the development of a digital identity system.

This push for digital identity also comes from a push to digitize much of our world and our

[1] Stan Higgens, "Australia's Postal Service Tests Blockchain Identity - CoinDesk," CoinDesk, August 08, 2016, accessed December 13, 2016, http://www.coindesk.com/australia-post-blockchain-identity-voting/.

[2] Ismail Bourass, Nadia Afifi, Hicham Belhadaoui, Mohamed Ouzzif, Reda Filali Hilali. "Towards a New Model of Management and Securing Digital Identities." Paper presented at the 2014 Fifth International Conference on Next Generation Networks and Services (NGNS) May 28-30, 2014, Casablanca, Morocco, p. 308.

[3] World Economic Forum. "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity." August 2016, p. 18. http://www3.weforum.org.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

economy. As stated by Rick Wingfield, a partner for the Australia Post Accelerator unit, at the 2016 Technology in Governance conference, "If we're going to successfully digitize the economy and the hard parts of the economy that haven't been digitized yet ... the hard things like health, education and government services, those things require trust. If we're going to digitize some of those things, then we need to know someone is who they say they are."[8] As we move from a world of paper to screens and look to digitize these records that are often used as identification, there will need to be some sort of digital identity to access these. Thus, any sort of system for digital identity system must be secure and create as much trust as needed between two entities.

In order for a digital identity system to match the current systems in place, the solution must allow for the following. A digital identity system needs to be capable of issuing identities and then storing each user's identity data.[9] This system needs to be able to authenticate a user when said user attempts to assert their identity as well as authorize a user for transactions upon authentication.[10] Users should also be able to recover and "regain access to their identity data, should they lose it" as well as update the data associated with their identity.[11] Lastly, "identity data and the process by which it is recorded and accessed needs to be auditable. . . ."[12] That is to say that the validity of the identity system should be assessable. These are considerations and precautions that must be included when designing and developing a digital identity system.

Blockchain and Identity

Many companies and groups, from IDEO CoLab to big Financial Technology companies around the world, are currently investing a great deal of time and money to bring about a digital identity system. This is because "[n]o entity seems to be immune – from small banks to large health insurance companies; organizations of all sizes in many industries are affected. Criminal fraudsters are illegally accessing millions of consumer credit cards and private data files, even while new payment systems are evolving with new technology and capturing consumer spending habits."[13] With the possibility

[8]Stan Higgens, "Australia's Postal Service Tests Blockchain Identity - CoinDesk," CoinDesk, August 08, 2016, accessed December 13, 2016, http://www.coindesk.com/australia-post-blockchain-identity-voting/.

[9]Dan Elitzer, "A Framework for Identity," IDEO Colab, May 24, 2016, accessed December 13, 2016, https://medium.com/ideo-colab/a-framework-for-identity-f7f072829cbb.fvqoz5pce.

[10]Ibid.

[11]Ibid.

[12]Ibid.

[13]Amit, "12 Companies Leveraging Blockchain for Identification and Authentication," Let's Talk Payments, March 28, 2016, accessed December 13, 2016, https://letstalkpayments.com/12-companies-leveraging-blockchain-for-identification-and-authentication/.

of a widespread effect, many companies want to develop a digital identity system quickly and many of these endeavors involve some sort of blockchain.

Most of these companies, especially the Financial Technology, or FinTech, companies hope to leverage a type of blockchain within their digital identity system because a blockchain is a distributed database with limited trust between peers.[14] According to those hopeful about blockchain's involvement with digital identity, the blockchain can be used for "[t]he storage of all types of data and transactions in a secure and open way" as well as assist in authenticating users over the Internet in real time in attempts to lower identity fraud.[15] These attributes lend themselves to many of the points above about a digital identity system and its requirements.

Proponents of the blockchain also claim that it will allow for authorization and identification, two important aspects of a digital identity system. There are hopes to combine "decentralized blockchain principle with identity verification" to create a digital identity.[16] This identity would "act as a digital watermark which can be assigned to every online transaction."[17] Although creating and attaching a "digital watermark" to online transactions does work towards creating trust within the Internet, these companies driving forward a blockchain based digital identity system are eager to overlook the limitations of such a technology.

To the Community

The need for a form of identification to distinguish oneself from the many is universal. According to Yorke Rhodes, a Blockchain Business Strategist, millions of children are born but do not officially exist because they lack any sort of legal identification.[18] He claims that, "without legal identification, children and people are invisible to society which makes them most vulnerable to trafficking, prostitution and child abuse."[19] The need for digital identity also extends beyond legal identity for children in so far that it does not only offer solutions to obtaining identity to distinguish one from

[14]Dmitry Khovratovich, Jason Law. "Sovrin: digital identities in the blockchain era." Github Commit by jasonalaw October 17, 2017. Accessed December 13, 2016. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/topics-and-advance-readings/Sovrin–digital-identities-in-the-blockchain-era.pdf

[15]Amit, "12 Companies Leveraging Blockchain for Identification and Authentication."

[16]Ibid.

[17]Ibid.

[18]York Rhodes, III, "What Does Identity Mean in Today's Physical and Digital World?," Microsoft Azure Blog, May 31, 2016, , accessed December 13, 2016, https://azure.microsoft.com/en-us/blog/what-does-identity-mean-in-today-s-physical-and-digital-world/.

[19]

the rest of the world, but this new system could also improve the current situation of identity theft.

The United States Department of Justice defines identity theft and identity fraud as "terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."[20] And according to the United States Bureau of Justice, "17.6 million U.S. residents experienced identity theft in 2014."[21] Granted, the amount of information located online does nothing to ameliorate the situation; someone can still fall victim to identity theft or fraud without ever using a computer. A lost wallet, an overheard conversation, trash are all pieces of information that a thief can use to piece together someone else's identity.[22] These bits of identity that can be left around, found online, or taken by some other means, make people susceptible to social engineering hacks where a malicious attacker uses this information to gain access to even more data. And with the number of online transactions taking place increasing as well as hacker work around techniques and tools to gain this information, the need for a secure digital identity is prominent. While the push towards digital identity has begun, the immediate reliance on blockchain technology will be ultimately detrimental to the design of a digital identity system.

Action

"The real impact of blockchain was always going to be its inspiration. Blockchain 'squared the circle' in digital currency and that was amazing. But the first generation algorithm is not efficient or practical for other applications, What the community needs is real research and development that will begin to solve these challenges — not solutions that arbitrarily jam the blockchain algorithm into every pet problem."

- Steve Wilson, Constellation Research [23]

While the push towards digital identity means well and gears us towards gaining more trust within the Internet and possibly decreasing identity fraud, the immediate jump to and the reliance

[20]The United States Department of Justice, "Identity Theft," Updated December 2, 2016, accessed December 13, 2016, https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

[21]Bureau of Justice Statistics. "17.6 Million U.S. Residents Experienced Identity Theft in 2014." Press Release September 27, 2015. Bureau of Justice Statistics. Accessed December 13, 2016.

[22]United States Computer Emergency Readiness Team. "Security Tip (ST05-019): Preventing and Responding to Identity Theft." US-CERT. September 17, 2008. Last Updated October 1, 2016. Accessed December 13, 2016. https://www.us-cert.gov/ncas/tips/ST05-019.

[23]JP Buntinx, "Swirlds Addresses Blockchain Limitations with Hashgraph," Bitcoinist, June 7, 2016, accessed December 13, 2016, http://bitcoinist.com/swirlds-blockchain-limitations-hashgraph/.

on blockchain technology are misplaced. As a popular and innovative technology, blockchain has gained a following and many seem to view it as the end all to many problems within the digital world. Blockchain technology has been used in previous applications, such as cryptocurrencies, to bring about distributed consensus, which in turn works to generate distributed trust, but developers and investors are eager to overlook or ignore its shortcomings. This rush to integrate a technology into a system and deploy a products is not uncommon in the technology industry and it leads to potentially faulty systems that could put users at an increased risk.

For example, because of its proof-of-work algorithm, blockchain technology does not have trusted timestamps or proof of receipts.[24] Systems that rely on a blockchain "have distributed trust, but do not ensure fair ordering of events. . . ."[25] This makes it difficult for these sorts of systems to enforce fairness, a concept much needed in order to match buyers with sellers in auctions and stock markets which need to authenticate users.[26] Additionally, there have been a number of hacks into applications of blockchain technologies recently. With these inherent limitations and vulnerabilities of the blockchain, developers and investors should consider other technologies, such as hashgraphs, when looking to develop a digital identity system.

Accordingly, in order to engineer and develop software and systems to integrate into the world today, engineers, developers, and investors all need to look at technologies through a much more critical lens. No single technology should become the solution to all of the current digital challenges we face before we explore others. This especially applies to those we view as popular technologies.

Not only should developers proceed with caution when looking to force a popular technology into their system, but they should also take the time to reflect on how and why they are developing a system in a certain way. To avoid creating a vulnerable or faulty system, more research into the tradeoffs and consequences of a system failure need to be done. Those developing systems or solutions need to understand the systems they are building, the implications of the systems they are trying to put in place, and how to best protect them.

[24] Ibid.

[25] Swirlds, "Swirlds Emerges from Stealth with Blockchain Alternative Technology: Better Security and Fairness, Without Wasteful Mining," news release, June 6, 2016, Swirlds, accessed December 13, 2016, http://www.swirlds.com/swirlds-emerges-stealth-blockchain-alternative-technology-better-security-fairness-without-wasteful-mining/.

[26] Ibid.

Conclusion

"This is what happens when you deploy technology naively and you don't think about the implications"

- Ming Chow

By forcing a solution or system to use a particular technology with a lack of information about said technology, these investors are encouraging a weak, vulnerable, or inadequate system. Thus, it is particularly important for developers and companies investing in these systems to view their solutions critically. Rather than employ a technology because it is the current popular technology, those creating solutions need to clearly understand the tradeoffs of the technologies they wish to utilize for their solutions. In a world where solutions are designed and brought to fruition with little testing or research of the consequences of a system failure, it is imperative that we begin to take these steps in order to create appropriate systems for the current challenges of the digital world, especially digital identity.

Bibliography

Amit. "12 Companies Leveraging Blockchain for Identification and Authentication." Let's Talk Payments. March 28, 2016. Accessed December 13, 2016. https://letstalkpayments.com/12- companies-leveraging-blockchain-for-identification-and-authentication/.

Bourass, Ismail, Nadia Afifi, Hicham Belhadaoui, Mohamed Ouzzif, Reda Filali Hilali. "Towards a New Model of Management and Securing Digital Identities." Paper presented at the 2014 Fifth International Conference on Next Generation Networks and Services (NGNS) May 28-30, 2014, Casablanca, Morocco.

Buntinx, JP. "Swirlds Addresses Blockchain Limitations with Hashgraph." Bitcoinist. June 7, 2016. Accessed December 13, 2016. http://bitcoinist.com/swirlds-blockchain-limitations-hashgraph/.

Bureau of Justice Statistics. "17.6 Million U.S. Residents Experienced Identity Theft in 2014." Press Release September 27, 2015. Bureau of Justice Statistics. Accessed December 13, 2016. http://www.bjs.gov/content/pub/press/vit14pr.cfm/.

Elitzer, Dan. "A Framework for Identity." IDEO Colab. May 24, 2016. Accessed December 13, 2016. https://medium.com/ideo-colab/a-framework-for-identity- f7f072829cbb/.

Higgens, Stan. "Australian Delivery Service Exploring Blockchain Identity Solutions CoinDesk." CoinDesk. March 16, 2016. Accessed December 13, 2016. http://www.coindesk.com/australian- delivery-service-exploring-blockchain-identity-services/.

Higgens, Stan. "Australia's Postal Service Tests Blockchain Identity - CoinDesk." CoinDesk. August 08, 2016. Accessed December 13, 2016. http://www.coindesk.com/australia-post-blockchain-identity-voting/.

Khovratovich, Dmitry, Jason Law. "Sovrin: digital identities in the blockchain era." Github Commit by jasonalaw October 17, 2017. Accessed December 13, 2016. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/topics−and-advance-readings/Sovrin–digital-identities-in-the-blockchain-era.pdf/.

Rhodes, York, III. "What Does Identity Mean in Today's Physical and Digital World?" Microsoft Azure Blog. May 31, 2016. Accessed December 13, 2016. https://azure.microsoft.com/en-us/blog/what-does-identity-mean-in-today-s-physical-and-digital−world/.

United States Computer Emergency Readiness Team. "Security Tip (ST05-019): Preventing and Responding to Identity Theft." US-CERT. September 17, 2008. Last Updated October 1, 2016. Accessed December 13, 2016. https://www.us-cert.gov/ncas/tips/ST05-019.

The United States Department of Justice. "Identity Theft." Updated December 2, 2016. Accessed December 13, 2016. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

World Economic Forum. "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity." August 2016. Accessed December 13, 2016. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf/.