

Prospectus


A New Web of Trust
(Technical Topic)


The Paradox of Digital Trust
(STS Topic)

By
James Foster

November 1, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed:  _____ Date 20 April 2022
James Foster

Signed:  _____ Date 10 May 2022
Richard D. Jacques, Ph.D., Department of Engineering & Society

Introduction

Relationships are dependent on the fine filament of trust that holds them together. Each individual in a relationship recognizes a certain level of dependability from the other party involved. At first, the level of dependability makes it difficult to confide secrets in someone who is not a close friend, a relative, or an expert in their field. As time goes on and people are more exposed to each other through conversations and interactions, they relax and it becomes more comfortable to reveal information to an individual that is now considered trustworthy. This is the natural process of discerning friend from foe and potential confidants from gossipers. It is an exhaustive and lengthy process that has now become overbearing as it has translated to the online world. The internet allows us to add "friends" and meet new people at an accelerated rate. It has become costly to double check if every website visited is to be trusted and every user added a true friend. It is not feasible for each internet user, on their own, to evaluate these variables every day. Take, for instance, an online persona masquerading as someone they are not. It is impossible for a layperson to verify the legitimacy of the account and its owner without watching the user create it right before their eyes. Scenarios similar to this occur all too frequently while people wander online. They imbue users with distrust toward all digital media. Consequently, it would be beneficial to have an underlying technology that un.masks all the users and media that we encounter online. I will design a robust and decentralized service that allows users to advertise and share who and what they trust with other users. I will also explore the paradox of digital trust and how it affects online media.

Technical Discussion

It is elementary for users to identify and verify themselves to the medium they are using online, but near impossible for them to verify other users that exist on the medium with them. It is not that there is a lack of data to confirm these details, given that all user data is stored on the cloud, or private corporate servers, but rather that there is no channel or logic for this type of function. This is a difficulty especially faced by individuals who use social media. Since the 2016 election it has become clear how prevalent malicious actors are online, disseminating misleading information, scamming individuals out of their money, and even phishing for them to download malware. The environments where these actors live are ones we all know well: Facebook, Instagram, and Twitter among others. These companies chiefly want to protect their own business from such ill-mannered individuals but do not pay too much mind if their own user base is exposed to them. Time and again, the companies divert attention away from their feeble security protocols by blaming hackers. This is unfortunate and users should be able to have more confidence online and not have to worry if another user they are interacting with is a bad actor. My system will try to answer this call. It will be designed around a social networking trust platform. Users will add other users as "friends" and assign them a trust "rating". Users will also be able to rate businesses in a similar

manner. This data will be distributed to the original user's friends and they will be able to see which entities their "friends" trust. This is so that individuals have a group of users whom they trust to some degree, who in turn trust other users, who also trust others, et cetera until a web of trust is formed. This idea sounds novel, but it has been around for a while. One of the earliest implementations of this was the Pretty Good Privacy encryption keys and practices. Users each own a key-pair that consists of a public and private component. The public key component allows users to build your own personal web of trust (Lucas, 81). A user simply must sign another individual's public key to indicate to others that they have verified that individual's public key and identity. This process is repeated ad infinitum, and eventually a web of verified PGP keys and identities is formed; a web of trust. PGP was designed for encrypting emails and is rarely used today, but it still works as intended. My system will build on this idea and assign users encryption keys that will be hidden and verified in a decentralized manner: through a consensus of users. This is similar to a more modern technology, called blockchain. It is a decentralized, immutable ledger that keeps records of digital transactions (Choo, 33). A couple of downsides of blockchain technology is the price users must pay in "gas" to transact with the chain and the number of active verifier nodes that must be active for the chain to function. My system will instead take the form of a distributed ledger that exists on each user device, in parts, and can be refreshed upon connection with an internet source giving access to the trust system server. The records each user will submit to the ledger will simply be their own connections and trust ratings they have accumulated on the trust service. Other users with overlapping information will verify that this new information is correct. The users' devices will gossip with each other to form a majority opinion to validate new information on the system and make sure malicious attacks are snuffed out. As users amass larger "friend" groups through the service it will be harder to fool the ledger and input malicious or misleading data. The most practical applications for this system will involve extensions on web browsers and background services on mobile devices. All of this, of course, is the end goal and much testing will first occur on a smaller centralized system and a virtualized distributed system before the trust service can be implemented on real devices.

STS Discussion

Consumer trust is vital for the success of any business. If people distrust a company or their practices then they will avoid using the services provided by them. This has been the dynamic for thousands of years. However, in the age of industrialization and with the rise of mega corporations, this practice is becoming more difficult to uphold. Companies today, especially online, are diversifying and carving out large portions of the market for themselves. Acquisitions and mergers are becoming more commonplace and large companies are able to expand immensely. Instances such as Facebook's purchase of WhatsApp for \$19 billion (Covert) allow companies to hold more market share and influence over consumers. These mega-corporations are perfect targets for hackers who want to steal user data and sell it for profit. One such breach on

Facebook in 2019, five years after their acquisition of WhatsApp, leaked the information of 400 million Facebook accounts (O'Sullivan). It is events such as this that have now led consumers to distrust the security and competency of companies involved online. Even so, the monthly active users on Facebook continues to climb. A staggering 2.8 billion Facebook users existed as of December 31, 2020 as compared to 2.5 billion in 2019 (Richter). Herein lies the paradox of digital media; even if users distrust an online company and their business practices, they continue to use the service. This phenomena applies to many other online giants that provide unique, unmatched services. Amazon, for instance, commonly puts their own products before competitors and requires large fees from third-party sellers (Weise), yet it is still one of, if not, the largest online retailers in the world. Users understand the flaws with these companies, but cannot resist using them due to their ease of use and cost effectiveness. It is more difficult to stop utilizing the services these companies have developed and find new ones than it is to continue using them and ignoring the privacy and data concerns. However, these are just centralized companies whose business models have been found to be prone to corruption, scandal, and ineffectiveness (Botsman). With the introduction of blockchain to the mainstream, now is the time to query whether decentralized companies and applications will also be in danger of the same ailments. Decentralized technology touts transparency and trust due to the intrinsic nature of the underlying mechanisms, where nodes on the chain come to a consensus to verify transactions before allowing them to occur (Gao). However, this is just describing the security of the technology itself and not the trust required from humans to validate its usage. To avoid the trust paradox that centralized entities are tangled up with, decentralized systems must ensure the infallibility of their technology. This goes beyond the code itself, it also regards the advisory boards that oversee the development of the blockchains. These groups must also be held to high standards and should not feel the need to bend the knee to lobbyists or corporate strongmen. Decentralized businesses will soon be commonplace, and it is in everyone's interest that they differentiate their impact on users from that of their centralized brethren.

Conclusion

My technical work aims to join the ranks of upcoming decentralized solutions and harden the trust users have in individuals and entities online. This will allow for a less stressful online experience for many individuals as they are able to see the opinions of their trusted connections regarding a website or a user versus having to trust the comments of a John Doe they encounter online. These individuals can then make more informed decisions while browsing the internet. Along those lines, decentralized tech as a whole needs to step up and deliver on their promise for a more reliable basis to conduct business online. The markets are currently flooded with decentralized start-ups which is a good prospect for the future. Competition must remain high in the decentralized ecosystem so that businesses are incentivized to innovate and retain the trust of their users. Right now, money, in the form of cryptocurrencies, is encouraging the decentralized platform excitement. Many users are investing in these technologies

today even though many are vaporware: that is, they have not been implemented yet. In the near future, to retain these financial gains, these platforms and their technologies must be used in real world applications. Adoption by governments and regulations they impose will also vastly increase the legitimacy of this technology and its potential. These things will stave off the digital trust paradox and allow the technology to be much more easily trusted than centralized competitors. Only time will tell if decentralized services are the best way forward, but it is exhilarating to be able to watch an entirely novel form of business develop in the 21st century.

References

- Botsman, R. (2021, August 31). The Changing Rules of Trust in the Digital Age. Retrieved October 13, 2021, from <https://hbr.org/2015/10/the-changing-rules-of-trust-in-the-digital-age>
- Covert, A. (2014, February 19). Facebook buys WhatsApp for \$19 billion. CNNMoney. Retrieved October 23, 2021, from <https://money.cnn.com/2014/02/19/technology/social/facebook-whatsapp/index.html>.
- Choo, K. R., Dehghantanha, A., & Parizi, R. M. (2020). Blockchain cybersecurity, trust and privacy. Cham: Springer.
- Gao-19-704SP, Science & Technology spotlight: Blockchain. U.S. Government Accountability Office. (n.d.). Retrieved October 23, 2021, from <https://www.gao.gov/assets/gao-19-704sp.pdf>.
- Harper, R. (2014). Trust, computing, and Society. Cambridge University Press.
- Lockwood, F. (n.d.). Get in Touch. Retrieved October 12, 2021, from <https://www.dronedeliverygroup.org/the-trust-paradox-how-much-trust-is-enough>
- Lucas, M. W. (2006). PGP & GPG: Email for the practical paranoid. San Francisco, CA: No Starch Press.
- O'Sullivan, D. (2019, September 5). Hundreds of millions of phone numbers tied to Facebook ... CNN. Retrieved October 24, 2021, from <https://www.cnn.com/2019/09/04/tech/facebook-phone-numbers-exposed/index.html>.
- Richter, F. (2021, February 4). Infographic: Facebook keeps on growing. Statista Infographics. Retrieved October 24, 2021, from <https://www.statista.com/chart/10047/facebooks-monthly-active-users/>.
- Weise, K. (2019, December 19). Prime power: How Amazon squeezes the businesses behind its store. The New York Times. Retrieved October 24, 2021, from <https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html>.