Application of the Blockchain For Authentication and Verification of Identity

Ben Cresitello-Dittmar
November 30, 2016

Abstract

The greatest obstacle for migrating many services online is the ability to secure the data and verify the identity of the users of that service. Currently, online authentication relies on a password or on rare occasions the use of dual-factor authentication. The problem with these methods are that passwords are notoriously insecure and dual-factor authentication generally relies on sending a code over SMS or a third party service. A solution to this problem could be the blockchain. Currently, the blockchain is used to handle the ledger for a $10 billion dollar currency. However, the same cryptographic principles could be applied to authentication.

By distributing a ledger among all members of the network, blockchain authentication eliminates someone from maliciously altering the ledger. Every time a 'transaction' or block of data is added to the chain a majority of the network must verify its validity. This guarantees the integrity of the ledger. One could then use public key encryption, such as the extremely secure RSA encryption, to securely send their credentials. The recipient could then verify this against an entry in the immutable blockchain resulting in an incredibly secure and reliable way to handle verification of identity.

These principles could be applied to transition everything from the electoral process to state identification cards to dual-factor authentication into a secure, fast, reliable, and readily available service.

1 Introduction

The blockchain provides a solution for a variety of different security concerns that are present in our everyday lives. Every day we are tasked with proving our identity, either by entering credentials for an online service such as Facebook , or Outlook or showing a drivers license to prove we are who we say we are. These methods however are antiquated and wrought with security concerns. Email and password credentials are notoriously easy to crack as can be seen in the latest Yahoo breach of 500 million accounts.[1] Drivers licenses on the other hand have the risk of giving someone more information than they need to. If a store needs to verify your age they only need to know that you are who you say you are and your date of birth but they are also provided with address, height, weight, hair color, and eye color. Information that may be crucial in stealing ones identity. The ideal solution would be a form of authentication that only grants access to certain information and eliminates the need for each service provider to store credentials for every client. The blockchain can offer this approach by decentralizing the ownership of credentials and offering a universally available protocol for verifying one's record in a immutable chain of data. This data rather than being stored on a per app basis is stored in a shared ledger. This shared ledger is downloaded by each individual user of the blockchain and is a record of every transaction ever made.

1.1 Why the blockchain is secure?

The blockchain's relies on 3 major pillars, consensus, distributed, and trustless, and the security is derived from a proof of work problem.[2,3] This problem is design to take a large amount of computational power to complete and thus, for a single person working it may take years but for a network of computers it may take only minutes. "Proofs of work that are tied to the data of each block are required for the blocks to be accepted. The [difficulty of this work](/what-is-bitcoin-mining-difficulty/) is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes."[4] Thus, the chain can be continually added to and transactions are still processed in a timely manner while securing the data from tampering. The nature of this problem makes it mathematically impossible for someone to change the blockchain. "Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain."[5] This could theoretically be done given enough time but the formerly mentioned public ledger is chosen by a consensus, where the network of users agrees on the longest blockchain to be the recognized chain. This makes up the first pillar of the blockchain. By agreeing on the longest blockchain, the only way for a user to successfully alter the chain would be to alter a block and then generate subsequent transaction blocks to make a new longest chain. However, the usage of a proof of work problem makes this mathematically impossible. Because the network of users will be adding blocks at a much faster rate than any single person could add blocks. Thus, the security

is trustless, meaning the security lies in preventing malicious parties from doing harm by nature of the protocol, without having to authenticate a transaction.

Finally, the ledger is distributed, meaning that every user stores the current ledger, preventing someone from altering a single point of truth. In traditional cryptography, a single point of truth could be a certificate authority, however, if that certificate authority was to be breached, a malicious attacker could replace the stored keys with their own keys, thus enabling them to masquerade as a plethora of users. By distributing the ledger, an attacker would have to breach every member machine and replace the blockchain with their own making it functionally impossible for an attacker to alter the chain.

1.2 Applying the Blockchain to Authentication and Identification

New companies have now begun to harness the potential of the blockchain and develop a variety of services using the technology. The center of blockchain authentication would be a blockchain ID. This ID is essentially a block of data on the chain that can be both verified by any third and can display necessary information such as date of birth. The secret to this verification is the ECDSA (elliptic curve digital signature algorithm). When adding an ID to the blockchain, an identification issuing service binds a public key by default and then transfers ownership of the private key to the user. This allows the user, and only the user, to sign a signature that can be verified against the public key stored in the blockchain. This identification of a user would serve as a decentralized source of authentication. It would essentially be a single-sign-on portal that can be accessed by any app while not being owned by any single entity. A protected app would only have to request a digital signature and an ID from a user requesting access. The app could then verify that the signature is valid and that the user's ID verifies who they say they are.[6]

2 To The Community

The need for this technology is becoming all too vital, currently US retailers lose about $32 billion to fraud.[7] This is in no small part due to the horrible insecurity of our identification systems. However, switching entirely to this decentralized system is going to be a long process and in the mean time, users need a way to secure their data and identities. This is where multi-factor authentication comes in. Without having to scrap contemporary methods of authentication, service providers could enable multi-factor authentication with the blockchain. This would serve to add an extra layer of security to applications while slowly introducing people to the benefits of the blockchain. As easy to use as taking a picture, the entire process could be automated, only requiring the user to create an ID and download an app that handles the necessary authentication handshakes. The decentralized nature of the blockchain could allow the user to manually sign the request and return it, however, for usability one would most likely rely

on an app that leverages this technology. Simply take a picture of a QR code that encodes the authentication request and the app would sign the request and return it to the protected app. In a day and age where our smartphones rarely leave our sides, this form of two-factor authentication would be incredibly easy to adopt by not only the power-user, but also the average consumer.

3 Problems With Current 2-Factor Authentication

There are a few options currently used for two-factor authentication. These have relatively wide spread adoption, however, the methods are antiquated and pose other security threats. For example, one of the most common methods is to send a code over SMS. This is great, however, SMS messages are notoriously insecure. A potential attacker could sniff messages from any number and read them in addition to spoofing the sender of the message.[8] This posses a great problem because if an attacker knows that your account uses text messages as a backup method of authentication and your name, they could find your listed phone numbers online and then intercept those messages, gaining access to whatever code they send. It is easy and ubiquitous but impossible to secure without changing the SMS protocol itself. The other problem with current two-factor authentication is the proprietary nature of the services. Methods such as Google Authenticator are secure and easy to use, however, Google then has access to all your two-factor codes. This option is much more secure but brings back the issue of a single entity owning the authentication data. A breach of Google could cause all your authentication codes to be leaked. The decentralized approach offered by the blockchain eliminates this problem because the chain is 100% open to the public and no sensitive data is stored in the clear on the blockchain.

4 Applications of the Blockchain

Blockchain ID's are a viable solution to solve the task of verifying a user is who they say they are. Furthermore, this functionality could be expanded to do a variety of secure data transfers on behalf of an individual. One service deeply linked with identity verification is the sharing of identity information without the disclosure of unnecessary information. In addition to sharing data, a user could also add data to the chain as proof of a transaction, without giving away the original data of the transaction. Either party could verify a document against this entry and show that it is in fact valid, enabling fast and reliable audits of data. This methodology would be based on the principle of message signing and hashing. Many services already use this technology to securely verify data (such as JSON Web Tokens) while not disclosing the original data.

4.1 A Proposed Authentication Flow Using the Blockchain

A generic authentication flow that has been tested and utilized by companies such as Blockstack relies on a blockchain centered handshake. This 'handshake' verifies to both the authenticating app and the user that the other party they are communicating with who they think it is. In this example, the protected app is the application requesting authentication, and the user is the entity attempting to gain access to the protected app. The first step of this flow is similar to that of any login. However, the user would not be prompted to enter a password. Instead, a user would see a form on the protected app for a username, it will then either display a QR code for authentication or look in its records for the preferred method of authentication. The QR code example would be easier to set up and would simply encode the authentication request from the protected app.[9] This authentication request is the first step of the handshake. The next step is to verify the request and send a response. This step contains many steps to ensure authentication. First, the user would verify that the request data is legitimate and the protected website is who they are expecting. This could be done by using public key cryptography. This would allow the protected app to sign the request, which is then publicly verified either through the blockchain or a certificate authority.[10] In order to support simple transitions, it would be reasonable for this to begin with a certificate authority system used in TLS for HTTS. This could however be transitioned into a full blockchain authentication by creating an application ID on the blockchain which could then be verified. After verifying this request, the user would click a button saying verify login. This would then create a response, sign it, and then send it back to a specified route on the protected app. This request would then be verified using public key cryptography on the protected app and the user will be logged in.[11] The benefit of using the blockchain is that it is completely decentralized. If you didn't want to use an app to facilitate this flow, the user could simply generate their own signature with their public key and submit it in a form, which the website would then verify. This shows the true benefit of a decentralized system. Because anyone can access the data and the user is in control of their private key, then you as a user are not forced to use a given API to facilitate this request. Putting as much trust in other system as you are willing to give.

4.2 Sharing Only the Identity Information Want

A current problem with identity verification is that you are required to give more information than the system really needs. The problem with this if your transaction is compromised and someone is able to intercept the data in some way, they will have a lot of information to start forging an identity. To solve this problem, the previous authentication flow could be expanded to support this type of service. Blockstack has proposed a suggested format for these requests; first the protocol would first define a 'permission' set or request for particular set of data. This 'permission' level would be defined by a common use case.[12] For example, if the system wants to collect credit information, it could send a 'payment' request. Which the user could then see and

determine if they want to disclose their credit card information to this vender. If they trust it, they could sign the request and send a data packet containing the relevant information. If their bank supports blockchain authentication, they could simply send a signed payment packet, that the website could then forward to the bank and complete the transaction. Thus preventing the user from giving the store any personal information. Otherwise, the data packet could include the relevant financial information such as credit card number etc. However, the website in order to prevent fraud, could verify that this person is really the owner of the data and they are not using a stolen card. To do this, cryptographic hashing could be to verify the data, a principle applied by Tieron to achieve this effect. [13] The packet would first be hashed and signed by the user. This would tell store that it is really a given person sending the data. Next, the site would look on the blockchain for a signed and hashed version of that data. If the hashes match up along with the signatures, the store will know that the data is in fact associated with that person and that the data is un-tampered, giving them reasonable assure that the card is owned by the authenticated individual. By applying the principles used by Blockstack and Tierion, a comprehensive, secure, and most importantly, distributed system of authentication and identity verification could be established.

4.3 Anonymous and Secure Voting

Another use case of this technology could be secure and anonymous online voting, and the best part of this system would be that it could entirely leverage systems already in place. Just as a currency system is based on transactions that trade a limited amount of a given resource, voting is a system of transactions where everyone is only able to gain 1 unit of the currency and they must pay this one unit in order to submit a vote. Therefore, the system of transactions that the bitcoin is based on could be used to secure online voting. A potential solution to voting could be a system of government issued wallets. One would receive one of these wallets by verifying their identity and they would become the sole owner of this wallet. Each transaction would then use the blockchain to verify that no user overspends by voting more than once, thus securing that each person is able to vote only once.[14] However, voting is not only required to provide everyone with a vote, but also ensure the anonymity of such a vote. By design, the blockchain is completely public where everyone can trace back a transaction back to an address, however, the use of government issued wallets would prevent anyone from determining your real identity because a wallet itself does not need to contain any information about the user's identity. Of course, a potential attacker could still trace the transaction back to your system or determine that this transaction originated from you in a different way. Or perhaps it is better for you to associate this government wallet with a blockchain ID. In these cases, the system could rely on a commonly used anonymizing technique called bitcoin 'tumbling'.[15] This method, although simple, virtually ensured that this transaction can not be tracked back to a given wallet. This is achieved by

transferring a coin among a network of different wallets. Therefore, in the list of transactions, this coin appears to have been owned by everyone. Thus, obscuring the true owner of the coin and anonymizing the original owner.[16] The voting wallet could have this feature baked in, ensuring that everyone's vote is anonymous.

In addition to making voting simpler and quicker, and therefore most likely increasing voter turn out, this system would also ease concerns of a hacked voting system that has been a common concern after this most recent 2016 election. By using the blockchain, every vote is publically visible and therefore, easily auditable. Any person could therefore very easily and cheaply verify all votes for a given candidate. Making audits both cheaper and a regular part of the voting process. Giving the people more confidence in the voting system.

5 Final Remarks

Despite there being many possible applications for the blockchain, it should not be assumed that the blockchain is a perfect solution to these issues. As with any system, there are still drawbacks and insecurities. No system is 100% secure and therefore, this must be considered in the conversation to adopt this technology.

In the case of authentication, the problem is still that it may rely on a type of certificate authority, thus placing trust in a third part. In order to ensure that an ID is really the person that it says, more secure forms of verification would be required than simply using social media posts etc. Either a trusted authority must distribute these IDs or a third party must securely audit sensitive documents of the user that can better verify the ID. Therefore, similar to the case of certificate authorities for the TLS protocol, people would have to trust that these authorities are properly vetting these documents. A hash based system could be used to store a record of the document used so someone can verify that a document is for a given identity, however, this document may be sensitive and thus the owner would not want the plaintext to be available on the blockchain. This introduces the current issue of placing trust in a third party.

For voting, the concern becomes whether or not a given person is actually using their vote. By making the vote anonymous and making voting so easily accessible, there becomes the issue of people selling votes. If all one had to do to sell their vote is click a button that transfers their 'vote coin' to someone else, could this incentivize people to sell their vote? Because the vote is anonymous, this would remove the ability to trace each vote to a given person making sure that each vote is legitimate. The vote issuer would simply be ensuring that everyone is only in control of a single vote to begin with. Making voting easier could also make selling a vote easier. Furthermore, this would benefit certain people more than others. Tech savy individuals and

people with easy access to the internet would be more convenience by this system then those in impoverished regions because they would still have to travel to the equivalent of a polling area to make this transaction.

In regards to the security of such protocols, the transactions themselves can be considered sufficiently secure, the system relies on the elliptic curve digital signature algorithm public key cryptography to verify identities and associate data with a certain person. However, this makes one's private key essentially the key to their identity. If someone is somehow able to steal this key, they now steal your identity. You could potentially re-associate a different key with that ID by proving your identity, however, in that interim, an attacker would have full access to everything, therefore increasing the risk of losing this key. Furthermore, although ECDSA is extremely secure, and public-key cryptography is tried and true, people are notoriously insecure with such data. Especially in the case of people who do not understand the technology they are using, which would be a majority of the people using it.

These issues must be considered before creating a wide spread system of blockchain identities, however, the possible use cases and benefits to society are undeniable. As society becomes increasing techno and internet centric, a better form of digital identification is necessary and contemporary forms of authentication and identification are becoming increasingly insecure and insufficient for the world we are living in. A major overhaul of these systems is inevitable and the blockchain is a possible avenue to explore in solving these problems.

Endnotes

1. Constantin, Lucian. "Here's What You Should Know, and Do, about the Yahoo Breach." PCWorld. IDG News Service, 23 Sept. 2016. Web. 09 Dec. 2016. <http://www.pcworld.com/article/3123398/security/heres-what-you-should-know-and-do-about-the-yahoo-breach.html>.
2. Ibid
3. Mining?, What Is Bitcoin. "What Is Proof of Work." *Everything You Need to Know about Bitcoin Mining*. N.p., 18 June 2015. Web. 09 Dec. 2016. <https://www.bitcoinmining.com/what-is-proof-of-work/>.
4. Ibid
5. Ibid
6. Blockstack. "Blockchain Auth" GitHub. N.p., n.d. Web. 04 Dec. 2016. <https://github.com/blockstack/blockchain-id/wiki/Blockchain-Auth>.
7. Admin. "Identity Management on the Blockchain." *ShoCard Identity for a Mobile World*. ShoCard, 8 Oct. 2016. Web. 09 Dec. 2016. <https://shocard.com/cpt_news/identity-management-on-the-blockchain/>.
8. Dennis, Tonny. "Text/SMS Messaging Totally Insecure." N.p., 28 Feb. 2013. Web. 9 Dec. 2016. <http://www.theinquirer.net/inquirer/news/1041587/text-sms-messaging-totally-insecure>.

9. Blockstack. "Authentication" GitHub. N.p., n.d. Web. 04 Dec. 2016. <https://github.com/blockstack/blockchain-id/wiki/Authentication>.
10. Ibid
11. Ibid
12. Blockstack. "Blockchain Auth" GitHub. N.p., n.d. Web. 04 Dec. 2016. <https://github.com/blockstack/blockchain-id/wiki/Blockchain-Auth>.
13. "Tierion: Blockchain Proof Engine | API." Tierion - Cloud Datastore | Backed by the Blockchain. N.p., n.d. Web. 04 Dec. 2016. <https://tierion.com/features>.
14. @BitcoinMagazine. "Blockchain Technology: The Key to Secure Online Voting." Bitcoin Magazine. N.p., 27 June 2015. Web. 04 Dec. 2016. <https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899>.
15. @cryptorials. "How To Use Bitcoin Anonymously." Cryptorials. N.p., 05 Sept. 2016. Web. 04 Dec. 2016. <http://cryptorials.io/how-to-use-bitcoin-anonymously/>.
16. Ibid