Understanding the Safety of Information Contained within Blockchains

Author, Chris Tomlinson

A Data Science Foundation White Paper

July 2018

---

www.datascience.foundation

Data Science Foundation
Data Science Foundation, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3641 Email: contact@datascience.foundation Web: www.datascience.foundation
Registered in England and Wales 4th June 2015, Registered Number 9624670

Data security has never been a more important consideration for consumers or for the businesses they patronize and partner with. It's also never been more difficult to ensure. Every single day, consumers' personal, health and financial information is at risk of theft. This can lead to identity theft, and to serious financial ramifications.

While military-grade encryption on websites and through smartphone and tablet apps can be an important precaution, it's just a Band-Aid. More must be done. Blockchains may hold the key to ensuring data security, but how does the technology that underpins bitcoin and other cryptocurrencies ensure data security for consumers and businesses?

The State of Data Security Today

Currently, over 2.5 quintillion bytes of data are produced every single day. Most of that comes from the digital world – Twitter, Facebook, bank websites, financial advisers, and more. However, that information is not well protected. Even the most sensitive of information – think credit card numbers and Social Security numbers – is not really safeguarded all that well. Consider some of these eye-opening statistics:

- 2017 saw an average of 130 major security breaches per month.
- 2018 is expected to see 27% more major security breaches.
- Security breaches affect companies large and small, including global leaders like Equifax and Under Armour.
- A single data breach left hackers holding information about 3 billion users (Yahoo!).
- An attack at Equifax in 2017 compromised the identity of 147.9 million consumers.
- It takes the average company 50 days to rectify security after an attack.
- A new ransomware attack occurs ever 14 seconds.
- The Cambridge Analytica breach exposed the information of millions of people.
- 40% of larger companies around the world have no protection for customer credit card information or health records.

This, as they say, is just the tip of the iceberg. We live in the Digital Age, and data is big business. It has replaced financial assets as the most targeted for theft. With that data, hackers can do almost anything – they can apply for new credit cards in a consumer's name, or they can use their identity to establish residence in another area. They can create online accounts, and in some cases can even access bank accounts, or delve into sensitive health information.

Obviously, that's bad news. Our current security measures are just not enough to protect that data from all the threats out there. Blockchain has the potential to change that paradigm, though.

What Is Blockchain?

Unless you've been living under that proverbial rock, you've at least heard of blockchain technology. It's the platform on which things like bitcoin and ether operate. However, it's highly likely that you're not entirely sure what it is or how it works. There is also much more to blockchain than just cryptocurrency. While the technology is actually quite complicated, understanding it is relatively simple.

Blockchain is, at its heart, a distributed ledger system. That is, it allows information to be recorded, stored, and accessed remotely, without the need for a central storage system. Imagine a small business using Microsoft Excel to do its books on a single workstation on the business premises – this is a centralized system. There is only one source of control, one source of access, and one source of security and verification for the data. In a decentralized system, that's not the case.

The Guardian sums up the situation quite well. In an article for the publication written by Josh Hall, the author explains, "Blockchains are distributed ledger systems – that is, information is stored not in a single, centralised database, but in a potentially infinite number of places."

TechRepublic also offers a simple, direct explanation. "The blockchain ledger records every transaction that has ever taken place on that blockchain. That transaction gets verified, uploaded, and secured by anyone that's on that particular blockchain network."

Information contained within a blockchain is stored across multiple systems, with each user having access to the same information at the same time. The data is contained in a digital block, which is made up of transaction records. Each block is connected to the one before it, and the one following it, creating a seamless whole.

The data within those blocks is updated everywhere, instantly, to ensure accuracy. There's also the fact that data within the blockchain cannot be changed without a 51% majority consensus from those decentralized users. This means there is not a single point of failure that could give hackers access to consumer credit card, identity or health information.

In order for a hacker to gain access to and change the data within a single record within a larger block, they would need to gain access to the entire block, change the entire block, and then change the blocks adjoining it. That would require an immense amount of computing power to achieve.

There are also several other important security benefits to blockchain technology, which we'll explore in the next section.

Blockchain's Baked-In Data Protection Properties

Blockchain offers a number of baked-in proprieties that allow enhanced data protection and that make this technology a potential game changer for virtually every industry.

Peer-to-Peer Network Hosting: Perhaps the single most important protective property offered is the fact that blockchains are hosted on peer-to-peer networks. They are not contained on any single network. This means there is no single point of failure. In virtually every major data breach in the past several years, a single point of failure was responsible for hackers gaining access to business and consumer data.

A single phishing email leads to a purloined username and password, which then gives access to the records stored within a company's intranet, for instance. With blockchain, this is impossible because there is no single point of failure and no centralized storage for the data contained within the blockchain. As noted by The Guardian, that data is stored in a potentially infinite number of places.

Immutable: Blockchains offer the ability to create immutable records, which means they are virtually impossible to alter. As mentioned, any change to a single record within the blockchain requires a change to every single block within the chain. That requires either a 51% majority consensus, or enough computing power to force the issue, which is virtually impossible on all blockchains, and is completely impossible on large blockchains. Any single bad actor, or even a group of bad actors, can easily be identified and their acts prevented in this manner.

Continuous Updating: One of the most interesting aspects of blockchain technology is the fact that it is always up to date, and that all copies of the ledger stored with each peer on the network are updated at the same time. This ensures that all information is always accurate, and fosters trust and security.

In order for a new transaction to occur on the blockchain, it must be authenticated across the entire network, and only then can it be added to the next block in the chain. Because each node in the network contains a complete, up to date copy of all transactions, it becomes impossible to game the system.

Secure Timestamping: Timestamping is a concept that has been around for some time, and has numerous uses outside of digital technology. When it comes to blockchain, you'll find that secure timestamping plays a role in cryptographic protection. Every transaction within a blockchain includes a record of the transaction's date and time.

That information is stored within every copy of every transaction on the network, and it can be used to verify that the data within the record existed at a specific time and on a specific date. This helps to guard against the insertion of unauthorized changes within records on the blockchain.

As you can see, there are quite a few baked-in data protection properties inherent to blockchain technology. Moreover, those properties can be enhanced with any number of additional security measures. As Josh Hall wrote for The Guardian, "Connect that technology to existing payment systems and platforms, and combine it with biometric security features on our smartphones or tablets and we could then enjoy significantly more control over what information we share with whom – and say goodbye to passwords at the same time."

Understanding the Benefits of Blockchain for Data Security

We've explored some of the most important blockchain security protocols, but how do those translate into benefits where data security is concerned? How might consumers and businesses benefit from the application of blockchain in place of more conventional or traditional data security measures, such as endpoint encryption, or practicing good password hygiene?

For one thing, with blockchain, there is no need for user accounts and passwords in the first place, which eliminates the need for password hygiene, and may completely do away with the threat of phishing emails, as well. Of course, there's more to know here. In this section, we'll explore some of the more interesting benefits fostered by the use of blockchain technology for data security.

Multiple Authorizations – Accessing data stored on a blockchain will require multiple authorizations. These come from the inpidual nodes on the chain itself, and can be used to foster greater trust in a wide range of environments and use cases. As CIO magazine notes, "The digital signatures and verifications make it

difficult to envision a scenario wherein a bad actor could cause fraud and introduce problems that are costly to remove and resolve. The cryptographic integrity of the whole pending transaction, as well as examination by multiple nodes of the blockchain architecture, protect against threats and malevolent use of the technology."

This increase in trust could have dramatic repercussions for any number of situations, ranging from identity verification to applying for a home mortgage. It would play a role in business-to-business transactions and processes, business-to-consumer relationships, and even in consumer-to-consumer situations. With greater trust comes not only peace of mind, but greater speed in transactions, and more convenience.

Eliminating Third Parties – Third parties play crucial roles in a myriad of situations today. Take real estate transactions, for instance. Consumers buying homes must rely on escrow companies and title companies to conduct research into the history of a property, and to prove that they not only have the financial wherewithal to purchase a home, but the good intentions to follow through on an offer.

Or, think about the process of using a notary public for important records – the notary public must be contacted, and then you must visit their office to have hardcopy records notarized. Blockchain technology has the potential to turn this situation on its ear by eliminating the need for these third parties. Imagine how much more streamlined the homebuying process would be without the need for escrow companies, or for title insurance.

As Harvard Business Review notes, "The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically. With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision."

Private Keys – Both private and public keys are used in the blockchain to enhance integrity and ensure authenticity. This provides protection for information that might otherwise be shared without realizing it. Because the blockchain takes any information stored within it and spreads that information around a peer-to-peer network, businesses and consumers could find that their sensitive financial, personal or health data is shared with others.

Public and private keys provide the means to allow blockchains to process this data without ever really

seeing it. MarketWatch reports, “A combination of biometric security on your device, and the blockchain principles of private keys controlled solely by the user, opens up the opportunity to ditch usernames and passwords forever. And with the most popular password still being 123456, that’s got to be a good thing. As well as that, add the potential to store identity information on the blockchain where only the user owns and controls it.”

No Central Storage of Data – Yet another benefit of blockchain technology for data security is to businesses and business owners or creators interested in pursuing affiliate relationships, or joint ventures. This is due to the lack of a central authority or storage for data within a blockchain. It has the ability to ensure complete accuracy and authenticity without any need for an arbitrator (again, the removal of third parties).

In fact, there is the potential that blockchain technology could completely remove the need for entire institutions, such as clearinghouses and settlement agents. Blockchain promises to reduce business operating costs, increase transparency and trust, and improve the speed with which records and data can be verified, as well as the protection provided to data stored within the blockchain.

Dramatic Improvements for Privacy on the Part of Consumers – Today, consumer information is shared far and wide by companies. Almost any information can be purchased today, with a few exceptions that are regulated by federal law, and even that information can often be found through dark web sources. Blockchain promises to usher in a new age of privacy for consumers.

It all comes down to the use of private keys. With their private key, a consumer could authorize the sharing of specific information with specific companies. For instance, they could share the fact that they were in the market for furniture to welcome their new baby home, or they could share that they were in the market for a new car. They key here is that the consumer is in control of the data that’s shared, allowing only the information they want to go to companies, and maintaining privacy for the rest of their data.

Another way that blockchain can help enhance the privacy of consumer data is through smart contracts. These are essentially small programs designed to execute specific steps, such as verifying information, or enforcing contract-specific terms. They essentially take the place of third parties that would otherwise be entrusted with consumer information for verification or authentication purposes.

Greater Control Over Personal Information – Consumers today have information scattered all over the World Wide Web, as well as in the private ledgers of companies large and small. By and large, they have

little to no control over how that information is used, although the EU has taken a first step toward providing greater control over consumer information with its new data protection laws. Blockchain technology provides consumers with dramatic improvements in terms of privacy and control over their own data.

As VentureBeat reported in 2017, “This is where blockchain and distributed ledgers promise consumers real value. Blockchain’s architecture enables user data to be siloed from the server applications that use it ... The key idea behind blockchain applications should be to shift the Internet from application-centric models to structures where users are at the center, maintain control of their digital footprint, and can decide who will access it.”

Blockchain technology offers a host of important benefits and advantages, both for consumers and for businesses. From cost cutting to process streamlining to ensuring greater control and protection of invaluable data, blockchain delivers significant rewards. However, there are challenges ahead.

Not All Blockchains Are Created Equal

While blockchain technology promises significant control and incredible protection, not all blockchains are created equal. Today, there are both public and private blockchains, and they do not operate in the same ways. This can lead to reduced protection for data stored on an incorrect blockchain.

In late 2017, IBM noted that the most obvious difference between public and private blockchains is that public blockchains utilize computers connected to the greater World Wide Web without any filtration in between. Private blockchains, on the other hand, generally connect to inhouse intranets, which may or may not be connected to the public Web at some point. Why does this matter?

Simply put, any blockchain attached directly to the public Internet will allow any computer to become part of the network. There is no vetting process in place. Private blockchains usually only allow organizations that are known to the other members of the blockchain to join. This creates a private network in which only known, trusted actors record, store, and access data.

Harvard Business Review further delves into the topic. Speaking of blockchain’s decentralized nature specific to cryptocurrency, author Allison Berke writes, “This decentralization and relative freedom of access has led to some unanticipated consequences: Because anyone can read and write transactions,

bitcoin transactions have fueled black market trading.

Because the consensus protocol is energy consuming, the majority of users operate in countries with cheap electricity, leading to network centralization and the possibility of collusion, and making the network vulnerable to changes in policy on electricity subsidies. Both of these trends have led to an increased interest in private blockchains, which could ultimately give businesses a greater degree of control."

Ultimately, network architecture and conscious design are vital considerations for blockchains, large or small, public or private. Internodal communication is required to achieve consensus, to read, write and access information, and to approve transactions that will be recorded in the blockchain, which means care must be exercised as to which computers are allowed to communicate in the network in the first place.

Private blockchains are currently the only options in which that degree of control is possible. In the future, it may be possible to create public blockchains that lack the security concerns noted above, such as the network being subject to changing policies within the energy sector, or the consolidation of blockchain users in nations where energy is cheap. However, until that time, private blockchains remain the most secure option for businesses and consumers seeking to protect their data.

Source:

https://www.theguardian.com/commentisfree/2018/mar/21/blockchain-privacy-data-protection-cambridge-analytica

https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

https://www.marketwatch.com/story/how-blockchain-can-protect-our-personal-data-from-hackers-2018-01-03

https://medium.com/@Elysian_Ely/how-blockchain-can-protect-data-22f20e3e5c8b

https://www.acronis.com/en-us/articles/data-protection/

https://www.techrepublic.com/article/how-blockchain-encryption-works-its-all-about-math/

https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

https://www.cio.com/article/3055847/security/what-is-blockchain-and-how-does-it-work.html

https://blog.varonis.com/cybersecurity-statistics/

https://www.cpomagazine.com/2018/07/09/cybersecurity-in-2018-what-you-need-to-know/

https://themarketmogul.com/blockchain-future-data-security/

https://bravenewcoin.com/news/timestamping-on-the-blockchain/

https://community.blockcerts.org/t/blockchain-benefits-over-traditional-pki-techniques/17

https://hbr.org/2017/01/the-truth-about-blockchain

https://venturebeat.com/2017/09/09/how-blockchain-will-finally-convert-you-control-over-your-own-data/

About the Data Science Foundation

The Data Science Foundation is a professional body representing the interests of the Data Science Industry. Its membership consists of suppliers who offer a range of big data analytical and technical services and companies and individuals with an interest in the commercial advantages that can be gained from big data. The organisation aims to raise the profile of this developing industry, to educate people about the benefits of knowledge based decision making and to encourage firms to start using big data techniques.

Contact Data Science Foundation

Email:contact@datascience.foundation
Telephone: 0161 926 3641
Atlantic Business Centre
Atlantic Street
Altrincham
WA14 5NQ
web: www.datascience.foundation