BlockChain Proposal: A Secure Decentralised Credential Management Solution

Jonathon Taaffe

Post Graduate Diploma in CyberSecurity

National College of Ireland

PUBLICATION COPYRIGHT

BlockChain Proposal: A Secure Decentralised Credential Management Solution

I. Abstract

The creation and maintenance of digital username and password credentials are ubiquitous in our daily digital lives. To gain access to digital services, users must recall exact username and password combinations. Digital Service Providers are then tasked with managing these credential stores, often unsuccessfully.

Since the inception of digital credentials, the 3 core pillars of Information Security; Confidentiality, Integrity and Availability have been repeatedly breached either through human error or malicious activity.

Digital encryption technologies can securely store credentials but due to the volume of credentials to be managed, users have resorted to simplifying their passwords and then reusing these simplified passwords. Digital Service Providers, in an attempt to secure access to their content and services, have deployed disparate, disconnected credential management systems which, in themselves, provide single points to attack and hack.

This paper focusses on BlockChain technology characteristics and if those characteristics could be employed to ease user credential management burden in a secure distributed manner.

Table of Contents

II. Research Problem Background

The creation and maintenance of digital username and password credentials are ubiquitous in our daily digital lives. To gain access to digital services, users must recall exact username and password combinations. Digital Service Providers are then tasked with managing these credential stores, often unsuccessfully. Since the inception of digital credentials, the 3 core pillars of Information Security; Confidentiality, Integrity and Availability (ForcePoint.com, 2019) have been repeatedly breached either through human error or malicious activity. Digital credentials have created the following critical Cyber Security issues:

A. Password Simplification

Memorising and recalling numerous username and password combinations has led users to simplify their passwords, clearly demonstrated in online password lists (HaveIbeenPwned.com, 2019). The top 3 most used passwords from 2017 and 2019 are '123456', 'password' and '12345678' (Wikipedia.org, 2019c). These simplified passwords are employed by a considerable number of users, simplifying the job of the hacker. More worryingly, according to Verizon's Data Breach Investigations Report (DBIR) from 2017, *"81% of hacking-related breaches leveraged either stolen and/or weak passwords"* (Verizon, 2017).

B. Password Reuse

In addition to simplification, users frequently reuse the same or similar passwords. In an Empirical Analysis of User Passwords across Online Services, it was found that *"password reuse was observed in 52% of users"* (Wang et al., 2018). With one valid reused password identified, a hacker has uninhibited access to additional online services.

C. Centralised Password Storage

Digital Service Providers centrally store user credentials on behalf of users, creating a centralised single point of attack. Attacks on centralised credential stores have, in the first 6 months of 2019, led to the exposure of 4.1 billion records (Winder, 2019). Analysis of these figures shows that no sector or industry is immune, from 885 Million Banking records, to 550 Million Social Media records, to 25 Million Healthcare records in 2019 alone (CyberWarZone.com, 2019).

III. Research Question

In today's alarmingly insecure cyber environment, what characteristics of BlockChain technology could be employed to simplify credential management, advance credential security, decentralise and distribute credential management stores, and eliminate username and password authentication mechanisms?

IV. Literature Review

Encryption is the process of encoding data making it unintelligible, guaranteeing Data Confidentiality (Wikipedia.org, 2019b). Decryption is the reverse process of decoding encrypted data making it intelligible, guaranteeing Integrity (Techopedia.com, 2019).

A BlockChain is a distributed chain of encrypted data blocks, into which any digital data can be securely stored (Markelevich, 2018). Fundamentally BlockChain is a secure distributed encryption, decryption mechanism.

A. Secure Hashing Algorithm

BlockChain employs two encryption processes; the first is Hashing which takes input of any length of characters and generates a unique fixed length random 256-bit alpha numeric output, or digest (Beal, 2019). The hashed output of a preceding data block is incorporated in the hashing process of the proceeding data block. This process requires the availability of all previously hashed data blocks in the chain to decode any one data block, guaranteeing Integrity, Confidentiality and Non-Repudiation (Cryptomathic.com, 2019).

The hashing algorithm BlockChain uses is Secure Hashing Algorithm 256 (SHA-256) (Asolo, 2018). Hashing is a 1-way process; you cannot retrieve or recover the original input from a hash digest, therefore providing data Integrity. The exact same character input will always generate the same hash digest, making hashing deterministic. SHA256 can generate up to 2^256 unique hashing digests; there is a 1 in over 115 quattuorvigintillion, i.e. 78 digit number, (LearnCryptography.com, 2019b) possibility of a collision (LearnCryptography.com, 2019a).

B. Asymmetric Public-Private Key Encryption

BlockChain also employs Asymmetric Public-Private Key Encryption to encrypt data blocks using two encryption keys; a unique public key and a unique private key, both of which are bound to the same data block (Cryptography.io, 2019).

The unique public encryption key is used to encrypt data and the unique private encryption key is used to decrypt data (Li, 2014). The encryption key is public so that anyone can encrypt data using the public key. But the decryption key is private so only the intended recipient can decrypt the data. In a BlockChain scenario, a public encryption key is associated with a block of encrypted data in the chain. The owner of that data block maintains the private decryption key. For the data block owner to access the data block contents, the data block owner uses both the public encryption key with their private decryption key.

The asymmetric encryption process also generates a unique public key certificate which publicly confirms ownership of the data block. A private key certificate is also generated and is securely stored by the block data owner. The private key certificate is not publicly available and is required, in combination with the public key certificate, to gain access to the data in the specific block. This encryption process provides Authentication, Validation and Transactional Trust in a distributed BlockChain.

C. Decentralised Public Key Infrastructure

A key functional component of a conventional Public Key Infrastructure (PKI) (Fruhlinger, 2019) facilitating asymmetric public-private key encryption is a centralised Certificate Authority (CA) (Globalsign.com, 2019). A CA is a third-party entity that issues digital certificates and centrally manages public keys and credentials to facilitate asymmetric encryption. Vital to a functioning PKI is the level of trust a CA maintains; certificate authenticity is the foundation of PKI. Unfortunately CA's are not immune to hacks as illustrated by the Comodo (McCullagh, 2011), DigiNotar (Higgins, 2011) and NIC.br (Greenberg, 2017) CA hacks. Even though these breaches occurred in 2011 and 2017 respectively, it sets a precedent. For conventional CA's to operate they

must be centralised which provides a single point of attack. This centralisation also provides an end-point against which Man-in-the-Middle (Wilton, 2019) attacks can be launched.

Enter Decentralised Public Key Infrastructure (DPKI). As cited in 'Decentralized Public Key Infrastructure, A White Paper from Rebooting the Web of Trust' (Allen et al., 2015) the authors introduce the concept of a DPKI which *"returns control of online identities to the entities they belong to...", "makes permissionless bootstrapping of online identities possible and provides for the simple creation of stronger SSL certificates"* (Allen et al., 2015).

For DPKI to function in a secure decentralised distributed manner it utilises BlockChain technology. With BlockChain providing the decentralised distributed secure platform, DPKI is not centrally managed by any third parties eliminating a central point of attack, and, due to its secure, distributed, peer-to-peer infrastructure, is not vulnerable to Man-in-the-Middle attacks.

DPKI further enhances the Authentication, Validation and Transactional Trust in and of a distributed BlockChain.

D. Peer-to-Peer Distributed Ledger Platform

BlockChain uses a Peer-to-Peer Distributed Ledger Platform to securely distribute encrypted data blocks between participating nodes, i.e. computers(Voshmgir, 2019). Every node participating in the BlockChain is a peer or equal, each storing an exact copy of the same ledger or data blocks. There is no single centralised authority or database maintaining the BlockChain as each node participating in the BlockChain maintains the BlockChain. This distributed platform eliminates the need for a centralised credential store removing any single point to attack and hack and, the more nodes that join the BlockChain, the greater the BlockChains availability. This distributed multi-peer-node platform guarantees Availability.

E. The Emergence of the BlockChain Platform

So far this literature review has introduced the core components of a BlockChain, how those components function and the functional requirements they provide to a decentralised credential management system. BlockChain technology has been evolving and developing over the past number of years but the concept was only initially presented in Satoshi Nakamoto's seminal 2008 whitepaper 'Bitcoin: A Peer to Peer Electronic Cash System' (Nakamoto, 2008). Nakamoto's whitepaper proposed a 'peer-to-peer electronic cash system' titled Bitcoin (Bitcoin.org, 2019). Nakamoto's white paper focusses on the functional aspects of the Bitcoin cryptocurrency and provides little detail of the underlying secure decentralised platform required for Bitcoin to function. To facilitate the public offering of Bitcoin in 2009 (Bitcoinwiki.org, 2019), Bitcoin.org developed the first public BlockChain platform. To many observers Bitcoin and BlockChain were considered synonymous; one in the same.

In 2014, that perception changed with the publication of the whitepaper 'A Next Generation Smart Contract & Decentralized Application Platform' by Vitalik Buterin (Buterin, 2014). In his whitepaper, Buterin introduces the concept of a BlockChain to clearly identify the core decentralised platform on which Bitcoin functions. With this clear separation of service function from platform infrastructure, the BlockChain platform was defined.

As Sally Davies, Financial Times Technology Reporter, explains in 'How bitcoin and its blockchain work', *"blockchain is to bitcoin what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one."* (Davies, 2015).

F. BlockChain Platforms Today

Since the initial inception of BlockChain, the platform has evolved into 2 distinct BlockChains offerings; Public Permissionless and Private Permissioned (Sharma, 2019). A Public Permissionless BlockChain is public; anyone can join and participate, and it

is permissionless; no permission or pre-approval is required to join and participate. Examples include Bitcoin (Bitcoin.com, 2019), Litecoin (Litecoin.com, 2019) and Ethereum (Ethereum.org, 2019). A Private Permissioned BlockChain is private; only approved users can join and participate, and it is permissioned; authorisation through a Central Authority is required. Development of this type of BlockChain has been aimed at private organisations and enterprises across a wide range of sectors from Banking to Medical to Governmental. Both MultiChain.com (MultiChain.com, 2019) and R3.com (R3.com, 2019) provide Enterprise-class BlockChains, with companies like Accenture (Accenture.com, 2019) and IBM (IBM.com, 2019) providing BlockChain solutions for the Financial sector.

V. JUSTIFICATION

Credential management is a manual tedious process requiring users to create and then memorise complex username and password combinations. Due to the volume of credentials, users employ password simplification and reuse strategies. Digital service providers then centrally store these simplified credentials making them a single point of hack. The motivation behind this research is to simplify the credential management process and to ensure credential data is securely available in a distributed manner.

Confidentiality – Encrypted BlockChain Blocks

BlockChain is simply a chain of data blocks, each block secured with the cryptographic hashing output of the previous block in the chain. Blocks can contain any data, including credentials, and, combining the hashed output of the previous block with the next block, generates a new hash output which is unique to that block. This is the fundamental security principle of BlockChain.

The Genesis block, the first block in a BlockChain, is seeded with a random number to represent a hashed output. This block is passed through a cryptographically secure SHA256 hashing algorithm to generate a unique hash digest. This hash digest is incorporated into the second block in the BlockChain, and the second block is then passed through a secure SHA256 hashing algorithm to generate a new unique hash digest. The hash digest from the second block is incorporated into the third block in the BlockChain which is also passed through a SHA256 algorithm to generate a third unique hashing digest.
This hashing, incorporation and hashing processes is repeated for each and every block in the BlockChain.

Integrity - Secure Cryptographic Hashing Function (SHA-256)
BlockChain uses the cryptographic algorithm Secure Hashing Algorithm 256 (SHA-256). A hashing algorithm takes an input of any length of characters and generates a fixed length random 256-bit alpha numeric output or digest. This process is a 1-way process; you cannot retrieve or recover the original input from a hash digest. The exact same character input will always generate the same hash digest, making hashing deterministic. SHA256 can generate up to 2^256 unique hashing digests; there is a 1 in over 115 quattuorvigintillion, i.e. 78 digit number, (LearnCryptography.com, 2019b) possibility of a collision (LearnCryptography.com, 2019a).

Availability - Distributed Peer-to-Peer Platform: BlockChain is a Peer-to-Peer distributed platform where all nodes (PC's, Smartphones, etc.) participating in the chain, store a copy of the chain. This distributed peer-to-peer platform should ensure:

- No single point of failure or attack.
- The BlockChain is always available as long as 2 or more nodes are online.
- The more nodes that join the chain, the higher the chains availability.

VI. Proposed Approach

Combining the understanding of BlockChain functional components from Section II. Literature Review, with the key functional component requirements defined in Section III. Research Question, the following details the proposed approach for a solution implementation.

A. Hashing

As a core component of a BlockChain and, consequently, a core component of the proposal, the hashing function must be capable of receiving variable size inputs, produce fixed length alpha-numeric string message digests (outputs), be easy and efficient to compute, pseudorandomly and uniformly distribute values across a table, be one-way pre-image resistant and weak collision resistant minimising hashing output collisions. To meet these requirements and to ensure the hashing function is future proof, Secure Hashing Algorithm 3 (SHA-3) is preferred over SHA-2. SHA-3 is computationally collision free from both a conventional X86 Central Processing Unit perspective and from a quantum computing perspective.

Chosen Technology: Secure Hashing Algorithm 3 (SHA3-256).

B. Public Key, Private Key Encryption

With a Public Key, Private Key cryptographic requirement to ensure Authenticity, Authentication, Integrity and Non-Repudiation of credential data in blocks, the chosen encryption scheme must provide a robust Key Generation Algorithm, a Signing Algorithm for signature generation and a Signature Verification Algorithm to confirm signature authenticity. Elliptic Curve Digital Signature Algorithm (ECDSA) (Wikipedia.org, 2019a) provides key generation, signature generation and signature verification for private and public keys. As ECDSA is based on algebraic functions over elliptical curve mathematics where a specific mathematical equation is satisfied by a set of points on an elliptical curve, it is today's most secure key-based algorithm. ECDSA utilises a Point Multiplication Trapdoor Function (Engineering, 2014), a mathematical operation which is computationally undemanding to perform a forward function on, but computationally expensive or infeasible to perform a reverse function on. ECDSA generates smaller signature and key sizes comparative to other Digital Signature Algorithms (DSA) requiring less network bandwidth and less device storage and is computationally faster for large key signature generation enhancing the security level of the generated keys.

In addition to key and signature generation and verification, a process of secure key exchange is also required. Key exchange is a method of securely exchanging keys over an untrusted public network. The Diffie-Hellman Key Exchange mechanism (Baker, 1999) is today's secure standard for key exchange. With Diffie-Hellman key exchange a secret number is shared between two parties. This shared secret then allows for the secure exchange of asymmetric keys. This mechanism uses the modulus of integers to generate a shared secret. This process provides encryption, forward secrecy, password authenticated key agreement and facilitates public key infrastructure

Chosen Technology: Elliptic Curve Digital Signature Algorithm (ECDSA) with Diffie-Hellman Key Exchange.

C. Decentralised Public Key Infrastructure (DPKI)

Ensuring the data blocks in a decentralised credential management solution are securely distributed across a network is a foundational component. A DPKI solution must ensure each participant is in complete control of their identifier and only the participant can modify their own identifier. The DPKI solution must also provide for all-or-nothing processing where every participant witnesses every other participants' identifier updates, or no one observes any updates invalidating all updates. The

DPKI must allow Permissionless Writes where participants do not require permission to write or update their identifier and employ a robust consensus protocol which ensures no single entity or participant can take control of the DPKI which fosters trust between the participating nodes and individuals.

The consensus protocol must be computationally expensive and incrementally build on previous output verifying work previously computed.

Chosen Technology: Proof-of-Work (POW).

D. Peer-to-Peer Distributed Ledger

A Peer-to-Peer Distributed Ledger should provide for secure distribution where an exact copy of the ledger (data blocks) is maintained on each participating node, trusted consensus where all nodes use a consensus protocol to confirm ledger validity, verification where nodes verify the ledgers integrity; any unverified changes are discarded, transparency where nodes publish their ledger verifications to all participating nodes, trust through node transparent verification enforcing node-to-node trust, secure data storage employing sequential time stamped blocks with secure cryptographic hashing functions.

Chosen Technology: Ethereum.

VII. BIBLIOGRAPHY

Accenture.com. (2019). *Blockchain Financial Services Infrastructure*. Accenture.Com.

Allen, C., Brock, A., Buterin, V., Callas, J., Lundkvist, C., Kravchenko, P., Nelson, J., Reed, D., & Slepak, G. (2015). *Decentralized Public Key Infrastructure*. http://www.weboftrust.info/downloads/dpki.pdf

Asolo, B. (2018). *What Is SHA-256 And How Is It Related to Bitcoin ?* Mycryptopedia.Com. https://www.mycryptopedia.com/sha-256-related-bitcoin/

Baker, K. A. (1999). *Diffie-Hellman key exchange*. Math.Ucla.Edu.

Beal, V. (2019). *Hashing*. Webopedia.Com. https://www.webopedia.com/TERM/H/hashing.html

Bitcoin.com. (2019). *Bitcoin.com*. Bitcoin.Com. https://www.bitcoin.com/

Bitcoin.org. (2019). *Bitcoin.org*. Bitcoin.Org. https://bitcoin.org/

Bitcoinwiki.org. (2019). *Bitcoin History*. Bitcoinwiki.Org. https://en.bitcoinwiki.org/wiki/Bitcoin_history#Bitcoin_in_2008

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. In *Etherum* (Issue January). https://github.com/ethereum/wiki/wiki/White-Paper

Cryptography.io. (2019). *Asymmetric algorithms*. Cryptography.Io. https://cryptography.io/en/latest/hazmat/primitives/asymmetric/

Cryptomathic.com. (2019). *What is non-repudiation?* Cryptomathic.Com. https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation

CyberWarZone.com. (2019). *2019 Top 12 Worst Data Breaches, So far*. CyberWarZone.Com. https://cyberwarzone.com/2019-top-12-worst-data-breaches-so-far/

Davies, S. (2015). How bitcoin and its blockchain work. *Financial Times*. https://www.ft.com/video/2be94381-66dc-3320-a292-6a1cde0a3d5f

Engineering, E. (2014). *The importance of trapdoor functions*. EvaluationeEgineering.Com. https://www.evaluationengineering.com/instrumentation/article/13010746/the-importance-of-trapdoor-functions

Ethereum.org. (2019). *Ethereum is a global, open-source platform for decentralized applications*. Ethereum.Org.

ForcePoint.com. (2019). *What is the CIA Triad?* ForcePoint.Com. https://www.forcepoint.com/cyber-edu/cia-triad

Fruhlinger, J. (2019). *What is PKI? And how it secures just about everything online*. CSOOnline.Com. https://www.csoonline.com/article/3400836/what-is-pki-and-how-it-secures-just-about-everything-online.html

Globalsign.com. (2019). *Certificate Authorities & Trust Hierarchies*. Globalsign.Com. https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/

Greenberg, A. (2017). *How Hackers Hijacked a Bank's Entire Online Operation*. Wired.Com. https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/

HaveIbeenPwned.com. (2019). *Pwned Password*. HaveIbeenPwned.Com. https://haveibeenpwned.com/Passwords

Higgins, K. J. (2011). *Digital Certificate Authority Hacked, Dozens Of Phony Digital Certificates Issued*. DarkReading.Com.

IBM.com. (2019). *IBM Banking and Financial Markets*. IBM.Com. https://www.ibm.com/blogs/blockchain/category/blockchain-in-financial-services/banking-and-financial-markets/

LearnCryptography.com. (2019a). *Hash Collision Attack*. LearnCryptography.Com2. https://learncryptography.com/hash-functions/hash-collision-attack

LearnCryptography.com. (2019b). *Why Is 2^256 Secure?* LearnCryptography.Com. https://learncryptography.com/cryptanalysis/why-is-2-256-secure

Li, N. (2014). *Asymmetric Encryption*. Encyclopedia of Database Systems. https://doi.org/10.1007/978-1-4899-7993-3_1485-2

Litecoin.com. (2019). *Litecoin.com*. L2itecoin.Com. https://litecoin.com/

Markelevich, A. (2018). *What is Blockchain Technology*. Accounting Education News. https://doi.org/10.1227/01.NEU.0000210001.75597.81

McCullagh, D. (2011). *FBI probes Comodo Web security breach*. Cnet.Com. https://www.cnet.com/news/fbi-probes-comodo-web-security-breach/

MultiChain.com. (2019). *MultiChain.com*. MultiChain.Com. https://www.multichain.com/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. In *SSRN Electronic Journal*. https://bitcoin.org/bitcoin.pdf

R3.com. (2019). *R3.com*. R3.Com.

Sharma, T. K. (2019). *Permissioned and Permissionless BlockChains: A Comprehensive Guide*. BlockChain-Council.Org. https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/

Techopedia.com. (2019). *Definition - What does Decryption mean?* Techopedia.Com. https://www.techopedia.com/definition/1773/decryption

Verizon. (2017). *2017 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

Voshmgir, S. (2019). *Blockchains & Distributed Ledger Technologies*. BlockChainHub.Net. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

Wang, C., Jan, S. T. K., Hu, H., Bossart, D., & Wang, G. (2018). The next domino to fall: Empirical analysis of user passwords across online services. *CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy*, *2018-Janua*, 196–203. https://doi.org/10.1145/3176258.3176332

Wikipedia.org. (2019a). *Elliptic Curve Digital Signature Algorithm*. Wikipedia.Org.

Wikipedia.org. (2019b). *Encryption*. Wikipedia.Org. https://en.wikipedia.org/wiki/Encryption

Wikipedia.org. (2019c). *List of the most common passwords*. Wikipedia.Org. https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Wilton, R. (2019). *What Is a Man in the Middle (MITM) Attack?* InternetSociety.Org. https://www.internetsociety.org/blog/2019/11/what-is-a-man-in-the-middle-mitm-attack/

Winder, D. (2019). *Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019*. Forbes.Com. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/