**Blockchain Technology for Information Technology Risk Management**

1. Introduction
2. Industry Papers and Reports on IT Risk Management & Blockchain
   1. KPMG International Cooperative Report

“HOW WILL BLOCKCHAIN IMPACT AN INFORMATION RISK MANAGEMENT APPROACH” <https://www.compact.nl/en/articles/how-will-blockchain-impact-an-information-risk-management-approach/>

This article focuses on the risks introduced by the implementation of blockchain technology in the IT environments and proposes possible solutions. One of the major additional risks introduced is Scalability. Another threat is centralization caused by ownership of majority nodes by a single entity. Compatibility issues cause interoperability between different technological generations. Incorrectly designed smart contracts and flawed consensus protocol add to the list of several other threats. It is to be noted that these risks relate to the absence of a trusted third party. The article studies the key risks to the Libra cryptocurrency (Facebook). The author has stressed on the importance of governance model for risk management using Tradelens (by IBM and Maersk) as an example. Solutions to risks of data management and centralization are proposed. The article concludes by the remark that the shift towards distributed ledger technology results in a shift towards distributed control environments as well.

* 1. Vikash Kumar on YOURSTORY

“HOW BLOCKCHAIN CAN MAKE DATA SECURE FOR COMPANIES”

<https://yourstory.com/2018/12/blockchain-make-data-secure-companies>

This article focuses on Blockchain solutions for data security while handling big data. Blockchain can be applied to any industry which has to deal with data. E-commerce companies have started to store small amounts of transaction data on blockchain to understand its interactions with producers and consumers. The article explains the innovative blockchain solutions being implemented in Estonia. Keyless Signature Infrastructure (KSI) is assumed to be used in Estonia to store public data to ensure data security. Key terms like Golem, Path, Skyry and Dapp builder have been explained. Blockchain technology is proved to be a powerful tool for big data analytics as it makes identification of malware, detection of patterns, compilation and verification of data more efficient.

* 1. COINACCORD report

“BLOCKCHAIN AND INFORMATION TECHNOLOGY: AN INDUSTRY ANALYSIS”

<https://raw.githubusercontent.com/coinaccord/resources/master/reports/blockchain-in-information-technology.pdf>

The report begins by briefing on each of the issues faced in Information Technology today such as data disconnects between companies due to centralization, single point of failure, difficulties in real-time data sharing, high infrastructure costs and data-tampering. Companies need to follow several regulations due to which it may become cumbersome to maintain proper business processes. Blockchain and cryptocurrencies are leading to a shift in business models where users maintain an ownership of their data. Benefits of blockchain have been discussed. Customization is a benefit of Blockchain technology due to which companies can build their own solutions or utilize the already existing architectures such as Stellar, Hyperledger and Ethereum. Trustless environment and increased data security are some other important benefits. The article further progresses to discuss the use cases of Blockchain. Multi-signature authentication and signed transactions facilitate user authentication. The article suggests Data Anchoring, Sharding and User Controlled Data as solutions to data security risks. Recently, Subscription as a Service (SaaS) model on the blockchain has been proposed, which comes with benefits for users as well as organizations. As monetization comes into play with Blockchain, there is an incentive to develop mesh networks allowing for a better internet experience with less down time and a robust infrastructure. Tokenization and DAOs are other important use cases of Blockchain Technology. Lastly, the article concludes by summarizing IT risks, their solutions and Blockchain use cases in a tabular form.

* 1. CHAINKIT Services

“INTRODUCTION TO DATA ANCHORING”

<https://chainkit.com/data-anchoring>

Blockchain technology is a promising solution when it comes to Data Security risks. However, it is inefficient to store large files and databases on the blockchain. This article proposes Data Anchoring to overcome this inefficiency. Rather than storing a full digital asset on the chain, a unique hash for that digital asset is stored on the chain, along with some method of identifying the asset you are trying to protect. This method does not prevent data-tampering but it provides a powerful tamper-detection as well as asset authentication mechanism. Data anchoring along with frequent recovery points via snapshots, mirrors, backups & archives increases the levels of system integrity in an IT environment. In centralized RBAC administrative authority model, invisible data-tampering is possible. Blockchain presents a decentralized solution to data security wherein data-tampering can be detected in minutes.

* 1. BUILTIN article by Sam Daley

“WALLETS, HOSPITALS AND THE CHINESE MILITARY: 19 EXAMPLES OF BLOCKCHAIN CYBERSECURITY AT WORK”

<https://builtin.com/blockchain/blockchain-cybersecurity-uses>

This article provides information about the latest progresses in Blockchain solutions for Cybersecurity throughout six major industries – Cryptocurrencies, Traditional Banking, Healthcare, Government, Defense and Internet of Things. Mobilecoin, Javvy, Coinbase and Founders bank use blockchain as a cybersecurity protocol in cryptocurrency trading. The traditional Wall Street banks like Santander, JPMorgan and Barclays are the early adopters of Decentralized Ledger Technology for cybersecurity issues.  JPMorgan has developed an enterprise-focused version of Ethereum called Quorum, which uses blockchain technology to process private transactions. Barclays recently registered two Blockchain patents, one for Secure Digital Data Operations and another for a Data Validation and Storage system.  Healthcare experiences [twice the amount of cyber](https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html) attacks of any other industry as patient data is sold at high values in the black market. Hashed health, Philips healthcare and Health Linkages are the pioneers in implementing blockchain solutions in the Healthcare industry. Currently, many government agencies fail to meet basic encryption goals and very few have the capability to detect large data compromises. The Governments of The State of Colorado, Australia and Malta are the world leaders in governmental blockchain implementation. Coming to defense, according to Accenture, [86% of defense companies plan to implement blockchain](https://coincentral.com/defense-industry-technology/) in the cybersecurity protocols within the next three years. The U.S. and Chinese militaries are actively looking into Blockchain technology for its use in encryption and secure data transfer. Lockheed Martin is involved in the research to use blockchain to secure its weapon development systems. Moving on to IoT, the companies HDAC, CISCO and Filament are taking the lead in combining Blockchain technology with IoT devices. Blockchain technology is rapidly establishing itself in the cybersecurity industry.

* 1. Deloitte article on DDoS prevention by Blockchain Technology

“PREVENTION OF DDOS ATTACKS WITH BLOCKCHAIN TECHNOLOGY”

<https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/cyber-security-prevention-of-ddos-attacks-with-blockchain-technology.html>

The article discusses the use of Blockchain technology as a solution to prevent Distributed Denial of Service (DDoS) attacks. IoT devices have a weak security configuration due to which they can be easily hacked and made a part of the botnet to launch DDoS attack. The centralized client/server model of the Internet causes the entire system to fail due to the failure of a single server thus facilitating DDoS attacks. A Blockchain solution will replace login credentials with public key cryptography making it difficult to scan and compromise devices. User’s private key will become necessary to communicate with other devices. By limiting the authority to install firmware to the manufacturer using his private key, the chances of installation of malware would become almost none. Storing public keys on the Blockchain will help IoT devices to authenticate login requests. Blockchain can thus establish a secure P2P network wherein the attacker will not be able to publish DDoS attack launch instructions. In addition, there are other ways to use blockchain to prevent DDoS attacks. Companies like Blockstack, Namecoin, Nebulis are working towards building a decentralized DNS system. Another way is to re-engineer the entire structure of the internet to make it a decentralized model. A blockchain may itself be a victim of DDoS Sybil attack, but already there exist solutions to prevent direct DDoS risks for blockchain.

[7] Marknet\_cloud\_computing

“WILL BLOCKCHAIN DISRUPT CLOUD 2.0?”

<https://www.mark-network.com/will-blockchain-disrupt-cloud-2-0/>

It is predicted that by 2025, the amount of data worldwide will be nearly 175 zettabytes. According to experts, 49% of data created will be stored in public cloud environments by 2025. Cloud computing is faced with many challenges related to cloud security, governance, compliance, migration, licensing and multiple cloud management. Blockchain is a promising technology which can solve these issues and reinvent the cloud. Blockchain enhances the security of cloud storage solutions with decentralization and cryptographic multi-layer encryption of data. User anonymity and economic incentives mechanism are enabled by blockchain. The world’s largest computing company, Avogadro Corporation has embraced blockchain-based cloud computing platform. The giants like Google Cloud, AWS, Alibaba, IBM and more hold majority of cloud computing making it heavily centralized. Adopting blockchain technology transfers the data back to the users even though there is centralization due to cloud computing service providers. Ankr, Transcodium and Dfinity are the recent projects that combine blockchain and cloud computing. Projects such as Oasis Labs are working towards a privacy-first version of cloud using blockchain. Projects like BonusCLoud and Sia are the examples of how blockchain solutions can prevent inflation of costs of services.

1. Academic Papers on IT Risk Management & Blockchain
   1. Thesis by Mari Thomas, Stellenbosch University, South Africa

“BLOCKCHAIN TECHNOLOGY: ADDRESSING THE RISK OF DIGITAL ASSETS EXCHANGE”

<https://scholar.sun.ac.za/handle/10019.1/103531>

This study intends to identify the most significant, ingrained risks posed to transactions in a digital environment and to understand how some specific characteristics of blockchain technology could potentially address those risks. Currently, the major risks with the exchange of digital assets are identified to be Lack of Trust, Double-spending, Repudiation and Theft (including fraud). In order to provide blockchain solutions, the author has first carefully studied the blockchain transaction process by splitting it into six stages. This has been further explained using the Bitcoin application as an example. The research focuses on how the characteristics of blockchain technology such as Peer-to-Peer (P2P) network, Distributed ledgers, Consensus mechanism, Asymmetric cryptography, Immutability could address the identified risks. The author has put together the risks and the corresponding blockchain characteristics in a mapping which serves as a quick reference matrix for potential users. Lastly, it is to be noted that blockchain brings into play additional risks, mainly associated with requirement of resources and lack of trusted third party, which should be considered before implementation.

* 1. 2016 Yuanfeng Cai and Dan Zhu

“FRAUD DETECTIONS FOR ONLINE BUSINESSES: A PERSPECTIVE FROM BLOCKCHAIN TECHNOLOGY”

<https://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0039-4>

This study focuses on the advantages and limitations of blockchain-based reputation systems to prevent rating fraud. Rating fraud is a phenomenon in which raters create biased ratings to promote their product or demote a competitor. Blockchain technology is effective in protecting customers’ privacy, thus encouraging them to give honest feedback. Blockchain systems are effective against rating fraud in non-computational and content-driven reputation systems as verification of claims is possible. In user-driven reputation systems, there is a lack of ground truth thus making verification difficult. The author has discussed the positives and negatives of proposed solutions to prevent subjective information fraud. Blockchain-based reputation systems can be used to prevent “bad mouthing”, “whitewashing” and “sybil” attacks, but are not resistant to “ballot stuffing”, “constant” and “camouflage” attacks.

* 1. August 2018 IEEE

“A BLOCKCHAIN-BASED RISK AND INFORMATION SYSTEM CONTROL FRAMEWORK”

<https://www.researchgate.net/publication/328608471_A_Blockchain-Based_Risk_and_Information_System_Control_Framework>

This paper proposes a blockchain-based Risk and Information System Control (RISC) framework as a mechanism for sharing risk information among insiders, IoT devices and information systems. The author explains each stage of the life cycle of RISC – Risk Identification, Assessment, Response & Mitigation and Monitoring & Reporting. The research has designed three types of risk smart ledgers and the Merkel tree is used to establish relationship between them. To avoid continuous monitoring, the study designs three risk smart contracts for automatic risk calculation and approval flow control during each of the four stages of the life cycle. The paper gives a description of the system architecture and network structure of the blockchain-based RISC prototype. Through blockchain technology, it can be ensured that all IT risks are evaluated without bypassing any risks. The study covers three common blockchain-based risk alleviation responses. Blockchain technology effectively handles Backtracking, Tracking, Falsification and Multi-trust issues in the traditional RISC making RISC more efficient.

* 1. International Journal of Engineering and Advanced Technology, Oct 2019

“CYBER SECURITY THROUGH BLOCK CHAIN”

<https://www.ijeat.org/wp-content/uploads/papers/v9i1/A9836109119.pdf>

The paper does a qualitative analysis of the implementation and deployment methods of Blockchain technology in cybersecurity as proposed in 30 recent research studies reviewed by Taylor et al. (2019) . The paper explains Blockchain technology in brief and how it’s characteristics can tackle identity thefts and fraud caused by unauthorized access to data which is caused due to centralized storage. It is observed that the main focus of many researchers is application of Blockchain to improve the security of IoT devices, data and networks. IoT devices are extensively used, yet they have a weak security configuration often targeted by hackers, making them a research priority. Blockchain security solutions can aid in managing access control and data sharing for IoT devices. Blockchain, due to it’s rigid nature, can tackle the risk of single point failure to ensure data security. Networks and data privacy can also be secured by Blockchain technology. The paper suggests future researchers to work on the practicality of a single Blockchain which can be used to develop security solutions so as to avoid integration of multiple Blockchains.

* 1. Sapiens Chain

“SAPIENS CHAIN: A BLOCKCHAIN-BASED CYBERSECURITY FRAMEWORK”

<https://airccj.org/CSCP/vol8/csit89509.pdf>

This study proposes a blockchain-based security framework – Sapiens Chain. In combination with artificial intelligence, this framework makes it possible to detect vulnerabilities automatically and handle website, application and blockchain securities simultaneously. In the proposed framework, the users submit tasks through the browser, fog nodes distinguish the tasks and assign fragments of tasks to selected nodes. Finally, results are gathered into a report. The structure of the chain consists of 4 layers- resource, transport, contract and application layer, each performing specific functions. The operation mode consists of fog and ordinary nodes, scheduling and security algorithms, Reward and Claim modes as well as incentive mechanisms for encouraging node participation and punishment mechanisms to tackle node dishonesty. The experimental data confirms that Sapiens Chain framework can distinguish between websites at high and low risk levels as well as it can detect vulnerabilities and provide corresponding suggestions. Lastly, the study discusses the applications of the proposed framework such as website, application and smart contract securities and Shared Economy.

* 1. IJEAIS research paper

“USE OF BLOCKCHAIN IN STRENGTHENING CYBERSECURITY AND PROTECTING PRIVACY”

<http://ijeais.org/wp-content/uploads/2018/12/IJEAIS181209.pdf>

This study intends to emphasize on the positive impact the blockchain technology can have on the IoT environment. Many examples of data breaches have been discussed. Currently IoT devices run on a centralized cloud-based server which uses firewalls to ensure cybersecurity. However, hackers have been able to penetrate through the firewalls. As against this, blockchain technology uses cryptographic hash functions which make it almost impossible to hack the system. The study further moves on to the cybersecurity risks faced by the Healthcare industry like malwares that affect data integrity and privacy, DDoS attacks and so on. Blockchain technology is a potential solution to these risks. The research compares centralized cloud model and decentralized blockchain model for IoT. Lastly, the use cases of blockchain in supply chain management and in the promotion of Fair Information Practices (FIPs) are studied.

[7] AuthLedger research paper

“AUTHLEDGER: A NOVEL BLOCKKCHAIN-BASED DOMAIN NAME AUTHENTICATION SCHEME”

<https://www.semanticscholar.org/paper/AuthLedger%3A-A-Novel-Blockchain-based-Domain-Name-Guan-Garba/9c4607f78cf1490421fd768b410d715aa8836646>

The study proposes a domain authentication system based on blockchain technology known as AuthLedger. The drawbacks of current systems have been discussed in detail. The current Public Key Infrastructure (PKI) authentication is mainly dependent on Certificate Authorities (CA) which have to be trusted by domain owners as well as operators. There is a disparity of rights between users and CAs. Methods such as Domain Name System Security Extensions (DNSSEC) and Certificate Authority Authorizations (CAA) are trust-based and are prone to single point of failure. The study sets up the threat model describing various malicious adversaries and their capabilities. The AuthLedger consists of five entities – CA, Domain Name Server (DNS), Browser Extention, Validating Authority, Blockchain. The domain authentication procedures are based on time and count and are described in detail. Rules have been formulated to prevent misbehavior of validator nodes as well as clients which also include incentives to promote node honesty and attract more nodes to join the system. Lastly, the research describes the implementation prototype with the help of Ethereum smart contracts and Solidity language.

1. IT risks and Possible solutions
2. **Data Security**

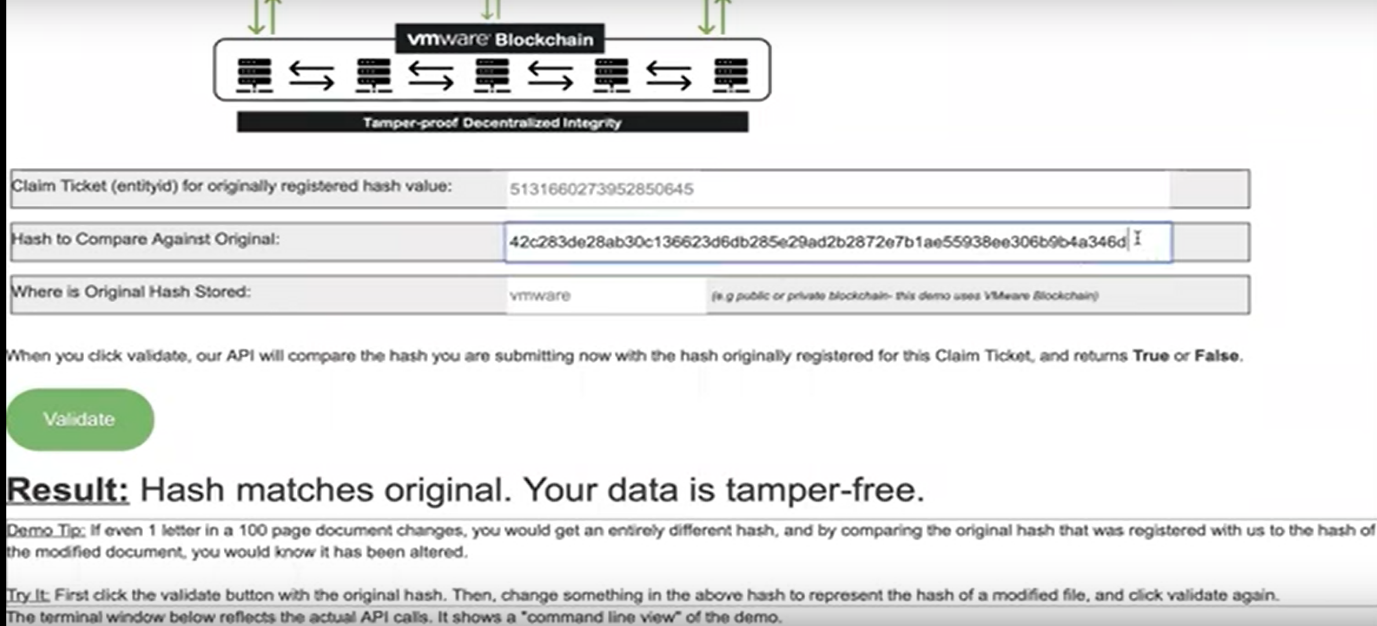
Method 1:

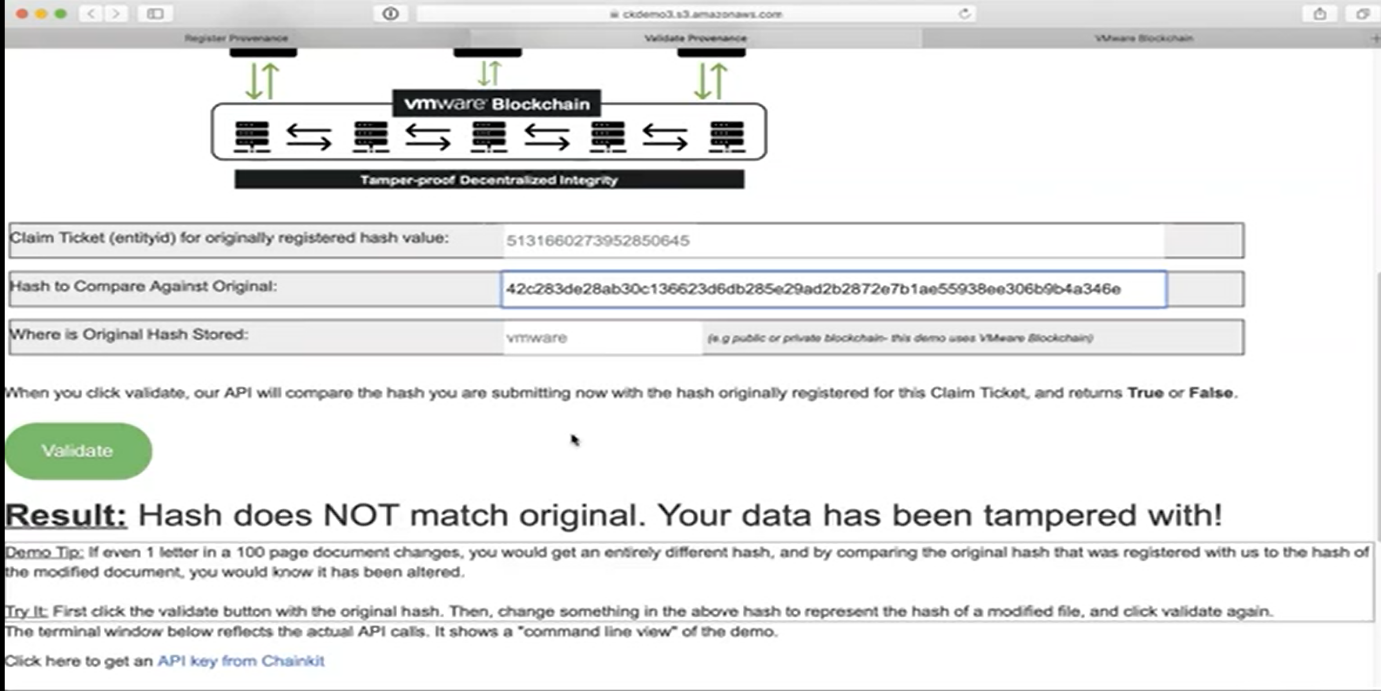
A system comprised of KSI, Golem, Path, Skyry and Dapp builder (in finance) can be used to ensure data security.

* **Keyless Signature Infrastructure (KSI)** : Uses blockchain. Stores public data securely. Monitors changes to prevent data tampering. Promotes data transparency.
* **Golem** : Decentralized supercomputer made up of the syndicate powering of user's machines ranging from PCs to entire data centres
* **Path** : Path is utilized for extra bandwidth. Path Mining Nodes installed on computers provide work insights back to Path.
* **Skyry** : Detects suspicious activity on the blockchain, eliminates synthetic identity theft
* **Dapp builder** : Used for data verification in the financial sector

Method 2: Data Anchoring

Data Anchoring allows companies to maintain off-chain database which can be referenced and verified on the blockchain, without the revelation of data stored inside the database. This allows the companies to detect data tampering without going through the inefficient process of storing entire files and databases on the blockchain. Example: Chainkit Services. <https://chainkit.com/data-anchoring>





1. Different areas where Blockchain can help IT Risk Management
2. Current Blockchain Platforms for Risk Management
3. Summary of Key Findings
4. References
   1. <https://www.compact.nl/en/articles/how-will-blockchain-impact-an-information-risk-management-approach/>
   2. <https://yourstory.com/2018/12/blockchain-make-data-secure-companies>
   3. <https://raw.githubusercontent.com/coinaccord/resources/master/reports/blockchain-in-information-technology.pdf>
   4. <https://chainkit.com/data-anchoring>
   5. <https://builtin.com/blockchain/blockchain-cybersecurity-uses>

