A comparison between SWIFT and Blockchain from a cyber resiliency perspective

Luisa Franchina[1], Guido Carlomagno[2] [0000-0003-2033-2080]

[1] Hermes Bay S.r.l., Rome (RM) 00143, ITALY
[2] Hermes Bay S.r.l., Rome (RM) 00143, ITALY
guido.carlomagno137@gmail.com

Abstract. Payments critical infrastructure is subject to rapid technological change. Increasingly sophisticated threats must be addressed to ensure the banking and financial system safety and integrity. Several high-profile cyber-incidents have recently shaken the global financial community and stimulated renewed efforts to reinforce and bolster its security framework. Two different cross border payments management approaches have emerged over the years: the SWIFT financial messaging standard and the innovative peer-to-peer transaction model based on the blockchain technology. Debates about which one will prevail as the best practice are currently a very popular topic. Security, and more specifically resiliency to evolving cyber threats, will likely be the main point of concern. Both the SWIFT and the blockchain models present potential exposure to such vulnerabilities. Ultimately, the discussion boils down to an assessment of whether a decentralized, distributed system like the blockchain better meets the integrity requirements of a modern payments infrastructure and is more suitable to mitigate the root cause of cyber incidents, which is human error.

Keywords: Swift · Blockchain · Distributed Ledger · Payments · Banking · Cybersecurity · Cyberattacks · Financial Services · Networks · ICT · Digital Transactions · Peer-to-peer Systems

1 Introduction

The payments landscape is changing rapidly. Customer demands are up, in terms of 24/7 availability, real time settling and enhanced cost efficiency. A constant stream of technology innovations is bringing interesting new tools to the payments sector and driving change in market dynamics, regulation and industry initiatives. Banks, financial institutions, fintech companies are required to do more and faster for less, while maintaining compliance, operational excellence and, most of all, security.

Such an evolving scenario is characterized both by opportunity and threat: the biggest challenge is improving the payments infrastructure resiliency to evolving cyber threats, thus ensuring transaction safety and integrity and financial data security. Evidence shows that in the last few years attackers are increasingly building advanced capabilities to target core banking systems, particularly around payment messaging and transaction authorization. Cybersecurity is therefore becoming the primary concern in the financial sphere for the years to come.

In this paper, we will draw a brief rundown of the digital cross-border payments historical evolution, then we will analyze the current situation in terms of leading technologies and recent cyber incidents that have affected the payment system. Finally, we will compare the two preeminent models (the SWIFT and the blockchain) from a cyber resiliency perspective. Given the emerging nature of this research field, this paper intends to stimulate the debate and provide original data and insights.

2 Evolution of cross border digital payments

2.1 SWIFT history and functioning

In 1973, 239 banks from 15 countries got together to solve a common problem: how to communicate about cross-border payments. The banks formed a cooperative utility, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), headquartered in Belgium [1]. Before SWIFT came into existence, international interbank telecommunication was handled through Telex-Messages. They were not very secure and not automated. Telex Networks were developed from the 1930s onwards and they have been on the decline since the 1980s [2]. SWIFT was founded with the vision of creating a global financial messaging service, and a common language for international financial messaging. Today SWIFT connect more than 11,000 banking and securities organizations, market infrastructures and corporate customers in more than 200 countries. The system provides about 1.8 billion messages per year [1, 3].

All payments involving a seller and a buyer who do not have their respective accounts in the same bank, trigger secondary "street side" transactions, such as clearing and settlement. SWIFT plays the intermediary for transactions in which banks are involved (business-to-bank and bank-to-bank). While national payment systems often rely on a clearing system where banks clear their account after a certain time period at one central location – i.e. the clearing-house - cross border payments are largely managed through correspondent banks, a method facilitated by SWIFT. SWIFT messages are programmed in a language know as FIN. It is heavily influenced by the Telex messages it replaced. A very simple SWIFT message could look like this:

:20:MT101-Test
:28D:00001/00001
:30:040403
:21:Start B-Seq
:32B:EUR1
:23E:CMTO
:50G:/Account Number
BANKDEM0XXX
:59A:/Account Number
BANKDEM0XXX
:71A:SHA

The SWIFT translation system combines several components: its own information transmission network, software that makes it possible to connect to the network and an algorithm for assigning each participant a unique SWIFT code. It is the SWIFT bank code that makes it possible to accurately determine the sender / payee and make the transfer within the shortest possible time. The risk of error in this case is minimal, because the SWIFT code is unique for each participant in the system and contains complete information about it. The SWIFT system aims to help organizations and individuals transferring money to each other in any required currency, regardless of borders between countries and other obstacles [4].

2.2 Blockchain history and its applications in the payment infrastructure

In 2009, an anonymous author who called himself Satoshi Nakamoto published the article "Bitcoin: A Peer-to-Peer Electronic Cash System", thus giving birth to the distributed ledger technology (also known as "Blockchain") [5].

Blockchain technology is an integrated multi-field infrastructure construction, containing elements of cryptography, mathematics and game theory. A peer-to-peer network that uses a distributed consensus algorithm to solve traditional distributed database synchronizing problem. Blockchain key elements are decentralization, transparency and immutability [5]. One of its main applications is funds transferring achieved by using an encrypted technique without relying on a central bank or other trusted third parties. In other words, blockchain is a cryptographically secure system of messaging and recording in a shared database that makes it possible to transact value from point A to point B without the intervention of a third party. What's more, having a single blockchain database to which all users have access not only eliminates the need for a central counterparty, but also eliminates the need for maintaining multiple individual databases [6].

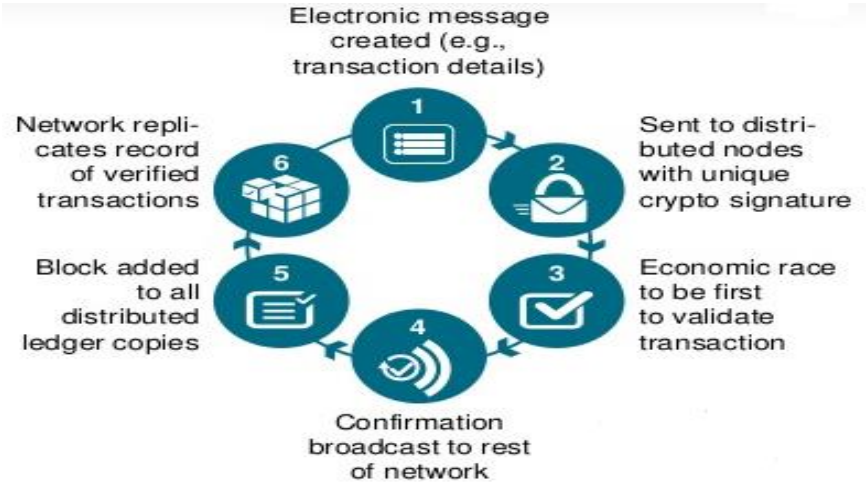

Fig. 1. Graphic elaboration of a digital transaction run on a blockchain network

It is important to stress that blockchain comes in many different types: the main distinction is between a public and a private blockchain. A public blockchain is a permission-less peer-to-peer network. Anyone can join the network, meaning that they can read, write, code, or operate within. On the other hand, a private blockchain is a permissioned network. Permissioned networks place restrictions on who is allowed to participate in the network and in what transactions. Private blockchains partially reintroduce the intermediary that the very concept of a distributed ledger had eliminated [7] This distinction will come in handy later in the paper when we specifically discuss about security challenges related to the blockchain implementation.

Many banks and financial institution have been studying distributed ledger technology attributes and launching blockchain-related projects. Ripple, a California company created in 2012 promising to make payments faster, cheaper and more secure, teamed up with Banco Santander in Aril 2018 to launch a service based on its blockchain messaging technology that allows the Spanish bank's customers in the UK, Spain, Poland and Brazil to send money in many currencies around the world. Santander is only one of more than 100 financial institutions that have registered with Ripple to use its blockchain-based messaging system, known as XCurrent [8]. Other noteworthy blockchain-related projects are the ones involving The Enterprise Ethereum Alliance [9], whose members include the likes of Credit Suisse Group AG and JPMorgan Chase & Co., who also said to be planning to include the mathematical operation known as "Zero Knowledge Proof" [10] in Quorum, its own private distributed ledger [11].

3 Vulnerabilities of the existing financial infrastructure

Banks and financial institutions have always been prime targets for attackers, who are increasingly taking advantage of technological enablers (connectivity, complexity) and are developing new tools and techniques to conduct their malicious activity. In the past decade, the capability and motivation of threats to the financial sector have transformed from small-scale opportunistic crimes to efforts to compromise entire networks and payment systems.

In 2011 and 2012, hackers staged distributed denial-of-service (DDOS) attacks against U.S. banks to disrupt banking services. Although these attacks were basic and caused minimal long-term damage, they were a preview of the cyber-incidents wave that was about to come [12]. Since then, a wide variety of sophisticated cyber-attacks, often characterized by the deployment of malware on payment systems to create a smokescreen for the fraudulent activity and gain access to user credentials, took place repeatedly in many parts of the world, causing concern in the financial sector [13].

3.1 Recent attacks on SWIFT systems

There have been at least six high-profile attacks on SWIFT systems in recent years (among many other lower-profile attacks), some of which resulting in significant financial loss. The number of successful attacks against these systems shows how SWIFT

security architecture needs improvements and customers must do more to protect their local infrastructures.

Sonali Bank (2013). Attackers were able to infect the bank's internal systems with key-logger software that was used to harvest user credentials. These credentials were then used to laterally move through the bank's network in order to gain access to the bank's internal SWIFT systems, where $250,000 worth of transactions were made [14].

Banco del Austroz (January 2015). Attackers stole the credentials of a bank employee and used these credentials to access the employee's Outlook email account. Using this access, the attackers located, cancelled and rejected SWIFT transfer requests, altered their details, and reissued them, resulting in $12,000,000 worth of legitimate transfer requests being sent [15].

Tien Phong Bank (December 2015). Attackers used malware that specifically targeted the Foxit PDF reader, which was known to be used by the bank employees when viewing SWIFT statements. Attackers were able to install a malicious version of the Foxit PDF reader on employee workstations, which altered statements (when opened) in order to hide evidence of any malicious activity. This malware was found to be installed on infrastructure provided by a third-party vendor. Employees at the Tien Phong Bank identified suspicious SWIFT messages and rapidly contacted all parties involved. This prevented the transfer requests from being completed and the attempt to steal $1,130,000 was halted [16].

The Bank of Bangladesh (February 2016). Investigations found that the attack had been patiently executed over the period of almost a full year. Attackers gained access to the bank's internal systems in order to monitor employee activity. Using this initial foothold, attackers were able to move laterally across the bank's internal network in search of SWIFT-connected systems. Once access to SWIFT systems was obtained, the attackers monitored employee behavior, stole user credentials, and deployed specifically-designed malware named evtdiag.exe, an executable file designed to hide the attackers' activity by changing the logs on a SWIFT database. The malware targeted the SWIFT Alliance Access application, bypassed its security controls, and removed evidence in order to cover the tracks of their fraudulent transfers [17]. A total of 35 SWIFT transactions worth $951,000,000 were made. However, only $81,000,000 of this was successfully exfiltrated from the Bangladesh Bank's account at the Fed Reserve in New York. The transfers were made towards Philippine casinos bank accounts between February 4 and February 5, 2016 [18].

The Far Eastern International Bank (October 2017). Attackers used malware to gain access to and move through the bank's internal network in order to infiltrate SWIFT systems. Attackers then compromised employee credentials and used this information to authenticate to the SWIFT Alliance Messaging Hub and issue a total of $60,100,000 worth of fraudulent transactions. Although it was initially understood that $500,000 was lost, the Financial Supervisory Commission (FSC) reported that the final amount lost by Far Eastern Bank was $160,000. Following an investigation, it was found that the bank's security posture was not in line with the requirements outlined by Taiwan's banking law [19].

The NIC Asia Bank (October 2017). Attackers specifically targeted the bank during the Hindu festival Tihar, one of Nepal's largest holidays. According to reports, $4,400,000 of fraudulent SWIFT transactions were issued during the heist. However, NIC identified the suspicious activity and informed Nepal Rastra Bank (which is Nepal's central bank), resulting in the recovery of all but $580,000 of the $4,400,000 [20].

The main common factor amidst these incidents is the deployment of some type of malware onto a bank's internal systems. We can also see that attackers frequently pair this with the compromise of user credentials. Overall, it can be concluded that none of the attacks directly compromised the SWIFT network itself, and that they were frequently the result of flaws in the security controls within the local targeted bank's IT environments. Another common element is the presence of some type of user error. This should come as no surprise, as showed by the 2014 IBM's Cyber Security Intelligence Index, which reported that 95% of all cyber incidents recognize "human error" as a contributing factor [21]. In fact, regardless of how resilient and strong a system is, human error can nullify any security framework and architecture.

3.2 SWIFT new security architecture and blockchain experimentation

Previously mentioned cases of data breaches and hacks involving banks linked to the SWIFT network have renewed the debate around SWIFT security and cyber resiliency.

As a countermeasure to the current cyber-threat landscape, SWIFT recently introduced the Customer Security Program (CSP) to support SWIFT customers in securing their local SWIFT infrastructure. This program requires that all customers implement a set of mandatory and advisory security controls outlined within SWIFT's Customer Security Controls Framework (CSCF) [22]. The main focus of CSP is to isolate all SWIFT systems into a secure zone. Without this type of security, attackers would have the opportunity to access SWIFT systems from a variety of entry points across the general enterprise network. With the implementation of all controls within CSCF, the attack surface of the SWIFT infrastructure is considerably reduced, removing a wide range of attack paths that could previously be exploited. However, CSP remains a compliance challenge, and as such it cannot be relied upon alone to mitigate and prevent the compromise of these complex payment systems. Within the CSP document itself, it is stated that CSP should not be considered an exhaustive approach to security and it does not replace a well-structured security and risk framework.

In April 2016, SWIFT and global consulting services company Accenture released a joint report that looked at the use of distributed ledger technologies (DLT) in financial services. Specifically, the paper acknowledged some strengths of the blockchain like efficient information propagation, traceability, simplified reconciliation and high resiliency [23]. In March 2017, SWIFT revealed that they had finished the Proof of Concept phase of its own distributed ledger prototype. According to SWIFT's R&D head Damien Vanderveken, blockchain's implementation would require a significant infrastructure overhaul for banks that had already invested in centralized solutions. "A

substantial number of banks would have to drastically modernize their systems before they could turn to a blockchain-based system for their cross-border payments" he said. Reportedly, the testing involved the creation of 528 sub-ledgers for 28 participating banks to avoid confidential information being revealed to rivals. All of the SWIFT members, thousands of banks, would require 100,000 sub-ledgers to be established, which is technically and economically burdensome, inefficient and presents maintenance issues [24].

4 Blockchain and cybersecurity

It is common sense that blockchain can help fortify the cyber security landscape. The potential of a strong, decentralized security proposition which represents an alternative to fully or partially-centralized systems that contain single access points of vulnerability is worth to be assessed and explored.

4.1 Security benefits of decentralization

With respect to the specific field of finance and payments, there are reasons to believe that blockchain features and applications can help deal with the type of malicious tactics implemented in the aforementioned attacks.

DDoS risk mitigation and operational resilience. We live in an age where DDoS attacks will only grow over time. Considering a rising number of unsecured IoT devices are connected to one another, the potential for DDoS attacks to creep in and overpower an organization is very real. With the number of IoT devices in operation expected to climb from around 8.4 billion in 2017 to 20.4 billion by 2020, according to Gartner research [25], the ease of launching massive DDoS attacks will increase and no existing system can address this problem unless it is truly distributed. That's where the blockchain solidly comes in handy. When it comes to a DDoS attack, the blockchain has protections to ensure transactions can continue even if several nodes go offline. Multiple blockchain nodes across many different institutions must be attacked to overwhelm the full infrastructure. If several nodes are offline, nodes under attack can be made redundant while the others continue working as usual, protecting the operational continuity of the whole system. The protocol recovers as nodes are brought back online and are re-synched to ensure that consistency and integrity is preserved [26]. Several blockchain startups have even claimed that they are able to protect against DDoS attacks by allowing users in a network to rent out their extra bandwidth to support networks who are being overloaded with traffic as a result of an attack [27].

Improved data validation and hacks prevention. Million new forms of malware are created every year [28]. They are often difficult to spot and come as a software download or a phony application update. Settings such as automatic updates can inadvertently include malware. The blockchain has the capacity to assign unique hashes to downloads and updates. This allows users to compare the hash on their would-be download with the developer's hash to significantly reduce the chances of infecting their

systems with fraudulent, well-disguised malwares [29]. Furthermore, experts are relying upon blockchain technology to recognize invalid or potentially corrupt commands and inputs. Data that is filtered through a decentralized network tends to be more trustworthy, as the multi-node security lends itself to greater verification and tamper prevention. The use of advanced cryptographic techniques makes it more probable that data is coming from correct sources and that nothing is intercepted in the interim [30].

Evolved identity authentication. The username-password login framework is rapidly growing obsolete, as clearly shown by the ever-increasing numbers of compromised user credentials [31]. As it currently stands, usernames and passwords for a given site or application are stored in central databases that are vulnerable to the typical single-point-of-failure hacking hazard. A superior method of digital access management is definitely needed. One of the main features of the blockchain is that it doesn't require passwords because it relies on either biometric data or private keys and multi-step authentication to verify the identity of a user. This kind of identity and access management process makes it more difficult for hackers to enter the network and leave undetected, preventing them the possibility to hide their tracks or erase records of their unwarranted access. Combining the decentralized architecture of the blockchain and the biometrics on the mobile device, this multi-signature/multi-factor authentication model is a more secure mean of granting access to a network, assigning digital identities not only to users but also to each device registered on the network. Only a combination of the authenticated user and device can provide an entry to the data [32].

4.2 Security issues of decentralized systems

In spite of all the points made above, someone could argue that Bitcoin and cryptocurrencies have been the ultimate hacker honey pot for many years now, with many renowned cases of cyber-theft connected to them [33]. It is very important to highlight that this argument is inconsistent with this paper's topic of discussion, as it only relates to the operational usability of cryptocurrencies exchanges, private wallets security and secure storage of cryptographic keys. It has nothing to do with the blockchain technology core network integrity and security. Actually, "Bitcoin Core" – the Bitcoin's open-source blockchain software underpinning - to date has successfully withstood cyber-attacks for many years [34]. Having cleared that up, there is no doubt that decentralized systems like blockchain are not per se immune to any issue regarding cyber security.

Consensus mechanisms alteration. The blockchain is updated via the consensus protocol that ensures a common, unambiguous ordering of transactions and blocks and guarantees the integrity and consistency of the blockchain across geographically distributed nodes. Since the consensus model maintains the sanctity of data recorded on the blockchain, it is important to ensure that it functions correctly in normal as well as adversarial conditions. In other words, a blockchain based system is as secure and robust as its consensus model [35]. Especially in a permission-less setup, the number of nodes is expected to be large, and these nodes are anonymous and untrusted since any node is allowed to join the network. Consensus mechanisms for such a setup need to account for maliciousness: particularly Sybil attacks, which can allow a single user to

generate several online identities to influence and manipulate the consensus process. Dominance can also be achieved by other means, as consensus round outcomes can be manipulated by a single or group of entities that is able to control the majority of the hash rate. In such a scenario, the attacker would have enough mining power to intentionally exclude, reverse or modify the ordering of transactions [36]. However, the key problem a hacker would need to solve to create a 51% attack is acquiring the majority of the power that supports that specific blockchain. This process becomes increasingly unlikely as the dimension on the blockchain network grows. The bigger the network, the stronger the protection against attacks and data corruption. With the rising price of Bitcoin as a currency, numerous new miners entered the system aiming to compete for the block rewards (currently set as 12.5 BTC per block) [37]. Such a competitive scenario is one of the reasons why Bitcoin is perceived as being highly secure. At least this is what conventional wisdom currently asserts: the mining protocol is incentive-compatible and secure against colluding minority groups, as it incentivizes miners to follow the protocol as prescribed (they have no incentive to invest large amounts of resources if it is not for acting honestly and striving to receive the block reward). Nonetheless, recent scientific paper shows that even a 25% share can incentivize selfish miners to join the set of colluding nodes, presenting an attack with which colluding miners' revenue is larger than their fair share and thus challenging the widespread 51% notion [38].

4.3 Operational challenges for blockchain implementation in payment infrastructures

It needs to be understood that the undeniably great cyber resiliency potential of the distributed ledger technology is not automatically applicable to the very complex and articulated modern payment infrastructures.

As previously discussed, not all blockchain networks are equal, and a particular network's robustness largely depends upon its diversity and number of nodes and its hash rate. We have seen that the maximum degree of security is provided by public, sizable and globally distributed blockchains like the Bitcoin's one, whose number of full nodes validating its transactions is close to 60,000 - according to prominent Bitcoin Core developer Luke Dashjr [39]. However, implementation of such distributed public networks must be evaluated on a large scale. If blockchain technology could be deployed on a large scale for payments, it would improve the level of security significantly, but it is evident that a fully open and public blockchain infrastructure is, at the current state of the art, not entirely applicable to the field of interbank cross border payments. Main reasons for this are issues related with redundancy, scalability and data sharing, which ultimately lead to inevitable inefficiencies that could make blockchain overall inferior to alternatives, including existing systems. Current claims that public ledger platforms can conduct financial transactions more efficiently ignore the inefficiencies associated with the huge computational power that is needed to maintain a widely distributed ledger (one study found that the electricity wasted in Bitcoin mining is comparable to the average electricity consumption of Ireland [40]). In addition, the feasibility of using a public blockchain employing a Proof-of-Work consensus for a high volume of

payment transactions still remains a big question mark, as demonstrated by the low amount of transactions per second supported by Bitcoin if compared to the VISA or MasterCard numbers [41]. Finally, blockchain experimentation conducted by the SWIFT organization showed how incompatible is confidential data privacy protection with a public ledger implementation: real-banking and financial institutions praxis would require the establishment of thousands of private small sub-ledgers [24], which is technically and economically burdensome because of operational and maintenance issues and, most of all, partially nullify the security benefits of large distributed ledgers.

5 Conclusion

In the present-day cyber-threat landscape, attacks on SWIFT systems have been the focus of advanced persistent threats. Specifically-designed malwares and advanced tactics are used to achieve the goal of performing fraudulent financial transactions. As with most compromises, the root cause of vulnerability will frequently remain human error, whether this error be made by administrators in a configuration file, developers in their application code, or employees being deceived into opening a malicious email attachment. In this respect, blockchain solutions have the potential to help mitigating this fundamental flaw in security (i.e. human error), due to their inherent trustless, automated operational structure. Blockchain is decentralized by nature, which means there is no single point of penetration for hackers to invade, no centralized weak points to exploit as the information never passes through a single server. It also offers improved capacity to recognize invalid or potentially corrupt commands and inputs, and enhanced data validation and identity authentication. In other words, with blockchain systems in place of legacy ones the window of opportunity and the attack surface for hackers are significantly reduced, whereas room for human error impact is kept as minimal as possible.

However, one thing is assessing and recognizing security benefits of this new technology, another thing is implementing its features in the extremely complex modern payment infrastructure. SWIFT has been so successful and widely adopted over the years because it offered a standardized solution completely tailored to the technical and operational demands of existing financial institutions. It should not be taken for granted that this will be the case with blockchain. Recent SWIFT's own distributed ledger experimentation demonstrates that there is interest around this new emerging technology's potential, yet its implementation presents quite a few areas of criticality. This includes, firstly, the trade off between the level of resiliency, integrity that a fully open, public, sizable chain like Bitcoin (which should be assumed as a central point of reference security-wise) ensures and the actual impossibility to adapt anything remotely resembling it to the existing cross-border digital payment management system. One of the reasons why being the fact that banks can't allow confidential information being revealed to rivals. This creates the need to implement a number of private ledgers, whose network size and inherent consensus mechanism does not necessarily grant the type of security and operational resiliency that characterizes a public chain.

It is for all these reasons that a step in the direction of a necessary reconciliation between blockchain systems and banks systems interoperability needs to be made before being able to exploit the great cybersecurity potential of the new decentralized paradigm. Furthermore, technology improvements on the scalability and energy consumption sides must occur before blockchain can be considered ready to be efficiently used. It is highly likely that, rather than completely replacing all major financial processes, the blockchain model will instead take its place beside and integrate with existing systems.

References

1. SWIFT Website, https://www.swift.com/about-us/history, last accessed 2019/09/09.
2. Huurdeman, A.A.: The worldwide history of telecommunications. Wiley-Interscience Publications, (2003)
3. Köppel, J.: The SWIFT Affair: Swiss Banking Secrecy and the Fight Against Terrorist Financing. 1st edn. Graduate Institute Publications (2011).
4. Scott, S.V., Zachariadis, M.: Origins and development of SWIFT, 1973–2009. Business History Journal (54), (2012).
5. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013. (http://bitcoin.org/bitcoin.pdf).
6. Crosby, M., Pattanyak, P., Nachiappan, Verma, S., Kalyanaraman, V.: Blockchain technology: Beyond bitcoin. Applied Innovation Review (2), (2016).
7. Yaga, D., Meel, P., Roby, N., Scarfone, K.: Blockchain Technology Overview. National Institute of Standards and Technology Internal Report 8202, (2018).
8. Ripple Website, https://ripple.com/ripplenet/process-payments/, last accessed 2019/09/09.
9. EEA Homepage, https://entethalliance.org/, last accessed 2019/09/09.
10. Pandit, V., Dayama, P.: Privacy in blockchain collaboration with zero knowledge proofs. IBM Blockchain Blog (2019).
11. J.P. Morgan Website, https://www.goquorum.com/, last accessed 2019/09/09.
12. Bank Info Security Website, https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989, last accessed 2019/09/09.
13. Nish, A., Naumaan, S.: The Cyber Threat Landscape: Confronting Challenges to the Financial System. In: Cyber Policy Initiative Working Paper Series, p. 8-9. Carnegie Endowment for International Peace (2019).
14. Reuters Website, http://uk.reuters.com/article/us-cyber-heist-bangladesh/exclusive-bangladesh-probes-2013-hack-for-links-to-central-bank-heist-idUKKCN0YG2UT, last accessed 2019/09/09.
15. Nettitude Website, https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf, last accessed 2019/09/09.
16. TrendLabs Security Intelligence Blog, https://blog.trendmicro.com/trendlabs-security-intelligence/high-profiled-cyber-theft-against-banks-targeted-swift-systems/, last accessed 2019/09/09.
17. LIFARS Website, https://lifars.com/2016/04/bangladesh-bank-hackers-used-malware-swift-software/, last accessed 2019/09/09.
18. Reuters Website, https://www.reuters.com/article/us-bangladesh-bank-idUSKCN0WF0IL, last accessed 2019/09/09.
19. Bae Systems Threat Research Blog, https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html, last accessed 2019/09/09.

20. The Himalyan Times Website. https://thehimalayantimes.com/business/kpmg-team-seek-time-draw-conclusion-nic-asia-bank-case/, last accessed 2019/09/09.
21. IBM Website, Research Report: IBM Security Services 2014 Cyber Security Intelligence Index, p. 3, https://www.ibm.com/developerworks/library/se-cyberindex2014/index.html, last accessed 2019/09/09.
22. SWIFT Website, https://www.swift.com/myswift/customer-security-programme-csp/security-controls, last accessed 2019/09/09.
23. SWIFT Website. https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services, last accessed 2019/09/09.
24. Financial Times Website, https://www.ft.com/content/966f5694-22c6-11e8-ae48-60d3531b7d11, last accessed 2019/09/09.
25. Gartner Website, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016, last accessed 2019/09/09.
26. Dheeraj, J., Gurhubaran, S.: DDoS Mitigation Using Blockchain. In: International Journal of Research in Engineering, Science and Management, Volume-1 Issue-10 (2018).
27. Liu, Z., Cheng, X.: Application of Block chain Technology in the Field of Network Security. In: International Core Journal of Engineering Volume-5 Issue-7 (2019).
28. G-Data Blog, https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017, last accessed 2019/09/09.
29. Nasonov, D., Visheratin, A. A., Boukhanovsky, A.: Blockchain-based transaction integrity in distributed big data marketplace. In: Computational Science ICCS 2018, pp 569-577 (2018).
30. Sigwart, M., Borkowski, M., Peise, M., Shulte, S., Tai, S.: Blockchain-based Data Provenance for the Internet of Things. arXiv:1905.06852v2 (2019).
31. Ismail, R.: Enhancement of Online Identity Authentication Though Blockchain Technology. DOI: 10.18517/ijaseit.8.4-2.6838 (2018).
32. Delgado-Mohatar, O., Tolosana, J. F. R., Vera-Rodriguez, R.: Blockchain and Biometrics: A First Look into Opportunities and Challenges. arXiv:1903.05496v1 (2019).
33. ZDNet Website, https://www.zdnet.com/article/bitcoin-blues-this-is-how-much-cyptocurrency-was-stolen-last-year/, last accessed 2019/09/09.
34. Deloitte Website, Research Report: Blockchain & Cyber Security. Let's Discuss, p. 10, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-blockchain-and-cyber-security-lets-discuss.pdf, last accessed 2019/09/09.
35. Baliga, A.: Understanding Blockchain Consensus Models. In: Persistent Systems Ltd White Paper, pp. 3-8. (2017).
36. Chang Lin, I., Chun Liao, T.: A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security (19), (2017).
37. Bitcoin Visuals website, https://bitcoinvisuals.com/chain-block-reward, last accessed 2019/09/09.
38. Eyal, I., Gun Sirer, E.: Majority is not enough: bitcoin mining is vulnerable. In: Magazine Communications of the ACM Volume-61 Issue-7, pp. 95-102 (2018).
39. Luke Dashjr Website, https://luke.dashjr.org/programs/bitcoin/files/charts/software.html, last accessed 2019/09/09.
40. O'Dwyer, K. J., Malone, D.: Bitcoin Mining and its Energy Footprint. In: ISSC 2014 / CIICT 2014 (2014).

DataLight Website, https://datalight.me/blog/researches/longread/bitcoin-becomes-the-main-method-of-international-payment/, last accessed 2019/09/09.