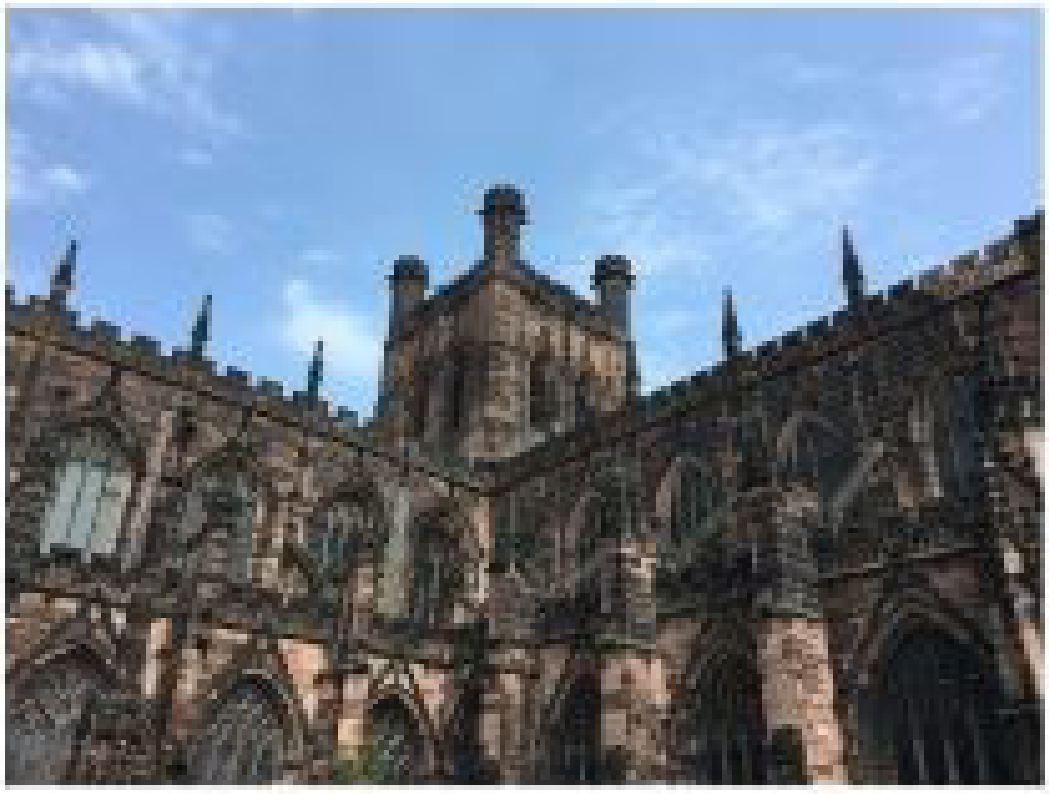
University of Chester

University of Chester

Proceedings of the 20th European Conference on Cyber Warfare and Security

a Virtual Conference hosted by
University of Chester
UK
24-25 June 2021



Edited by
Dr Thaddeus Eze, Dr Lee Speakman and
Dr Cyril Onwubiko

A conference managed by ACI, UK

aci

Proceeding of the

20th European Conference on Cyber Warfare and Security

ECCWS 2021

A Virtual Conference

Hosted By

University of Chester

UK

24th-25th June 2021

Peer2Peer Communication via Testnet Systems of Blockchain Networks: A new Playground for Cyberterrorists?

Alexander Pfeiffer[1, 2, 3], Thomas Wernbacher[1] and Stephen Bezzina[2, 3]
[1]Center for Applied Game Studies, Donau-Universität Krems (DUK), Austria
[2]Department of Artificial Intelligence, University of Malta (UoM), Msida, Malta
[3]B&P Emerging Technologies Consultancy Lab Ltd., St. Julian's, Malta
Alexander.pfeiffer@donau-uni.ac.at
Thomas.wernbacher@donau-uni.ac.at
mail@stephenbezzina.com
DOI: 10.34190/EWS.21.049

Abstract: Peer2Peer communication can take place in the traditional way via e-mail, forums or social media. One also finds dedicated apps for communication or organized in groups, such as WhatsApp, Telegram or Discord, the latter being particularly popular with digital gamers. Online games are another medium which can foster communication between people over a data connection, as direct messages can be sent through the provisions of the digital game worlds. Depending on the game provider and its headquarters, the terms and conditions differ in how the data is transmitted and processed. Access to private communications is important for governments and especially for the police work, for both to prevent and follow up on cybercrime and terrorist acts. On the other hand, the private and civil rights movements push for such interventions to occur only in the case of absolutely justified suspicion, with otherwise restricted access to transmitted conversations and data of private individuals and companies. Therefore, it is important that such access to messages is confirmed in advance by a law court. But even with approval, it is still difficult for the authorities to gain access from a technical perspective. While IP addresses and open communication can be intercepted quite easily, it is more difficult when secure messenger apps are used and only possible if there is direct access to the user's device or the app operator provides the authorities access via a master key. In digital games, access is even more complicated. In this work-in-progress paper the authors want to address a currently overlooked aspect of Peer2Peer communication; which is the provision of text messages via (testnet) blockchain systems, with special regard to the possibility of attaching encrypted messages to the transaction of blockchain tokens. It is to be noted that on the testnet versions of the blockchain systems no "KYC" takes place. While on the mainnet versions of the blockchain systems the purchase of tokens to send them later can only be done anonymously "over the counter", the testnet of most blockchain systems is completely free available. Everyone can create a blockchain Wallet, request testnet tokens and start sending encrypted messages anonymously. This work-in-progress paper aims to highlight and explain the authors' planned research in this field.

Keywords: blockchain, DLT, social media, utility tokens, cryptocurrencies, rewards

1. Introduction to the topic

The issue of communication between individuals, cells or gangs with criminal intentions using modern communication technologies has been part of the ongoing debate for a long time. Not only since 9/11 the issue of monitoring the communication between citizens is being discussed and investigated, but above all when is surveillance legitimate. Various preventive measures against crime have been taken, such as the self-registration obligation for pre-paid SIM cards, as is currently the case in the EU[1]. However, in reality, as the white paper "The Mandatory Registration of Prepaid SIM Card Users" from 2013 suggests:

> *"An increasing number of governments have recently introduced mandatory registration of prepaid SIM card users, hoping that the policy would support law enforcement and counter-terrorism efforts. However, to date there is no evidence that mandatory registration leads to a reduction in crime."*

It should also be noted, though, that this publication was written by a group representing the interests of the mobile communications industry.

The measures taken by governments in the fight against terrorism and the capabilities to read and analyze conversations go one step beyond the mere registration of devices and sim cards. At the end of 2020, for example, a cabinet decision was taken in Germany to be able to read encrypted messages from WhatsApp or

[1] Cf. Registration Law in Austria, according to EU legislation: https://www.bmlrt.gv.at/english/telecommunications-and-postal-services/telecommunications-/registration-of-mobile-phone-prepaid-card.html, last Accessed 26.01.2021

Facebook Messenger[2], although it was emphasized that this is allowed only in individual cases and after a court order. To access these messages, however, it is necessary either to install malware / Trojan horses on the user's devices, or to gain direct personal access to the devices for a short period of time. In this case, the browser services of the chat platforms are used by the police investigators, who connect the cell phone of the suspect to the browser service via a QR code and can thus read the messages[3].

Another way to communicate in an encrypted modality is via email and OpenPGP | S/MIME. In 2018, however, the research group behind efail published how, under certain conditions, but mostly due to user errors in the use of the encryption service, access to the plaintext of messages can be obtained. Another potential area of non-supervised communication is video games. In 2011, Thomas Gabriel-Rüdiger and Cindy Krems, both cybercrime experts from Germany, gave a lecture at the Danube University Krems in which they showed how online role-playing games can be used to plan terrorist activities[4]. It is especially difficult to track down when the language code is based on in-game terms or otherwise. For example, the name of a boss monster is assigned to the terror target. So the cell pretends to be planning a raid. Coordinates from the game can also be used here, which can then be applied to maps in the real world. Such conversations are even very difficult to interpret for Artificial Intelligence algorithms. Especially when working with private chats, it is also impossible for a gamemaster to notice. And so, these conversations can only be intercepted if there is already a suspect of terrorism, the user name of the player is known, and there is a corresponding court order that allows the authorities to cooperate with the game producers to receive chat data in real time.

In 2015, a broader discussion on this topic began, especially through mass media. This has partially forced the manufacturers to adjust the Terms and Conditions, and in some games players now agree that chat messages are stored for a certain time. As an example of the media discussion, a debate on this topic can be found on CBSN[5]. A large audience was made aware of this possibility of communication via a fictional terror scenario. In the television series Jack Ryan (2018), a (not in real-life existing) computer game was shown via which terrorists communicate across countries. What is particularly exciting is that this example encourages us to think not only of large commercial games, but of independent games, i.e. low-budget games with encrypted voice or text chats; games that can be used just under the radar of the investigators. Another important aspect in the discussion of using games as methods of communication is the aspect of data ownership. The senders of the messages do not know, apart from the set of rules described in the terms and conditions, what actually happens with their messages. For example, how long they are stored, and which authorities get access rights at which point in time. An alternative would be dedicated computer games that are used as a cover, but once revealed, these would be a fish pond for the investigators and therefore it is not assumed that these approaches actually exist.

The authors will now take a look at a communication technology that still seems unnoticed by cyberterrorism academia, as well as by the authorities. Blockchain and especially testnet systems of blockchain networks as means of communication. By definition, a Blockchain is a continuously growing chain of blocks, each of which contains a cryptographic hash of the previous block, a time-stamp, and its conveyed data (Nofer et. al, 2017). Grech and Camilleri (2017) describe (positive) effects of Blockchain technologies, like self-sovereignty, trust, transparency, immutability, disintermediation and collaboration. The concept of Blockchain, as we know it today, derives from Satashi Nakomoto's Whitepaper 'Bitcoin: A Peer-to-Peer Electronic Cash System', published in late 2008. Originally intended to create a non-manipulable account book to represent the possession of digital tokens, which in turn are traded for money on exchanges or over-the-counter (peer2peer), it is now about the technology behind it and what applications can possibly be developed using Blockchain technology to secure transactions. The idea of using the Bitcoin Blockchain for more than 'proof of payment transactions' arose from the fact that you can attach text messages to a transaction. To create an account book of any imaginable transaction, a fraction of Bitcoin (so-called Satoshis) was sent to an address and the text to be recorded was attached to it as a text message and thus stored forever on Blockchain. However, if such information is simply stored as a text message attached to the same kind of token, this strongly limits its possible applications. And since Bitcoin was not originally intended for other applications apart from payment, in early 2010, a network in

[2] Cf. Die Welt.de: https://www.welt.de/politik/deutschland/article218298328/GroKo-Beschluss-Geheimdienste-duerfen-nun-WhatsApp-Chats-mitlesen.html, last Accessed 26.01.2021

[3] Cf. Der Standard: https://www.derstandard.at/story/2000118906392/wie-deutsche-ermittler-bei-whatsapp-mitlesen-koennen, last Accessed 26.01.2021

[4] Cf. Die Presse: https://www.diepresse.com/687375/kriminalitat-virtuelle-spielewelten-als-tatorte-fur-verbrecher, last Accessed 26.01.2021

[5] Cf CBSN: https://www.cbsnews.com/video/terrorists-use-video-games-to-communicate-undetected/, last Accessed 26.01.2021

which sub-tokens (metatokens) can be generated for a specific application was developed. The Blockchain systems NXT and/or Ardor[6] and Ethereum[7] are particularly noteworthy in this context from a historical as well as current perspective.

Blockchain, in the sense of cryptocurrencies are found in the cybercrime literature and discussion primarily in the context of terrorist financing, the movement of funds and money laundering, but not in the scope of peer2peer communication. This also seems to make sense at first glance, as blockchain systems are characterized by information being stored forever on the one hand, and on the other hand, more and more countries have implemented strict know-your-customer regulations when it comes to converting the proceeds from the sale of blockchain tokens into FIAT currency (a currency established as money, often by government regulation). These steps are, of course, to be welcomed as it helps legitimize cryptocurrencies in regards to transnational trade.

However, for the scope of this paper, the authors would like to take a closer look at testnet systems of blockchains, more specifically how these can be easily set up by evildoers as completely private systems, operated off the grid of authorities. Also, it is important to note how the mainnet systems of public blockchains, especially those on which meta-tokens can be created, can be used to communicate encrypted and completely unnoticed. In addition, the authors would like to discuss how new technologies such as pruning, where the private information, i.e. the encrypted text message, can no longer be stored by the blockchain after a certain self-defined block height, increases the possibility of illegal activities via such testnet systems of different blockchains. This will in turn strongly address the issue of data ownership mentioned previously, because especially in the case of private networks, which in turn rely on technologies such as pruning within their network, the intrinsically positive aspect of data security and ownership could result in major barriers to investigation from the authorities' point of view.

2. Related research

In terms of communication and terrorism, most of the literature focusses on terrorists engaging in communication with the outside world. Matusitz (2013) described this from the different viewpoints, while Mahmood and Jetter (2020) analyzed the role of communication technology from 1970 to 2014, finding that online communication via internet is an emerging tool to spread the word to their followers. A similar aspect, often covered in literature is the role of media, reporting about terrorism. For instance, this is addressed bv Archetti (2013) who focuses on the aspect of news agencies producing headlines that might produce many “reads”, but whose content is not based on facts. Cahyan et. al (2017) research highlighted the importance of mobile device forensics in investigations involving the use of cloud storage services and communication apps along with the necessity and potential utility of the integrated incident handling and digital forensics models to investigate and reconstruct terrorist incidents. Their research included the investigation of three popular cloud apps (Google Drive, Dropbox and OneDrive), five communication apps (Messenger, WhatsApp, Telegram, Skype and Viber), and two email apps (GMail and Microsoft Outlook). However, blockchain as communication tool is an original and innovative idea that is not found in literature. This is probably explained by the fact that blockchain, as already mentioned, was originally designed to store data forever and immutably. However, the authors take a special look at testnet systems and new technologies such as pruning, where attached records are also deleted after a self-defined block height. Therefore, the intended research described in this WIP paper is an absolute novelty.

3. Planned research goals and methods used

Therefore, the aims of the upcoming research are:

- 1. To analyse the various Blockchain testnet systems in detail from different points of view: How difficult is it to install your own full node, how difficult is it to create a wallet, how can your own meta tokens be generated, how can encrypted messages be attached to the native tokens of the system or the meta tokens created by the users when transferring them, which encryptions are used in the process and which are used for the wallet-address of the user. Is pruning as technology implemented in the network? And above all, how users get test tokens of the native token system and what information is revealed about the user in the process? This analysis is done by installing and testing the common Bockchain testnet systems on the

[6] Jelurida: https://www.jelurida.com, last Accessed 26.01.2021
[7] More on Ethereum: https://ethereum.org, last Accessed 26.01.2021

one hand and by literature review including the whitepapers related to the respective networks on the other hand. In addition, resources such as Git-Hub will be consulted in order to evaluate specific functionalities.

- 2. To interview experts from different fields and perform a content analysis of the answers based on the results of (1).
- 3. To develop guidelines with suggestions for the blockchain community, as well as the authorities and cybercrime researchers, as to what measures should be taken in the future, for example in the form of a know your customer (KYC) light process when distributing blockchain testnet tokens to the users/developers of the corresponding testnet systems, including zero-knowledge proof systems for authentication and shared-key options – for example for multi-signature from different authorities – to access the necessary data only in a well-founded suspicious case.

These steps should always be crafted under the premise that blockchain systems have the potential to contribute very positively to the world of data security. As such, future regulations should therefore not interfere with the development of new applications via the testnet systems. Nevertheless, they should provide a necessary hurdle to make the use of these systems less attractive to cyberterrorists.

4. Conclusion

With this upcoming article, the authors want to contribute to the field of cybercrime and initiate a new discussion on this topic. The research will take place in the second half of 2021 and the final paper will be published and presented in 2022.

References

Archetti C. (2013) Terrorism, Communication, and the Media. In: Understanding Terrorism in the Age of Global Media. Palgrave Macmillan, London. https://doi.org/10.1057/9781137291387_3

Cahyani, N. Ab, R.;Glisson, W.; Choo, K. (2017). The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Storage Service and Communication Apps. Mobile Networks and Applications. 22. 10.1007/s11036-016-0791-8.

Cahyani, Niken Dwi; Wahyu; Rahman, Nurul Hidayah; Ab; Glisson, William Bradley; Choo, Kim-kwang Raymond (2017) .Mobile Networks and Applications; New York Bd. 22, Ausg. 2, (Apr 2017): 240-254. DOI: 10.1007/s11036-016-0791-8

EFAIL: EFAIL describes vulnerabilities in the end-to-end encryption technologies OpenPGP and S/MIME that leak the plaintext of encrypted emails. (2018) Retrieved from https://efail.de/#paper, last Accessed 26.01.2021

Grech, A. and Camilleri A. (2017) Blockchain in Education. https://doi.org/10.2760/60649; Accessed: January, 2020

GSMA Mobile for Development Foundation, Inc. (2013) Retrieved from https://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf, last Accessed 26.01.2021

Mahmood, R., & Jetter, M. (2020). Communications Technology and Terrorism. Journal of Conflict Resolution, 64(1), 127–166. https://doi.org/10.1177/0022002719843989

Matusitz, J. (2013) Terrorism & Communication, a Critical Introduction, Sage, Los Angeles

Nofer, M., Gomber, P., Hinz, O. and D. Schiereck (2017), Blockchain, Bus. Inf. Syst. Eng., vol. 59, no. 3, pp. 183–187, Mar. 2017. DOI 10.1007/s12599-017-0467-3

Satoshi Nakamoto (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, in Whitepaper online available https://bitcoin.org/bitcoin.pdf (Satashi Nokamoto is a pseudonym, it is not known to the general public who is behind this name.); Accessed: January, 2020