Design of Cryptopol: A serious game for teaching cryptocurrency tracing techniques to Law Enforcement

HANCOCK, Paul, VAN HARDEVELD, Gert Jan, JAKUBCEK, Jarek, AKHGAR, Babak <http://orcid.org/0000-0003-3684-6481>, DAVEY, Steffi and AMANN, Philipp

Design of Cryptopol: A serious game for teaching cryptocurrency tracing techniques to Law Enforcement

PAUL JOHN HANCOCK, CENTRIC, Sheffield Hallam University, Sheffield, United Kingdom of Great Britain and Northern Ireland
GERT JAN VAN HARDEVELD, Europol, The Hague, Netherlands
JAREK JAKUBCEK, Former Europol, The Hague, Netherlands
BABAK AKHGAR, CENTRIC, Sheffield Hallam University, Sheffield, United Kingdom of Great Britain and Northern Ireland
STEFFI DAVEY, CENTRIC, Sheffield Hallam University, Sheffield, United Kingdom of Great Britain and Northern Ireland
PHILIPP AMANN, Former Europol, The Hague, Netherlands

Tracing cryptocurrency transactions is a far from trivial process. This likely explains the increasing utilisation by criminal networks for a significant amount of criminal activity, not just cybercrime, but any crime requiring monetary transfers [1]. It is, therefore, vitally important that adequate training exists and is readily available for both new and experienced investigators to ensure that they are familiar with the latest techniques, tools and trends. Traditional training methods can be costly and resource-intensive, requiring highly qualified trainers to give their time to conduct training sessions. To address this issue, a training resource, in the form of a serious game, has been created. The game aims at providing a platform to improve the skills and expertise of law enforcement officers whilst reducing the workload of experienced investigators. This article describes the collaborative design and development of the serious game Cryptopol in a partnership between Europol and CENTRIC, which is a multi-disciplinary and end-user focused Center of Excellence, located within Sheffield Hallam University. Cryptopol is the first cryptocurrency-tracing training game of its kind, used by over 1,500 people representing over 550 law enforcement agencies from across the world.

CCS Concepts: • **Software and its engineering → Collaboration in software development**;

Additional Key Words and Phrases: Cryptocurrency, blockchain tracing, serious games, law enforcement, training

Gert Jan van Hardeveld, Europol staff contributed to the article in a private capacity, expressing their own opinion which shall under no circumstances be considered to be that of Europol.

Authors' Contact Information: Paul John Hancock, CENTRIC, Sheffield Hallam University, Sheffield, United Kingdom of Great Britain and Northern Ireland; e-mail: p.hancock@shu.ac.uk; Gert Jan Van Hardeveld, Europol, The Hague, South Holland, Netherlands; e-mail: gert-jan.van-hardeveld@europol.europa.eu; Jarek Jakubcek, Former Europol, The Hague, South Holland, Netherlands; e-mail: jarek.jakubcek@binance.com; Babak Akhgar, CENTRIC, Sheffield Hallam University, Sheffield, United Kingdom of Great Britain and Northern Ireland; e-mail: b.akhgar@shu.ac.uk; Steffi Davey, CENTRIC, Sheffield Hallam University, Sheffield, United Kingdom of Great Britain and Northern Ireland; e-mail: steffi.davey@shu.ac.uk; Philipp Amann, Former Europol, The Hague, South Holland, Netherlands; e-mail: philipp.amann@post.at.

ACM 2832-5516/2024/11-ART32
https://doi.org/10.1145/3697845

ACM Reference Format:
Paul John Hancock, Gert Jan van Hardeveld, Jarek Jakubcek, Babak Akhgar, Steffi Davey, and Philipp Amann. 2024. Design of Cryptopol: A serious game for teaching cryptocurrency tracing techniques to Law Enforcement. *ACM Games* 2, 4, Article 32 (November 2024), 14 pages. https://doi.org/10.1145/3697845

1 Introduction

By operating without the oversight of central banks, cryptocurrencies innately provide a level of privacy and anonymity, presenting an appealing opportunity for criminal exploitation [2, 3]. Alongside this, the number of different types of cryptocurrencies in circulation is growing, providing further opportunities for criminals to hide their virtual trails. As most cryptocurrency transactions are open source and recorded on a distributed public ledger, it is possible for **law enforcement agencies** (**LEAs**) to carry out blockchain forensic investigations to trace the flows of money [3, 4]. However, the aforementioned factors can extend the current challenges for LEAs when it comes to tracing criminal activities.

In order to assist in the fight against criminal activity using cryptocurrency it is important for LEAs to have access to the latest technologies and trainings to ensure that they remain ahead of the game. Agarwal et al. propose a system which utilises **artificial intelligence** (**AI**) and **machine learning** (**ML**) algorithms to assist with blockchain investigations, which shows promising results for cryptocurrency investigations [5]. However, there are still many challenges to be addressed before this technology can be adopted by LEAs. Furthermore, it is likely that such technologies will be used to enhance human capabilities instead of replacing them [6]. Therefore, it is vital that adequate up-to-date training exists to ensure investigators understand both the trends in criminality and what tools and techniques are being used to effectively track and trace this activity, and, ultimately, conduct efficient and effective investigations. Training is also required to safeguard the evidential value of cryptocurrency investigations [25].

For many investigators, cryptocurrency is a completely new and technical field that presents many challenges to fully understand. Tziakouris identifies core challenges that LEAs face regarding cryptocurrency crimes and investigations, highlighting the importance of innovative hands-on training [7]. In 2021 Taylor et al. responded to this by conducting a survey investigating the perceived efficacy of current cryptocurrency forensics training. The results showed that 96.7% of the digital forensic investigators questioned either agreed or strongly agreed that current training practices were insufficient [8].

With the recent rise in crimes involving cryptocurrencies [3] it is predicted that there will be an increase in demand for trained investigators. Therefore, training must be easily distributable to mass audiences. Training should draw upon past experiences of professional investigators and should be easy to update when new trends are exposed. To address these training needs, a novel online serious game, Cryptopol, has been developed to investigate the efficacy of this approach in providing a solution to the identified challenges. Serious games have been shown to achieve positive results when compared to traditional training methods, whereby in some instances serious games were seen to be more effective than traditional lecture-based tuition [9, 10].

While alternative cryptocurrency trainings are available, provided by developers of blockchain analytics tools, these are strongly focused on the promotion of commercial tools. Cryptopol is a novel, agnostic, free tool developed exclusively for the law enforcement domain, void of influence from commerce. Cryptopol is currently the only cryptocurrency-focussed serious game for law enforcement. To date, Cryptopol has trained over 1,500 investigators, representing over 550 LEAs, showing a distinct demand for such a resource. As it is free, it is accessible for investigators from

all kinds of agencies (local to federal) enabling training of personnel that would normally not have access to alternative expensive tools, ultimately increasing opportunities to improve and expand LEA capabilities in tracing cryptocurrencies.

This article provides an exposition around the field of serious games and explores trends around criminal activity where cryptocurrencies are used. The results of this are then used as the basis for defining the concept of a serious game to provide free training to LEAs, where the identified tools and techniques can be introduced. This is followed by a description of the design and development process of an online training application. Finally, the method of deployment for the resulting serious game is described along with defining the steps taken to validate the effectiveness of the resulting training application.

2 What Are Serious Games?

Games have historically been used to convey concepts, reinforce knowledge, or learn new skills. Serious games are designed to capitalise on this behaviour by utilising modern computer game technology. The differentiator between games and serious games is the definition of their core purpose. A serious game is designed to respond to a functional need, to train, educate or raise awareness, whereas standard games are built purely for entertainment purposes [11].

Serious games are gaining popularity, empirical evidence shows that they can increase knowledge acquisition [12]. Games-based learning can be considered a type of problem-based learning which demonstrates that learning is most effective when it poses significant, contextualised, real-world situations and provides resources, guidance, and instructions to help develop both content knowledge and problem-solving skills [13]. Serious games can also provide a cost-effective alternative to real-life training events. Game mechanics help to encourage and motivate the user to engage with the learning activity and require the user to apply their knowledge in order to succeed in the game [14].

Serious games are particularly helpful for LEAs: They can be used to create realistic scenarios to assist with situational awareness in order to enable understanding, enhance learning and gain new insights into how to manage a problem-solving process in the context of police operations [15].

By focusing on realism and experiential learning, serious games are powerful tools to facilitate knowledge acquisition processes within LEAs, where knowledge gained, whilst playing the game, can be applied to an actual operational environment. By simulating a real-world situation, serious games train knowledge and skillsets that investigators require before they experience real-life situations first-hand. Serious games can also be beneficial to more experienced personnel [16]. As most experienced officers are used to working in the field under time constraints, there is a chance that they may develop undesirable habits or shortcuts, which may lead to mistakes being made or cause inefficiencies in working practices. (It is important to note that this trait is not exclusive to officers, as research has shown that criminals are also prone to taking shortcuts and making common mistakes [17]. Understanding these shortcuts and mistakes can be an important step in tracing criminal activity.)

A serious game can provide officers with the chance to reassess their current knowledge and methodologies to develop alternative methods in response to the constraints of their job and, most importantly, learn from their mistakes in a safe and secure environment.

3 Crime Related to Cryptocurrency

Criminals are increasingly being drawn towards cryptocurrencies due to the perceived anonymity of financial transactions that they provide. As a result of this, cryptocurrencies are widely used by criminals as a preferred means of payment for illegal goods and services offered both online and

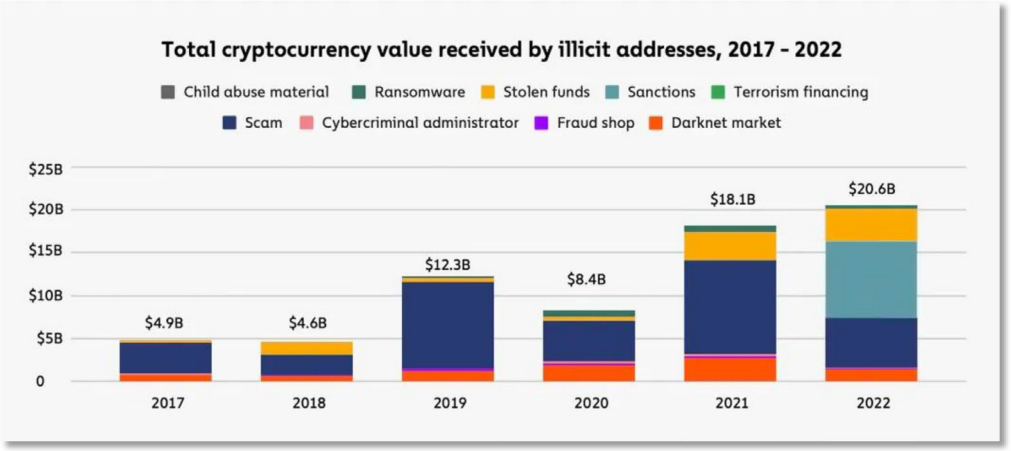

Fig. 1. Illicit transaction volumes [18].

offline [18]. Known crimes involving cryptocurrencies include fraud, ransomware, scams, drug trafficking, and even payments for child abuse material and terrorism financing.

In 2022, according to Chainalysis, illicit transaction volumes reached an all-time high of $20.68 billion. Figure 1 shows how the total value of illicit transactions has increased since 2017. It is important to note that this data is based only on illicit entities identified by Chainalysis, which is an American blockchain analysis firm. Neither Chainalysis nor any other cryptocurrency tracing company has a perfect dataset, their identified clusters and tags therefore do not represent all illicit entities, partially due to not having access to law enforcement information. Hence, Figure 1 is likely an underestimation of the true scale of illicit transactions.

In recent years there has been an increase in ransomware attacks, which is a trend that is still continuing. Ransomware groups have attacked numerous large enterprises, including operators of critical infrastructure; one example of this being an attack on the US pipeline operator Colonial Pipeline which led to temporary fuel supply shortages [19].

According to Chainalysis, in 2020, the total amount paid in cryptocurrency by ransomware victims showed an annual increase of 311%, reaching nearly $350 million. In the first five months of 2021, ransomware attackers received cryptocurrency valued at $81 million from victims. This figure is certain to rise significantly as more wallet addresses are identified as being involved in ransomware attacks [20].

It should also be noted that ransomware estimates and reported figures are likely to be lower than the actual value, not only due to incomplete datasets, as mentioned previously but also due to underreporting by victims [21]. Further to this, ransomware attacks are disruptive and destructive in that they can cripple governments, businesses and critical infrastructure for significant amounts of time. It is, therefore, also important to consider the total economic losses not just from payments but from businesses and governments being taken offline in attacks.

In order to obtain an accurate picture of the true patterns relating to cryptocurrency crimes, it is important to look at more than one source. This is primarily due to the reasons previously identified, whereby each source will base their conclusions on incomplete datasets. To ensure that the trends identified in the Chainalysis report are accurate, the annual report from another blockchain analysis company called Elliptic was also analysed. The report from Elliptic looks at cross-chain crime, which relates to a way of laundering cryptocurrency by transferring assets across different blockchains by swaps or cross-chain bridges.

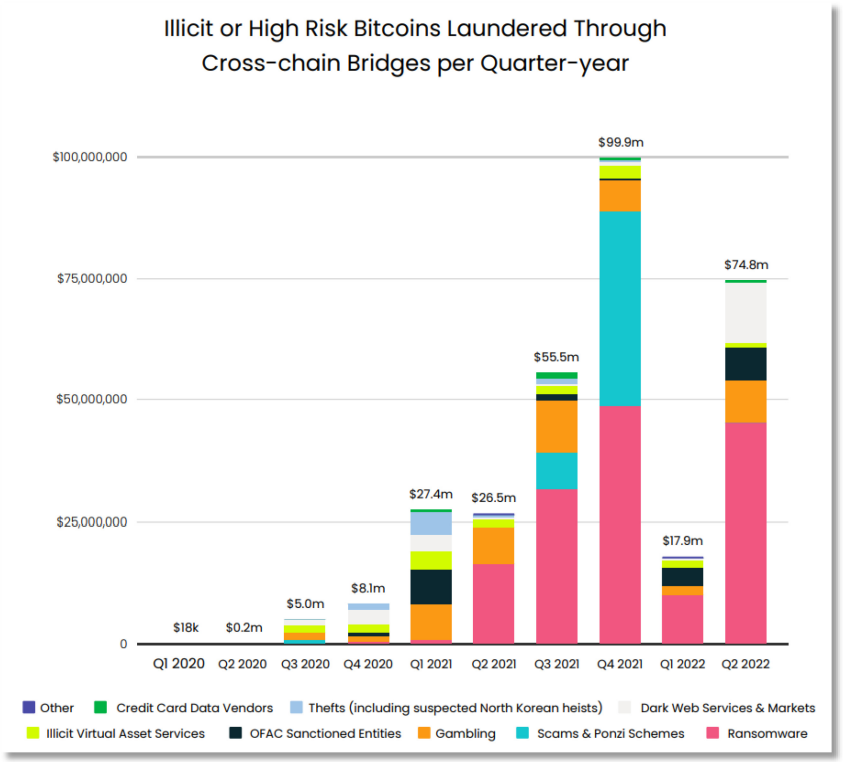

Fig. 2. Illicit Bitcoins laundered 2020-2022 [22].

Figure 2 shows the value of crimes relating to Bitcoin from the start of 2020 until the end of the 2nd quarter of 2022. Whilst this timeframe does not allow for a comparison with the data provided by Chainalysis, it is possible to compare the trends identified, primarily that ransomware is an increasingly damaging crime [22].

It is also important to note that, according to Europol, the criminal use of cryptocurrency is no longer primarily confined to cybercrime activities, but now relates to all types of crime. An example of this is money laundering networks, which specialise in large-scale money laundering as-a-service. These networks have been seen to adopt cryptocurrencies and then offering their services to other criminals [1].

4 How Can Transactions Be Traced?

Blockchains, as utilised by the majority of cryptocurrencies, store the complete historical records of financial transactions publicly. Traditionally, if investigators wanted to perform an investigation, they would need to download a copy of the blockchain as raw data and then perform manual analysis [23]. However, this has been greatly simplified by blockchain explorers, which removes the complexity of downloading and analysing the blockchain.

4.1 Blockchain Explorers

Blockchain explorers provide access to details related to transactions on specific wallet addresses and blockchains. One of the first public blockchain explorers for Bitcoin was provided by a company called Blockchain.com. It was introduced in 2011 and was used to explore the Bitcoin blockchain [24].

Blockchain explorers allow investigators to extract data related to transactions, wallets, and blockchains. Users are able to explore transaction histories by searching for a wallet address or transaction ID. By searching for an address, the user is able to see the current balance and a list of all transactions made to and from this address. By searching for a transaction ID, the user can see which addresses cryptocurrency was transferred to and from and the quantity of currency that was transferred.

4.2 Tracing Tools

In addition to Blockchain explorers, there are also tracing tools. Tracing tools tag entities by translating their pseudonymous addresses into real-life entities. Once entities have been tagged, they can be grouped together by applying clustering algorithms to identify wallet addresses belonging to the same owner. The user is shown a visual representation of the link between addresses along with the tags that have been identified for entities, where possible. These tags are crucial, as they can, for example, identify that a wallet address is associated with 'ransomware family x' or 'exchange y'.

Tracing tools also attempt to identify the controlling entity of a cluster, which could for example be an exchange or a more suspicious entity, like a darknet market or a ransomware wallet. Once this has been achieved, transactions between a series of previously seemingly random wallet addresses are now displayed to the user as interactions between real-world entities.

The rapid adoption of cryptocurrency by criminals across all types of crime has created a clear need for law enforcement officers to learn how to trace cryptocurrencies. This is not limited to cybercrime investigators but is of relevance for all types of investigators in a wide range of fields such as tax, terrorism financing, child sexual abuse material, money laundering, fraud, organised crime, and so on.

5 Rationale for an LEA Training Game

Between 2014 and 2018, Europol experts received an increasing number of requests for assistance in tracing cryptocurrency. This coincided with an increasing number of requests for in-person training around cryptocurrency. To address this demand, Europol delivered on-site events including conferences and meetings between law enforcement and cryptocurrency exchanges, as well as hands-on training sessions. Additionally, Europol's experts have delivered many training sessions worldwide. While these training sessions were effective and received very positive feedback, the EU agency could not train every interested officer in the EU and beyond.

This increase in requests for assistance led to the idea to create a practical, yet scalable, training application, as an online resource that can be played by any law enforcement officer from the EU and Europol's partners. The potential advantage of this online resource is that investigators would be able to play the game whenever they wanted and from any location.

6 Concept

The application developers, CENTRIC, were approached by Europol's European Cybercrime Centre to collaboratively develop a training resource exclusively for use by LEAs, to educate investigators in tracing and analysing cryptocurrency transactions.

A senior investigator from Europol provided an introduction to the techniques and tools which are used by trained officers to trace cryptocurrency transactions. This introduction led to the basic idea for the training application.

Working together, CENTRIC and Europol developed the first version of the training game 'Cryptopol', which was launched in 2019. An agile approach was adopted for the creation of the game.

This approach is widely used in software development as it ensures end-user satisfaction through regular communication. Additionally, it is reported to be an effective method for small serious game development teams [26].

The focus of the initial version of the game was primarily to teach investigators and prosecutors how to obtain relevant evidence from blockchains for a successful cryptocurrency investigation. With this purpose in mind, it was decided that real-world cases would be presented during the game to practice investigation skills. To achieve the teaching objectives, transactions in the blockchain would need to be analysed by using both free and commercial tools.

7 Game Design

A variety of different styles of training applications were considered and evaluated based on analysing previously developed serious games.

After consultations with law enforcement investigators, it was decided that the most suitable format for the game would be a quiz-style application with questions split into scenarios. Initially, the user would be guided through scenarios based on the theory of tracing cryptocurrency transactions before transitioning to scenarios based on the recreation of real investigations.

It was important that users would be required to use real tools to answer questions to ensure that all training outcomes were relevant. It was also decided that it would be beneficial if users were shown a video demonstrating what is believed to be the best method to find the answer for each question, once the user has provided their answer. This way, even if the user provides a correct answer, they can still improve their techniques.

This method of learning, based on social learning theory, has been proven to be very effective. Social learning theory suggests that observation of others plays a primary role in how and why people learn. Social learning can be used effectively in the workplace to observe and model productive behaviours [27]. In this way, the full demonstration that the user can see of an experienced investigator solving each problem using the latest tools and techniques provides a powerful learning tool.

8 Implementation

Based on the requirements and design concept, the Unity game engine was chosen to develop the training application. Since Unity is a cross-platform engine, the application could be deployed either as a web-based application or a PC/Mac application. It also allows for the possibility of developing a mobile version of the training application in the future.

Another consideration was how to develop the content for the scenarios. An important design decision was that the game should teach users the correct methods for solving problems, alongside providing an assessment of their current knowledge and abilities. Another key requirement was that the game should guide users through realistic and challenging scenarios, to ensure that all investigators, whether they are new to tracing cryptocurrency transactions or have many years of experience in this field, would receive valuable training.

The decision to split the game into multiple scenarios allows users to break their training into multiple sessions, whereby they may want to complete one scenario per session, or they may want to play for a set period of time. This is left entirely to the user's discretion and their learning preferences, offering flexibility in how users interact with the training game.

Once these basic requirements for the training application had been established, it was decided that the application would be developed as a typical client-server solution, with a WebGL frontend underpinned by WebAssembly (WASM), as this allows for good portability without the need to install any software locally.

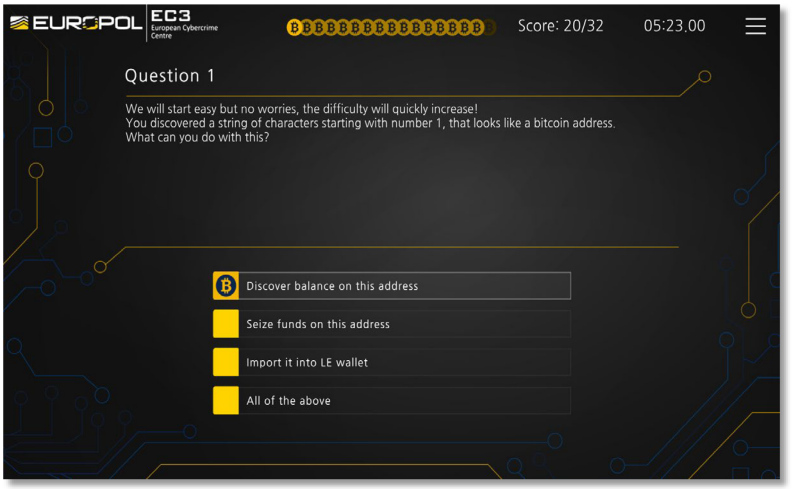

Fig. 3. An early question.

8.1 Scenario Types

The game begins with what are considered to be training scenarios. The questions in these scenarios often resemble more quiz-like questions, where the user's knowledge of cryptocurrency is tested. As with every scenario in the game, the questions in the training scenarios are followed by videos explaining the correct answer. This ensures that all users have a good understanding of the basic concepts once they have completed this section of the game.

Once the training section of the game has been completed, the user is provided with scenarios containing recreations of real investigations. Some of the questions in these scenarios still follow the quiz style but generally, the user is required to use external tracing tools and blockchain explorers in order to find the answers. These questions generally require the user to trace a transaction or find a cryptocurrency address. An example of a simple quiz-style question is shown in Figure 3.

For most questions, the user is asked to select the correct answer from a list, but there are also questions where the user is required to enter the correct answer into a text box, as shown in Figure 4. Once a response has been submitted, or the "Give up" button has been pressed, a feedback video is played explaining the correct way to answer the question, in the same way that feedback is proved to the more common multiple-choice questions.

8.2 Scoring

In order to assess users' performance, it was crucial to provide a scoring mechanism. Scoring is an important method of providing feedback to users, so they can assess whether there are any specific areas in which they are weaker than others and can target any further training in these areas. It was decided that the server should be responsible for calculating and storing each users' score, so as to maintain accuracy and prevent users' scores from being reset if they switch the device they have been using to play the game.

Only the first attempt a user makes at answering a question is scored. Accordingly, any incorrect answers result in a score of 0 for that question. The only exception to this rule is for questions that require the answer to be typed as opposed to selecting a response from a list. For the text entry questions, the user is allowed five attempts to type the correct answer, to allow for any typing

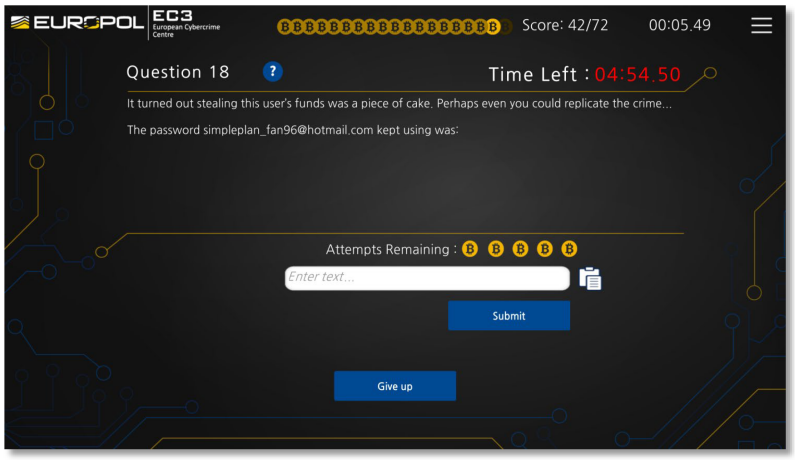

Fig. 4. Example of a text entry question.

Fig. 5. Example of a hint.

mistakes. Each of these attempts is awarded the same score if the user enters the correct answer. The maximum score for answering a question correctly is 2 points in the training scenarios and 4 points in the scenarios based on reconstructions of real cases. Many of the questions feature a time limit. Where this is the case, failure to answer a question within the allotted time results in the score being halved (therefore, making the scores available when the time limit has expired 1 point for training scenarios and 2 points for reconstructed case scenarios). There are also hints available for some questions, which the user can choose to view if they are unsure of the answer. An example of this can be seen in Figure 5. Hints are not available for every question, but when they are provided, the user will lose 1 point if they choose to view them.

The game also features a ranking system: as the user earns points by answering questions correctly, their rank will increase. This is to provide a feeling of progression and accomplishment and aims at encouraging all users to play through all available scenarios to try and achieve the highest rank they can.

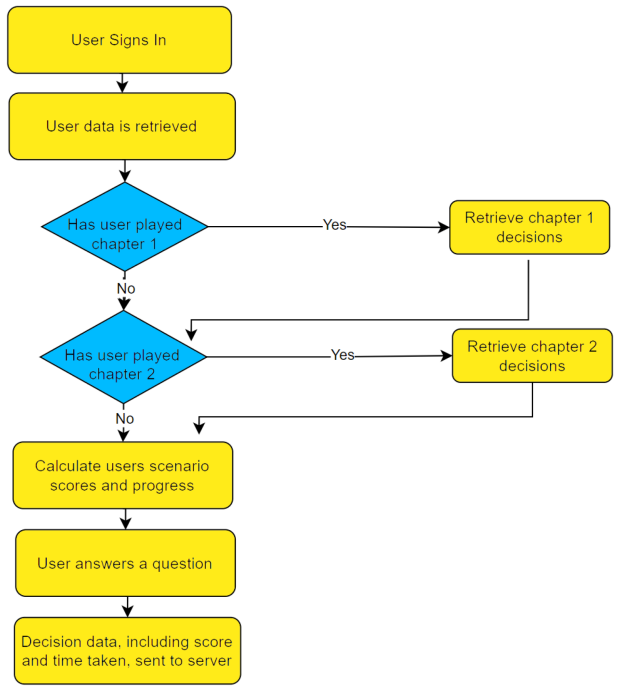

Fig. 6. High-level flow diagram.

Another reason for tracking the score for each user is so that certificates can be awarded to every user who achieves a score above a pre-defined threshold value. These certificates are automatically generated and sent to the user via their registered e-mail address and state that the user has successfully completed the serious game.

8.3 Leaderboard

A leaderboard is included in the game to allow users to compare their scores with their peers. The leaderboard ranks users by their total scores achieved on all of the scenarios they have attempted. In the event of a tie, the total time a user has spent making decisions is used, whereby the user who has taken the least time is ranked first.

8.4 Server Communication

As the game is exclusively for use by LEAs, users need to register before they are able to access the game. Users have to enter their e-mail address when registering and are then sent an e-mail which allows them to set a password. This allows for the domain in the users e-mail address to be checked against a whitelist of allowed domain names.

Whenever a user answers a question, decision data is sent to the game server to both provide data for the global scoreboard and for users to be able to restore their progress when they next sign into the game. The decision data contains a unique ID for the question that has been answered along with the score the user achieved and the time taken for that question.

Figure 6 shows a high-level flow diagram, which indicates how the game interacts with the server after the user signs into the game.

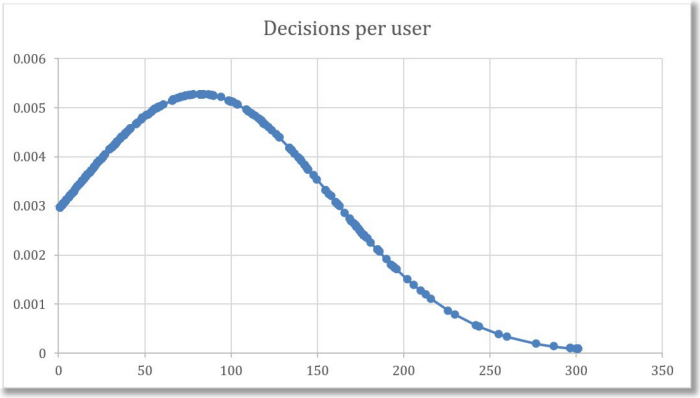

Fig. 7. Graph showing decisions made by users.

9 Deployment and Validation

9.1 User Numbers

The first iteration of the game was released in 2019. In April 2023, an updated version of the game, titled Cryptopol 2.0, was launched during a joint presentation by CENTRIC and Europol at the 2023 Europol Virtual Currencies Conference.

Whereas the original selection of scenarios in the initial game version mainly focuses on Bitcoin, the Cryptopol 2.0 selection of scenarios focuses on Ethereum, **Decentralised Finance** (**DeFi**), **non-fungible tokens** (**NFTs**) and more. These were included due to an increasing number of requests by investigators. This update introduced a chapter system, which makes the game easy to expand, as it is highly likely that new chapters will continue to be added to the game so that new cryptocurrencies and new tracing tools and techniques can be introduced. The Cryptopol 2.0 update demonstrates how the serious game can evolve over time to match any new threats.

At the time of writing, more than 1,500 people from 50 countries across the world, representing over 550 LEAs have trained using the game.

9.2 Usage Evaluations

Figure 7 shows a graph of the number of decisions made by each user, with a mean average of over 82 decisions per user. In this graph, the *X*-axis relates to the number of decisions, while the *Y*-axis shows the density of probability, which represents the chance of obtaining values near corresponding points on the *X*-axis.

Figure 8 shows the distribution of user scores achieved in the first chapter of the game (which includes all scenarios available when the game first launched in 2019), with a mean average of over 122 points per user. The *X*-axis in this graph relates to the total scores achieved by users in the original chapter 1 scenarios, with the *Y*-axis relating to the density of probability, as per the previous graph.

Evaluating this data shows that one in five users have answered all 173 questions that form the first chapter and 15% of users, who have played this chapter, were awarded a certificate. A certificate requires that all scenarios are completed with a total score above 60%. At the time of writing, chapter 2 had only recently been released. Therefore, a similar evaluation is not possible but similar figures are expected. This data shows excellent user retention: Despite the considerable

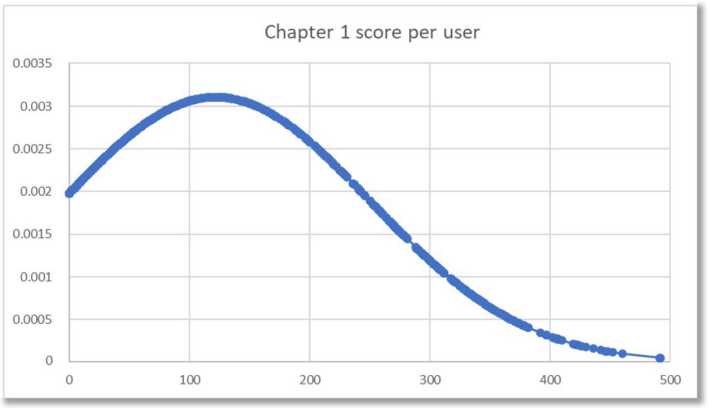

Fig. 8. Graph showing scores achieved for chapter 1.

amount of time required to complete every scenario, a significant number of users have done so and have generally achieved excellent scores which shows the effectiveness of the training platform.

In order to further validate the effectiveness of the Cryptopol training application, multiple investigators in LEAs were asked about their and their team's experience of playing Cryptopol. Some example responses are listed below:

> "The effort put into Cryptopol by leading figures in the field makes the material challenging and also very relevant in day-to-day investigations." Investigator – The Netherlands

> "Cryptopol (2.0) enhanced my cryptocurrency knowledge from previous trainings and job experience. It focused on some of the most discussed and difficult cryptocurrency cases. I consider Cryptopol as one of the best training experiences for cryptocurrency investigations." Investigator – Italy

> "Cryptopol is a vital tool in helping UK CT Policing develop their skills in track and tracing cryptocurrency to help detect, disrupt and deter subjects of interest. It is the only tool of its kind where we can develop our skills in technical areas we have not yet come across, ensuring our investigators are ready for any crypto challenge before it is required in the field." Former Acting Detective Sergeant – Police, UK.

Another indicator of Cryptopol's success is that the suppliers of leading commercial cryptocurrency tracing tools offer free trial licenses to players, indicating that they recognise the value of Cryptopol.

10 Discussion and Conclusion

The purpose of Cryptopol is to make the entry into cryptocurrency investigations easier, by introducing gamified scenarios based on real-life cases. Explanatory videos enable investigators to learn from and mimic the work of a successful cryptocurrency investigator. Cryptopol has been used to train over 1,500 investigators, demonstrating a clear demand for such a tool which is now used by LEAs worldwide.

Tracing cryptocurrency is vital and will continue to increase in importance given the criminal trends identified. The ever-increasing need for investigators to obtain skills in cryptocurrency investigations is a clear rationale behind the decision to design Cryptopol.

Overall, Cryptopol demonstrates the value of training games for the law enforcement domain and the importance of creating training games in close collaboration with expert end-users.

References

[1] Europol. 2022. Cryptocurrencies: Tracing the evolution of criminal finances. Retrieved October 15, 2024 from https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances, 2022.

[2] S. A. Raza, M. Shaikh, and K. Tahira. 2023. Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances. *Information Dynamics and Applications* 2, 3 (2023), 126–134.

[3] S. Kethineni and Y. Cao. 2019. The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review* 30, 3 (2019), 325–344.

[4] A. Trozze, J. Kamps, E. A. Akartuna, F. J. Hetzel, B. Kleinberg, T. Davies, and S. D. Johnson. 2022. Cryptocurrencies and future financial crime. *Crime Science* 11, 1 (2022), 1–35. DOI: https://doi.org/10.1186/s40163-021-00163-8

[5] U. Agarwal, V. Rishiwal, S. Tanwar, and M. Yadav. 2023. Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management* 34, 2 (2023), 1–32. DOI: https://doi.org/10.1002/nem.2255

[6] H. Hassani, E. S. Silva, S. Unger, M. TajMazinani, and S. Mac Feely. 2020. Artificial intelligence (AI) or intelligence augmentation (IA): What is the future?, *AI* 1, 2 (2020), 143–155. DOI: https://doi.org/10.3390/ai1020008.

[7] G. Tziakouris. 2018. Cryptocurrencies—a forensic challenge or opportunity for law enforcement? An INTERPOL perspective. *IEEE Security and Privacy* 16, 4 (2018), 92–94. DOI: https://doi.org/10.1109/MSP.2018.3111243

[8] S. K. Taylor, M. S. M. Omar, N. Noorashid, A. Ariffin, K. A. Z. Ariffin, and S. N. H. S. Abdullah. 2021. People, process and technology for cryptocurrencies forensics: A malaysia case study. In *Proceedings of the Advances in Cyber Security*. M. Anbar, N. Abdullah, and S. Manickam, (Eds.), Singapore: Springer Singapore, 297–312.

[9] J. Saunders, S. Davey, P. S. Bayerl, and P. Lohrmann. 2019. Validating virtual reality as an effective training medium in the security domain. In *Proceedings of the IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 1908–1911. DOI: https://doi.org/10.1109/VR.2019.8798371.

[10] A. Rahouti, R. Lovreglio, and S. Datoussaïd. 2021. Prototyping and validating a non-immersive virtual reality serious game for healthcare fire safety training. *Fire Technology* 57, 6 (2021), 3041–3078. DOI: https://doi.org/10.1007/s10694-021-01098-x

[11] D. Djaouti, J. Alvarez, JP. Jessel, and O. Rampnoux. 2011. Origins of serious games. In *Proceedings of the Serious Games and Edutainment Applications*. M. Ma, A. Oikonomou and L. C. Jain, (Eds.), Springer, London, (2011)

[12] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, and J. M. Boyle. 2012. A systematic literature review of empirical evidence on computer games and serious games. *Computers and Education* 59, 2 (2012), 661–686.

[13] E. Boyle, T. M. Connolly, and T. Hainey. 2011. The role of psychology in understanding the impact of computer games. *Entertainment Computing* 2, 2 (2011), 69–74.

[14] S. Arnab, T. Lim, M. B. Carvalho, F. Bellotti, S. de Freitas, S. Louchart, N. Suttie, R. Berta, and A. De Gloria. 2015. Mapping learning and game mechanics for serious games analysis. *British Journal of Educational Technology* 46, 2 (2015), 391–411.

[15] B. Akhgar, A. Redhead, S. Davey, and J. Saunders. 2019. Introduction: Serious games for law enforcement agencies. In *Proceedings of the Serious Games for Enhancing Law Enforcement Agencies*. Security Informatics and Law Enforcement, B. Akhgar, (Eds.). Springer (2019), 1–11.

[16] A. BinSubaih, S. Maddock, and D. Romano. 2009. Developing a serious game for police training. In *Proceedings of the Handbook of Research on Effective Electronic Gaming in Education*. 451–477.

[17] G. Van Hardeveld, G. Webber, and K. O'Hara. 2017. Deviating from the cybercriminal script: Exploring tools of anonymity (mis)used by carders on cryptomarkets. *American Behavioral Scientist* 61, 11 (2017), 1244–1266.

[18] Chainalysis. 2023. The 2023 crypto crime report. Retrieved October 15, 2024 from https://go.chainalysis.com/2023-crypto-crime-report.html

[19] A. Alper. 2021. Biden sanctions cryptocurrency exchange over ransomware attacks. Retrieved October 15, 2024 from https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21

[20] Chainalysis. 2021. Ransomware 2021: Critical mid-year update [REPORT PREVIEW]". Retrieved October 15, 2024 from https://blog.chainalysis.com/reports/ransomware-update-may-2021

[21] Chainalysis. 2020. Ransomware skyrocketed in 2020, but there may be fewer culprits than you think. Retrieved October 15, 2024 from https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

[22] Elliptic. 2022. Elliptic cross-chain report 2022. *The State of Cross-chain Crime*. 2022. https://www.elliptic.co/resources/state-of-cross-chain-crime-report
[23] M. E. Peck. 2019. What's in a blockchain? with new tools, anyone can find out". Retrieved October 15, 2024 from https://spectrum.ieee.org/whats-in-a-blockchain-with-these-new-tools-anyone-can-find-out
[24] Blockchain.com. 2011. Relentlessly building the future of finance since 2011. Retrieved October 15, 2024 from https://www.blockchain.com/about
[25] M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert, and P. Pesch. 2020. Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation* 33, 200902 (2020), 200902–200916. DOI: https://doi.org/10.1016/j.fsidi.2019.200902
[26] R. R. Zamora, I. A. S. Hernandez, and L. A. E. Nunez. 2018. Development serious games using agile methods. test case: Values and attitudinal skills. In *Proceedings of the Telematics and Computing: 7th International Congress*.
[27] A. Bandura. 1977. *Social Learning Theory*. Prentice-Hall.

Received 1 April 2024; revised 23 August 2024; accepted 27 August 2024