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

Abstract— **Tracing cryptocurrency transactions is a far from trivial process. As a significant amount of criminal activity involves the use or abuse of cryptocurrency it is vitally important that adequate training exists for both new and experienced investigators to ensure that they are familiar with the latest techniques, tools and trends. This paper describes the collaborative design and development of a training resource in the form of a serious game that aims to improve the skills and expertise of law enforcement officers in this area.**

Keywords—cryptocurrency, blockchain tracing, serious games, law enforcement, training

I. Introduction

In order to assist in the fight against criminal activity using cryptocurrency it is important that adequate training exists to ensure investigators understand both the trends in criminality and what tools and techniques exist, in order to track and trace this activity, and, ultimately, conduct efficient and effective investigations.

This paper 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 law enforcement agencies, 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.

II. 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 [1].

Serious games are gaining popularity as empirical evidence shows that they can increase knowledge acquisition [2]. Games-based learning can be considered a type of problem-based learning which has demonstrated 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 [3]. 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 [4].

Serious games are particularly helpful for law enforcement agencies (LEAs): They can be used to create realistic scenarios to assist with situational awareness in order to enable understanding, enhance learning and also gain new insights into how to manage a problem solving process in the context of police operations [5].

By focussing 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 have to experience real-life situations first-hand. Serious games can also be beneficial to more experienced personnel [6]. 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, that may lead to mistakes being made or 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 [7]. Understanding these shortcuts and mistakes can be an important step to tracing criminal activity.

A serious game can provide officers with the chance to reassess their current knowledge and methodologies and 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.

III. 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 offline [8]. Known crimes involving cryptocurrencies include fraud, ransomware, scams, drug trafficking, and even payments for child abuse material and terrorism financing.

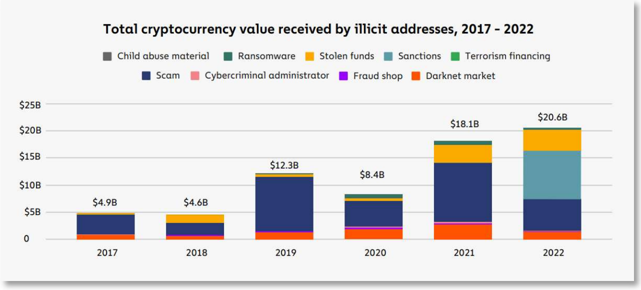


Figure 1 - Illicit transaction volumes [9]

In 2022, according to Chainalysis, illicit transaction volumes reached an all-time high of $20.68 billion. Figure 1 shows how the total value has increased since 2017. It is important to note that this data is based only on illicit entities identified by Chainalysis, who are an American blockchain analysis firm. Neither Chainalysis, or 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 under-estimation of the true scale of illicit transactions.

In recent years there has been an increase in ransomware attacks, which is a trend which 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 [10].

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. However, this figure is certain to rise significantly as more wallet addresses are identified as being involved in ransomware attacks [11].

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 [12]. Also, 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.

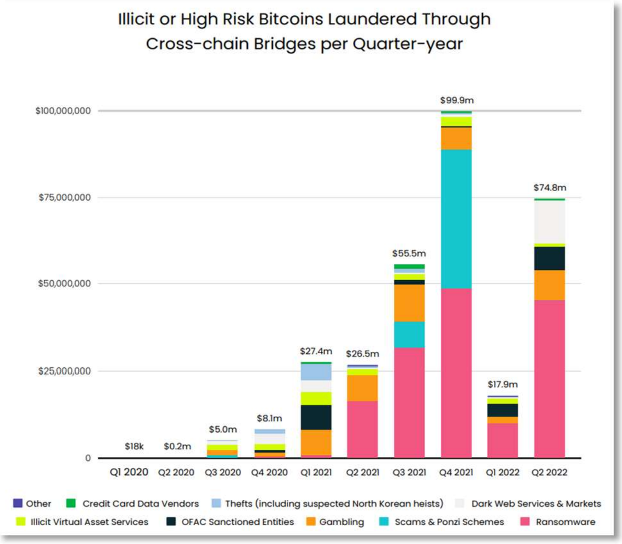


Figure 2 – Illicit Bitcoins laundered [13]

In order to acquire 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. In order 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.

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 [13].

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, who 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 [8].

IV. How can transactions be traced?

Blockchains, as utilised by the majority of cryptocurrencies, store the complete historical records of financial transactions publicly.

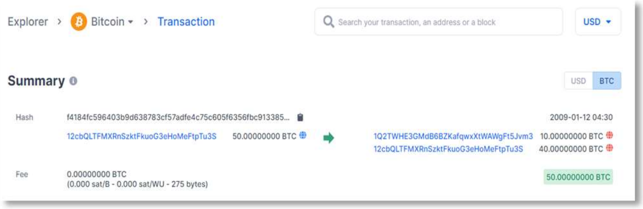
Traditionally, if investigators wanted to perform an investigation, they would need to download a copy of the blockchain as raw data and then perform manual analysis [14].

However, this has been greatly simplified by blockchain explorers, which remove the complexity of downloading and analysing the blockchain.

A. Blockchain explorers

Blockchain explorers provide access to details related to transactions on specific wallet addresses and blockchains. The first blockchain explorer for Bitcoin was provided by a company called Blockchain.com. It was introduced in 2011 and was used to explore the Bitcoin blockchain [15].

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.


Explorer › Bitcoin › Transaction
Search your transaction, an address or a block
USD
Summary
USD
BTC

Hash f4184fc596403b9d638783cf57adfe4c75c605f6356fbc913385... 2009-01-12 04:30

12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S 50.00000000 BTC → 1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3 10.00000000 BTC
12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S 40.00000000 BTC

Fee 0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 275 bytes) 50.00000000 BTC

Figure 3 – Bitcoin transaction

Figure 3 shows the result of a Bitcoin transaction in the Blockchain.com blockchain explorer. The wallet addresses of the sender and receiver are shown, along with the transaction fee and the timestamp created when the transaction took place.

B. 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 then be grouped together by applying clustering algorithms to identify wallet addresses belonging to the same owner. The user is able to see 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' [16].

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 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 etc.

V. Rationale for an LEA Training Game

Law enforcement agencies have received a growing number of requests for assistance in tracing cryptocurrency. To address this demand, LEAs require better access to on-site events such as conferences and meetings between law enforcement and cryptocurrency exchanges, as well as hands-on training sessions. While in-person training sessions can be effective, time and resource restrictions mean that in-person trainings cannot reach 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 used by any law enforcement officer from the EU and worldwide. The potential advantage of this online resource is that investigators would be able to train whenever they wanted to and from any location.

VI. Concept

The application developers were approached by a law enforcement partner to collaboratively develop a training resource exclusively for use by LEAs, to educate investigators in tracing and analysing cryptocurrency transactions.

A senior investigator from the law enforcement partner provided an introduction into 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, the application development team and the law enforcement partner developed the first version of the training game 'Cryptopol', which was launched in 2019.

The focus for 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. For this purpose, real-world cases are presented during the game to practice investigation skills. To achieve the teaching objectives, transactions in the blockchain are required to be analysed by using both free and commercial tools.

VII. Game Design

A variety of different styles of training applications were considered and evaluated, based around 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 around the theory of tracing cryptocurrency transactions before transitioning to scenarios based around recreations of real investigations.

It was important that users would be required to use real tools in order to answer questions to make sure 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 has been proven to be very effective. Renowned psychologist Albert Bandura introduced the social learning theory, which 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 [17]. 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.

VIII. Implementation

Based on the requirements and design concept, it was decided to develop the training application using the Unity game engine. Since Unity is a cross-platform engine, the application could be deployed either as a web-based application or a PC/Mac application. This approach 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 as well as 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 up 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.

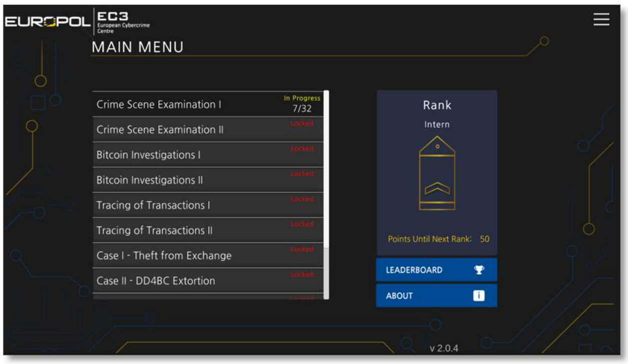
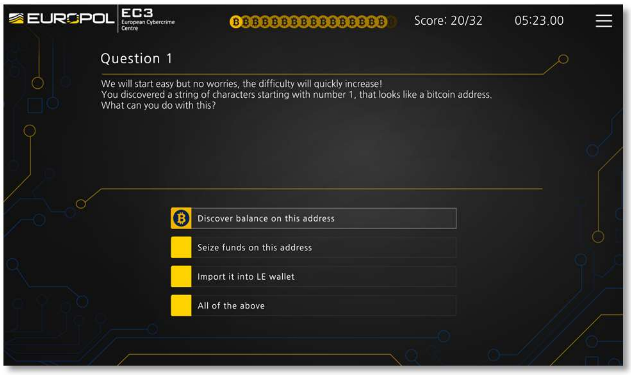

EUROPOL
EC3
European Cybercrime Centre
MAIN MENU
Crime Scene Examination I
In Progress
7/32
Crime Scene Examination II
Locked
Bitcoin Investigations I
Locked
Bitcoin Investigations II
Locked
Tracing of Transactions I
Locked
Tracing of Transactions II
Locked
Case I - Theft from Exchange
Locked
Case II - DD4BC Extortion
Locked
Rank
Intern
Points Until Next Rank: 50
LEADERBOARD
ABOUT
v 2.0.4

Figure 4 – Main menu

A. *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 users' 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 based around 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 5.


EUROPOL
EC3
European Cybercrime Centre
Score: 20/32
05:23.00
Question 1
Discover balance on this address
Seize funds on this address
Import it into LE wallet
All of the above

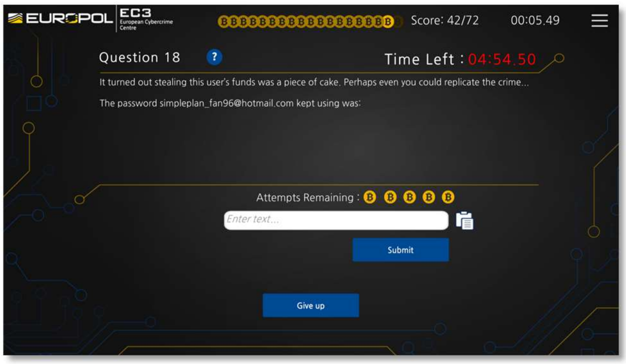
We will start easy but no worries, the difficulty will quickly increase!
You discovered a string of characters starting with number 1, that looks like a bitcoin address.
What can you do with this?

Figure 5 - An early question

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 6. Once an answer 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 provided to the more common multiple-choice questions.

B. *Scoring*

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

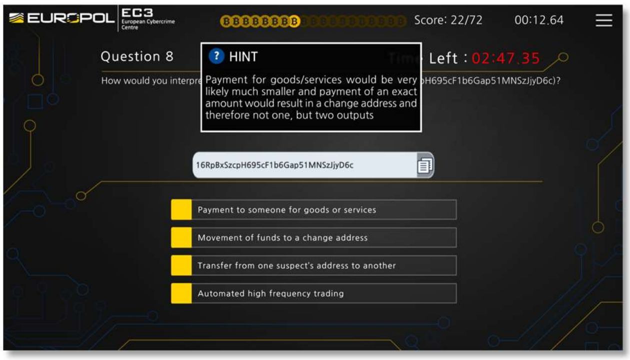


It turned out stealing this user's funds was a piece of cake. Perhaps even you could replicate the crime...

The password simpleplan_fan96@hotmail.com kept using was:

Figure 6 - Example of a text entry question

Only the first attempt a user makes at answering a question is scored, so any incorrect answers result in a score of 0 for that question. The only exception to this rule is with the questions that require the answer to be typed as opposed to selecting an answer from a list. For the text entry questions, the user is allowed 5 attempts to type the correct answer, to allow for any typing 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. When this is the case, failure to answer a question within the allotted time results in the score being halved (therefore reducing the scores available when the time limit has expired to 1 point for training scenarios and 2 points for reconstructed case scenarios). There are also hints available on 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 7. Hints are not available for every question, but when they are provided, the user will lose 1 point if they choose to view them.


EUROPOL
EC3
European Cybercrime Centre
Score: 22/72
00:12.64
Question 8
HINT
Left : 02:47.35
Payment to someone for goods or services
Movement of funds to a change address
Transfer from one suspect's address to another
Automated high frequency trading

How would you interpre

Payment for goods/services would be very likely much smaller and payment of an exact amount would result in a change address and therefore not one, but two outputs

H695cF1b6Gap51MNSzJjyD6c)?

16RpBxSzcpH695cF1b6Gap51MNSzJjyD6c

Figure 7 - Example of a hint

There is a ranking system implemented in the game: as the user earns points by answering questions correctly, their rank will increase. This is to provide a feeling of progression and accomplishment and will hopefully encourage all users to play through all available scenarios to try and accomplish the highest rank they can.

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

C. 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.

IX. Deployment and validation

Since the initial version was released in 2019, Cryptopol has been promoted by representatives of the law enforcement partner at speaking and training engagements and also through word of mouth advertisement from investigator to investigator.

A. User numbers

In April 2023, an updated version of the game titled Cryptopol 2.0 was launched during a joint presentation by the application developers and the law enforcement partner at the 2023 Europol Virtual Currencies Conference.

The idea behind Cryptopol 2.0 was to add a second selection of scenarios to the game, whereas the original selection of scenarios in the initial version of the game mainly focuses on Bitcoin, the Cryptopol 2.0 selection of scenarios focuses on Ethereum, Decentralised Finance (DeFi), non-fungible tokens (NFTs) and more. At the time of writing, more than 1,500 people from 50 countries across the world, representing over 550 LEAs had trained using the game.

B. Usage evaluations

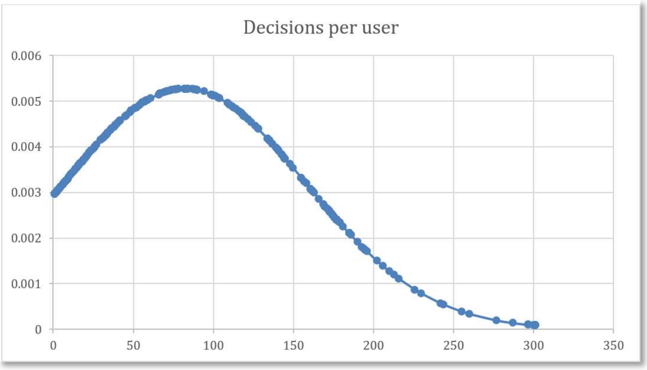


Figure 8 – Graph showing decisions made by users

Figure 8 shows a graph of the normal distribution 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. The Y-axis in normal distribution graphs represents the density of probability, which represents the chance of obtaining values near corresponding points on the X-axis.

Figure 9 shows a graph of the normal distribution of the scores achieved on the first chapter of the game (which includes all of the scenarios that were available when the game first launched in 2019) by each user, 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.

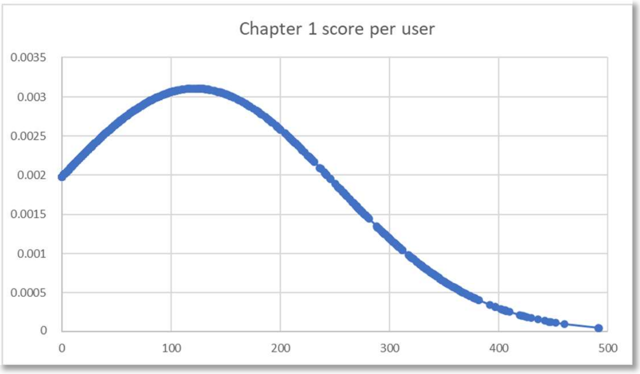


Figure 9 – Graph showing scores achieved on chapter 1

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 have been awarded a certificate, which requires all scenarios to be completed with a total score above 60%. At the time of writing, chapter 2 had only recently been released, so a similar evaluation is not possible, but similar figures are expected. This data shows excellent user retention: despite the considerable 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 from law enforcement agencies were asked about their experience of playing Cryptopol for them and their teams. 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.

Due to the success of Cryptopol, suppliers of the leading commercial cryptocurrency tracing tools offer free trial licenses to players, as they recognise the value of Cryptopol.

X. Conclusion

Tracing cryptocurrency is vital and will continue to increase in importance given the criminal trends identified. The rationale behind the decision to design and develop a serious game for teaching law enforcement agencies is clearly very strong. The serious game which was developed has now become an important tool used by law enforcement agencies worldwide. The Cryptopol 2.0 update demonstrates how the serious game can evolve over time to match any new threats. This update introduced a chapter system, which makes it 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. 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] D. Djaouti, J. Alvarez, JP. Jessel and O. Rampnoux, "Origins of Serious Games" in Serious Games and Edutainment Applications, M. Ma, A. Oikonomou and L. C. Jain, Eds. Springer, London, 2011

[2] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey and J. M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games", in Computers & Education, vol. 59, issue 2, 2012, pp.661–686.

[3] E. Boyle, T. M. Connolly and T. Hainey, "The role of psychology in understanding the impact of computer games", in Entertainment Computing, vol. 2, issue 2, 2011, pp. 69–74.

[4] S. Arnab et al, "Mapping learning and game mechanics for serious games analysis", in British Journal of Educational Technology, vol. 46, 2015, pp. 391-411.

[5] B. Akhgar, A. Redhead, S. Davey and J. Saunders, "Introduction: Serious Games for Law Enforcement Agencies", in Serious Games for Enhancing Law Enforcement Agencies. Security Informatics and Law Enforcement, B. Akhgar, Eds. Springer, 2019, pp.1-11.

[6] A. BinSubaih, S. Maddock and D. Romano, "Developing a serious game for police training", in Handbook of research on effective electronic gaming in education, IGI Global, 2009, pp. 451–477

[7] G. Van Hardeveld, G. Webber and K. O'Hara, "Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets.", in American Behavioral Scientist, vol. 61, 2017.

[8] Europol. "Cryptocurrencies: tracing the evolution of criminal finances.", https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances, 2022.

[9] Chainalysis. "The 2023 Crypto Crime Report.", https://go.chainalysis.com/2023-crypto-crime-report.html, 2023.

[10] A. Alper. "Biden sanctions cryptocurrency exchange over ransomware attacks", https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21, Reuters, 2021.

[11] Chainalysis. "Ransomware 2021: Critical Mid-year Update [REPORT PREVIEW]", https://blog.chainalysis.com/reports/ransomware-update-may-2021, 2021.

[12] Chainalysis. "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think", https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021, 2021.

[13] Elliptic. "ELLIPTIC CROSS-CHAIN REPORT 2022. The state of cross-chain crime.", 2022.

[14] M. E. Peck. "What's in a Blockchain? With New Tools, Anyone Can Find Out", https://spectrum.ieee.org/whats-in-a-blockchain-with-these-new-tools-anyone-can-find-out, 2019.

[15] Blockchain.com, "Relentlessly building the future of finance since 2011", https://www.blockchain.com/about, 2023.

[16] Coinfirm, "Battles of Dirty Money and Blockchain: How to Trace Stolen Crypto", https://www.coinfirm.com/blog/how-to-trace-stolen-crypto, 2022.

[17] A. Bandura, "Social learning theory", Prentice-Hall, 1977.