Cryptocurrency-Crime Investigation: Fraudulent use of Bitcoin in a Divorce Case

Johnny Botha[1] and Louise Leenen[2]
[1]Council for Scientific and Industrial Research, Pretoria, South-Africa
[2]University of Western Cape and CAIR, Cape Town, South-Africa

jbotha1@csir.co.za
lleenen@uwc.ac.za

Abstract: Bitcoin and cryptocurrency adoption has increased significantly over the past few years. The significant growth in the industry has been matched by growth of crimes in this domain; not only in scams and dark-web illegal trading, but also in white-collar crimes with fraud and perjury occurring increasingly. With blockchain technology, the world of financial infidelity has become increasingly sophisticated. There is a common belief that blockchain and cryptocurrency provide means of hiding funds from the public or close associates who may not be familiar with the technology. The rise of cryptocurrency has also led to spouses hiding digital assets during divorce settlements. This study presents a use case of a couple in the midst of a divorce where one of the spouses was accused of perjury for failure to declare bitcoin holdings, obtained via Bitcoin mining, and possibly other forms of cryptocurrency and digital assets to the court. The plaintiff is entitled to fifty percent of all assets. While property, stocks, bonds, and bank accounts can easily be traced, cryptocurrency assets are more complex to trace but it is not impossible. This paper illustrates how such a case can be investigated by following the flow of funds on the blockchain, using tools such as Maltego and QLUE. The paper thus presents an investigative process that can be followed for a new category of forensic investigation.

Keywords: Bitcoin, Blockchain, Fraud, Investigation, Perjury

1. Introduction

Bitcoin (BTC), the most popular cryptocurrency on the blockchain with the highest market capital (CoinMarketCap, 2023), has gained wide popularity since it was first created, due to its unique properties, turbulent price swings and surging value. Some may believe bitcoin gives back the power to the people because transactions can be performed without third parties such as banks. However, the popularity of cryptocurrency has attracted various types of fraud and crimes and has become a growing global concern (Trozze, et al., 2022) (Botha, Botha, & Leenen, 2023). Crime in the cryptocurrency space is increasingly moving into the white-collar crime category. Organised criminal groups need some way to "cash out" in ways to evade law enforcement (Gibson Miralis, 2023). The growth of cryptocurrency has also led to cases where spouses hide digital assets during divorce settlements. When a couple, married in community of property, file for divorce, both parties are usually obliged to declare all their assets obtained during their marriage, including digital assets. Most physical assets and bonds are fairly easy to track down, whereas cryptocurrencies could be a bit tougher to trace. A cryptocurrency and forensics investigator may be needed to assist in such cases. Dore (2021) quotes an attorney in New York who noted that awareness among attorneys of these hidden cryptocurrency assets is recent, and that the hardest aspect for attorneys is determine whether such investments exist. This paper illustrates the process that can be followed to identify hidden cryptocurrency assets, and to trace where the funds may have been moved.

Bitcoin is often perceived to offer anonymity. On the contrary, it is traceable. A person's identity is not directly linked to a bitcoin address, but all transactions are public and recorded on the blockchain. Bitcoin and Ethereum are older forms of cryptocurrency and are easier to track down than some of the anonymous or private cryptocurrencies such as Monero (XMR) [(Chainalysis Team, 2023), Zcash and Dash (Hayward, 2021)], but it is not impossible [(Masters Law Group LCC, 2022) (originstamp, 2023)]. These so-called privacy coins make use of varying cryptographic techniques with the aim to obscure details of transactions and to shield users from exposure of related information. Privacy coins have become the preferred method of payment for ransomware demands, criminal transactions on the dark web, and money laundering (Barone & Masciandaro, 2019). These criminals have attracted noteworthy attention from law enforcement and regulators (Hayward, 2021). However, this study's focus is only on tracking the flow of the bitcoins and not any other form of cryptocurrency.

A bitcoin transaction is a digital exchange of cryptocurrencies between two parties. The transaction can occur via an exchange or directly between individuals. All transactions are recorded in a public ledger. This public ledger is called the blockchain. The blockchain is a technology was first revealed by Satoshi Nakamoto in his white paper on 31 October 2008. The technology is the foundation of bitcoin and the heart of all cryptocurrencies (Di Pierro, 2017). When a transaction is recorded, it is also referred to as writing to a block on

the blockchain. Transactions take place without the need for a third party such as a bank or financial institution. The transactions can never be deleted or altered on the blockchain (originstamp, 2023). Blockchain explorers are software applications that allow anyone to view the blocks on the blockchain, as well as addresses and transactions connected to those blocks. Blockchain.com (Blockchain.com, 2023) is one example of a blockchain explorer (originstamp, 2023). To trace a bitcoin transaction, the bitcoin address or transaction-id to be traced has to be entered into the explorer's search field. All the recorded information related to the address or transaction are revealed. Upon entering an address into the blockchain explorer, the explorer will also reveal all transactions made from and to the given address. Other visible information are the block heights at which the transaction was made, as well as the time and date stamps (originstamp, 2023).

Tracing the funds on a blockchain explorer can become a very time-consuming task. Since all the data on the blockchain is publicly available, this falls in the Open-Source Intelligence (OSINT) space. Various OSINT tools exist to assist in crime investigations. One of the most popular tools is Maltego (Maltego, 2023). Maltego has various transforms that can be used to integrate into external data-sources. One of such a data source is the Tatum Blockchain Explorer. Tatum supports over 40 blockchain protocols and over 2000 digital assets (Maltego Technologies, 2023). Maltego makes it much easier to follow the funds on the blockchain. Although Maltego makes it much easier than working on the public blockchain explorers, the tool has limitations. It is almost impossible to match bitcoin addresses with their owners (users). Maltego does not perform clustering of addresses and does not indicate whether an address belongs to a crypto exchange.

One of the tools to perform blockchain investigations is QLUE. This tool was designed for law enforcement and financial investigators to secure evidence of fraud involving crypto. The tool is very effective in following the trace of funds on the blockchain and can reduce time spent on crypto investigations from weeks to merely hours (QLUE, 2023). The tool is capable of clustering certain crypto addresses and can also identify and highlight if an address is flagged as an address known to be fraudulent. The tool can also indicate whether an address is linked to a cryptocurrency exchange or not. For an investigator to identify and prove that transactions linked to an address and then linked to an exchange were executed, is of utmost importance and constitutes valuable information. Exchanges collect personal information on members, which is the type of information of interest to an investigator. However, one cannot request personal information without the involvement of law enforcement. A law enforcement agency can issue a subpoena to an exchange instructing the exchange to reveal the personal information related to a certain crypto or bitcoin address. A subpoena will provide the investigator with personal information, transactional information and evidence that could assist in linking a suspicious cryptocurrency address or transaction to a specific individual. The subpoena will also force the exchange to reveal any other addresses as well as all transactions linked to the target person.

This paper investigates a specific case of possible fraud and perjury during a divorce settlement. Limited information and background have been provided as inputs for the case. With the use of blockchain explorers and OSINT investigating tools such as Maltego and QLUE, it is possible to follow the flow of funds and it could be traced on the blockchain up to a point where a destination address can be reached. From the destination address, further findings and conclusions can be made. It should be noted that the plaintiff has given consent to the researcher to perform this study and to conduct a high-level investigation. Note that no personal information and no blockchain information are exposed in this paper, the bitcoin addresses and transactions have all been sanitised in this paper.

2. Case Background

With the unique properties of bitcoin, it is possible to hide assets from people who are not aware of how the blockchain with its public ledger works or how to trace funds on the blockchain. Tracking down hidden cryptocurrency stashes during a divorce has led to a completely new case category of forensic investigation. If one of the spouses is technically skilled and the other one is not, the prior can easily hide digital assets. The best method to get information on a spouse's cryptocurrency holdings is via a subpoena from a centralized crypto exchange. The alternative is a process that involves a forensic analysis of their computer or other devices to identify a wallet address and then a subsequent blockchain analysis. Crypto asset forensics, cryptocurrency forensics, and blockchain forensics have become an important part of legal divorce cases. Crypto can be stored on exchanges, but it can also be stored on "hot" or "cold" wallets or a combination of both. Hot wallets are connected to the Internet and allow users to easily spend the coins, but they are also more exposed to bad actors. Cold wallets are not connected to the Internet and the private keys are stored on the device itself. Investigating a case where the crypto is stored on cold wallets makes the case a bit more complex than hot

wallets. However, to cash-out one normally, one must go via an exchange or some kind of off-ramp service (Sigalos, 2023).

The use case we consider in this paper, concerns a divorced couple who was married in community of property. The plaintiff is entitled to fifty percent of all their assets. However, the defendant failed to declare any cryptocurrency holdings or assets obtained via bitcoin mining. Bitcoin mining is a method, or the process, of creating new bitcoins by solving complicated mathematical puzzles or problems that verify transactions on the blockchain. When a bitcoin has been mined successfully, the miner receives as a reward a predetermined amount of bitcoin (Baker, 2023). The plaintiff in the divorce case also claimed to have contributed funds to procure fourteen bitcoin Antminers. An Antminer is basically a bitcoin mining computer and is regarded as the most potent in the world when it comes to bitcoin mining. One Antminer could earn 0.1248924 bitcoin monthly (Masa, 2022). Figure 1 is a photo taken of four of the fourteen miners in possession of the defendant. It should be noted that the plaintiff has right of ownership of half of these miners, as well as half of the assets obtained through the mining processes.

Figure 1: Bitcoin Ant-miners

The defendant did not provide any information regarding the bitcoin holdings obtained via the miners. However, the plaintiff managed to obtain two bitcoin addresses linked to the bitcoin mining services. The two addresses given below are the only inputs provided to start this investigation *(please note the full addresses are not disclosed in this paper for privacy reasons):*

- 1DGDY…YSWwM (referred to as BTC_1 in this paper)
- 1JZYv…JPx8A (referred to as BTC_2)

With this limited information, the next step is to follow the funds on the blockchain to determine if the addresses contain any funds, and to view all the transactions performed on these addresses to determine where the funds have been moved to. The aim is to get to a destination address, possibly linked to an exchange. When a destination address has been identified and linked to an exchange, further information could be obtained via subpoena, instructed via an attorney and law enforcement. It should be noted that the destination can be a cryptocurrency wallet address that is not linked to an exchange. For such a case, no personal information will be available to link to the address. An investigator could flag the address and set up a notification when funds move out of the address in the future, with the hopes that it would be moved to an exchange or any other off-ramp where KYC (Know Your Customer) information could be obtained.

The next section illustrates how one could investigate, analyse and follow the funds on the blockchain.

3. Investigation and Findings

Using the blockchain.com explorer and Maltego, it could easily be determined that the two addresses contained 0 bitcoin and the last transaction performed on the addresses were in 2019 (Figure 2 and Figure 3).

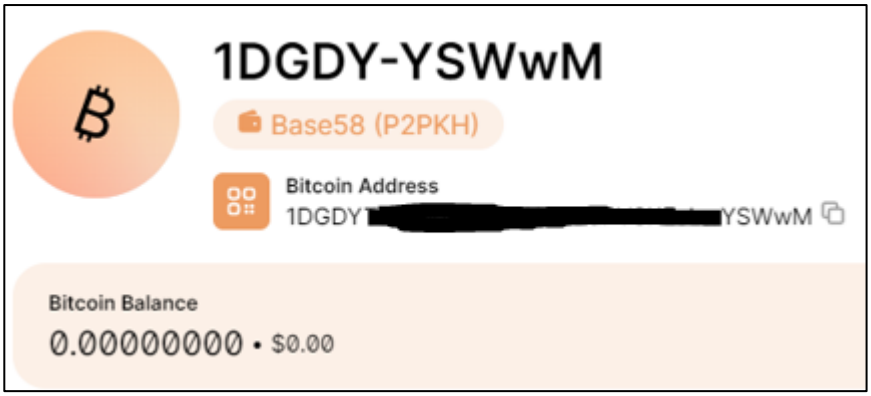

Figure 2: Blockchain.com Explorer - BTC_1 – Balance

The last amount transacted on this address (Figure 4) was 1.07147560 BTC and was sent out of the address into another bitcoin address, namely **177hB…wSxvh**.

Only the first four and last four characters of the address are displayed in Figure 3. If one clicks on the address or copies it from the copy icon next to the "To" address (Figure 3), the full address is revealed.

Figure 3: BTC_1 - Last Transaction Date

At the time of writing, the amount sent from BTC_1 was equivalent to $29, 920.57 (Figure 4).

Figure 4: BTC_1 - Last Transaction Amount

Table 1 lists both input addresses that was received by the plaintiff with their current balance, total received, and total sent.

Table 1: Input Bitcoin Addresses and Balances

BTC Address	Current Balance	Total Received	Total Sent
BTC_1	0	1.07147560	1.07147560
BTC_2	0	0.34892516	0.34892516

Using the Maltego tool, it was discovered that **BTC_1** has 24 incoming transactions and one outgoing transaction to the bitcoin address **177hB…wSxvh** (Figure 5). However, this output address also contained 0 BTC. Further traces have been followed, but all addresses ended up with a 0 BTC balance. **BTC_2** also had several inputs from various address and transactions and one output to the address **17rDj…wtCbK** (Figure 6). Similar to **BTC_1**, the output address had a balance of 0 BTC. The trace has also been followed and all addresses had a balance of 0 BTC. Since the transaction dates are very old, 2019, the assumption can be made that 0 bitcoins will be left in any of the addresses and that the defendant has already cashed out via an offramp such as an exchange. An offramp is a company or service that allows a client to convert cryptocurrency back in fiat money (Rockwallet, 2023). The audit trail could still be followed to a destination address to indicate how many bitcoins were transacted. If the defendant has cashed out the bitcoins, the plaintiff is entitled to a payment in cash equivalent to the amount of these bitcoins.

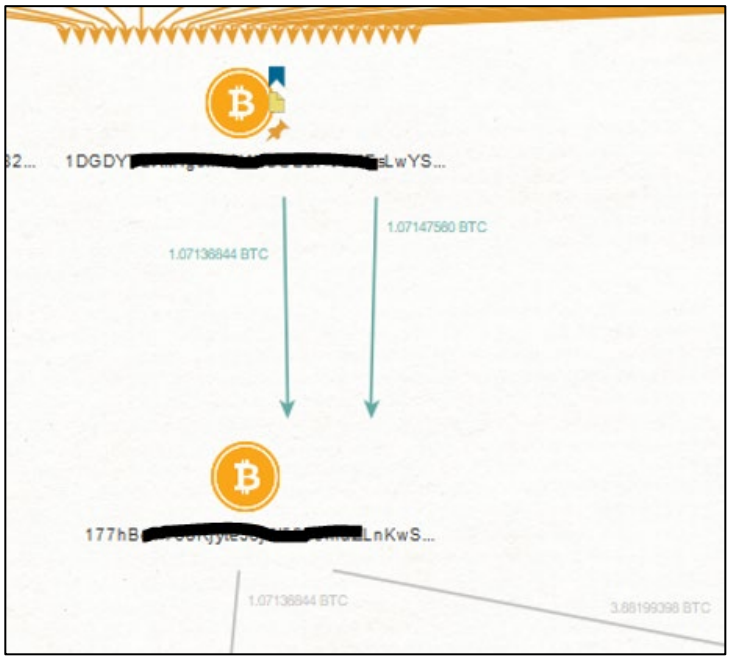

Figure 5: BTC_1 – Output Transaction

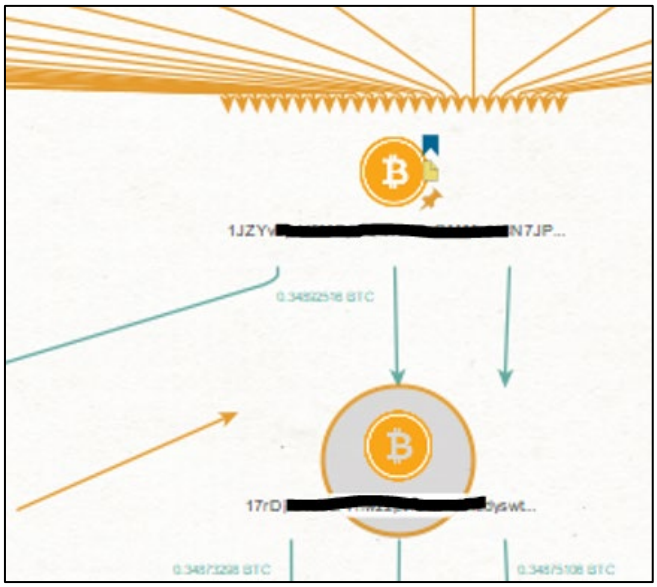

Figure 6: BTC_2 - Output Transaction

After several attempts to follow the funds, no clear conclusion or findings could be reached. The researcher reached out to a crypto-crime investigator who has assisted in a previous research study (Botha, Pederson, & Leenen, 2023). The investigator is involved in big cases such as the Mirror Trading International (MTI) scam as well as the Finalmente Global scam. MTI was a network or multi-level marketing scheme that claimed to offer automated cryptocurrency trading services via bots (Vermeulen, 2022a). Finalmente Global has claimed to take bitcoin investments from members to buy online advertising space. Both platforms have been shut down and are under investigation (Vermeulen, 2022b).

Access to the cryptocurrency graphing and investigation tool QLUE is restricted to licensed versions. Through collaboration with the crypto-crime investigator, access to the tool was received and the investigation was continued. QLUE makes it easier to follow the funds on the blockchain and it gives the investigator clustering capabilities. It can cluster addresses belonging to the same user, or addresses linked to a certain exchange. It also allows for the investigator to flag certain addresses as fraudulent or indicates cases where an address has been linked to a known scam. For the purpose of this investigation, a link to an exchange is required. This will allow the investigator, through an attorney, to send a subpoena to the exchange. A subpoena instructing the

exchange to reveal the personal information as well as indicating if any cash-out to a bank was performed, will then be issued. If a cash-out has been done, the cash-out transaction details need to be provided to the investigator. The type of information required is the amount that was cashed out as well as the dates and bank details.

The same two addresses, **BTC_1** and **BTC_2**, have been provided to TCG Forensics as inputs. By using QLUE, it was discovered that the transactions from both addresses ended up in an address that belongs to Luno (Luno, 2023), a South African cryptocurrency exchange (Figure 9). Figure 7, Figure 8 and Figure 9 show the flow of funds from the input addresses up to the destination address that is linked to Luno. In addition to the two provided input addresses, another input address, **1NTQf…8Es7e**, was also revealed (Figure 7). The address appears to be from the same source mining activity based on the clustering done by QLUE. This address will be referred to as **BTC_3**.

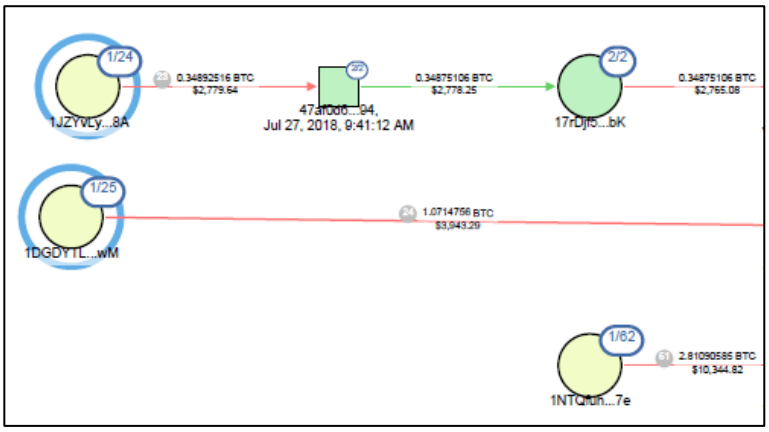

Figure 7: Inputs into QLUE (Flow of funds - a)

By continuing to follow the funds, three addresses have been identified with amounts sent to the destination address into Luno (Figure 8). QLUE hides the addresses in the diagram. It should be noted that bitcoin addresses are visualised in QLUE as round circles and transactions as square blocks. An arrow going out of a square block (transaction) into a circle (address) in Figures 7, 8 and 9 refers to an incoming flow of funds into a bitcoin address; an arrow going out of a circle (address) into a square block (transaction) indicates an outgoing flow of funds. An incoming flow of funds will always go from a transaction into an address and an outgoing flow of funds from an address into a transaction.

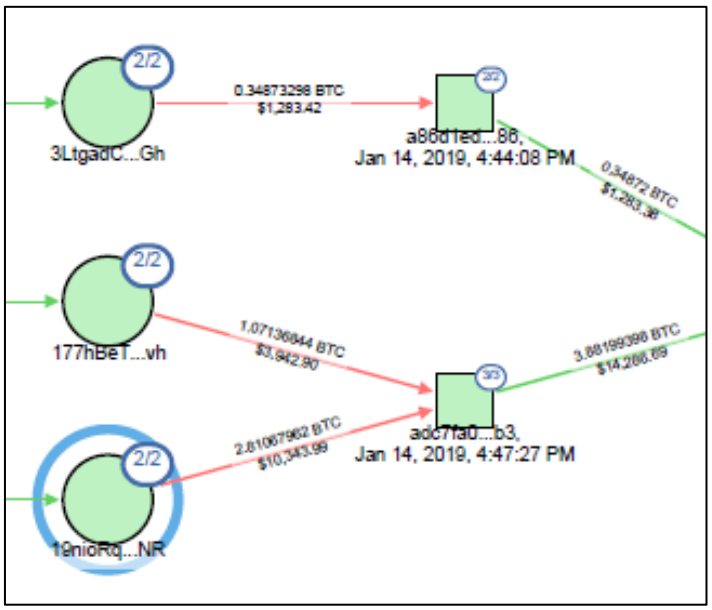

Figure 8: Flow of funds (continue - b)

Table 2 lists the three addresses (Figure 9) with the amounts sent from each address into the destination address, **1DRfj…xY9KN**, (Figure 10). The first column indicates the origin or starting point of the flow of funds,

the second column the last address before the funds moved to the destination address and the third column lists the amount sent to the destination address via each input stream (Table 2).

Table 2: Last Addresses Before Destination Address

From Input Address	Last Address Before Destination	Total Sent
BTC_1	3Ltga…a2eGh	0.34873298
BTC_2	177hB…wSxvh	1.07136644
BTC_3	19nio…WNUNR	2.81007962

The sum of these three amounts in Table 2 is equal to 3.916319358 BTC. Looking at the outflow of funds in Figure 9, only 3.88199398 BTC has been sent out of Luno to another address external from Luno. Thus, the remainder of 0.34872 BTC that went into the destination address could possibly still be in the balance.

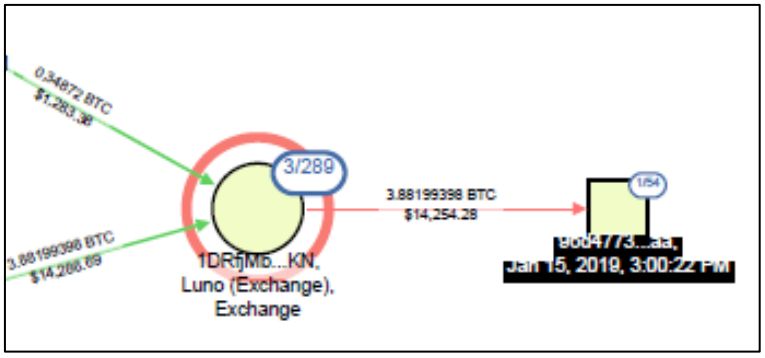

Figure 9: Flow of funds (continue - c) – Destination Address

However, QLUE indicated that the current balance on the destination address (Figure 10) shows a balance of 0 BTC. This means the full amount of BTC was transferred out of the destination address.

Figure 10: Destination Address

Upon further investigations using QLUE, it has been discovered that the remaining amount has been transferred from the Luno exchange into another address outside of Luno (Figure 11). The address it was sent to was also flagged by QLUE as a Hot wallet, and linked to the cryptocurrency exchange Bitssa (Bitssa, 2023), (see Figure 12). To see if this transaction was performed by the defendant one needs to obtain a transaction list from Luno. This can be obtained with a subpoena issued by law enforcement. At the time of writing this paper, no subpoena had been requested to take the investigation further. The aim of this paper is to reveal the amounts of bitcoin the defendant has been hiding from the spouse in the divorce settlement by following certain steps; subsequent legal action is beyond the scope of our research.

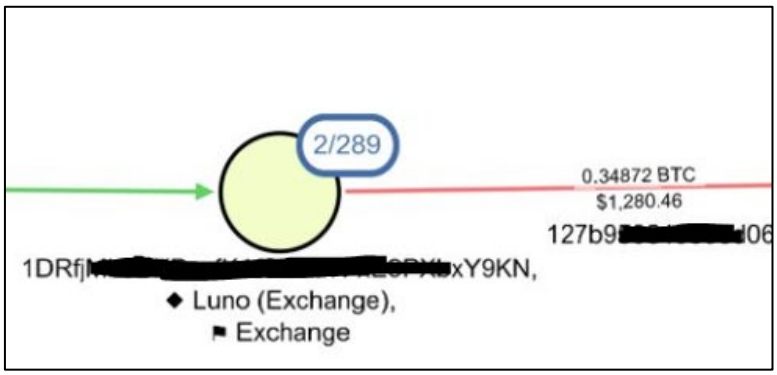

Figure 11: Remainder Amount - Transferred from Luno to Bitssa.in

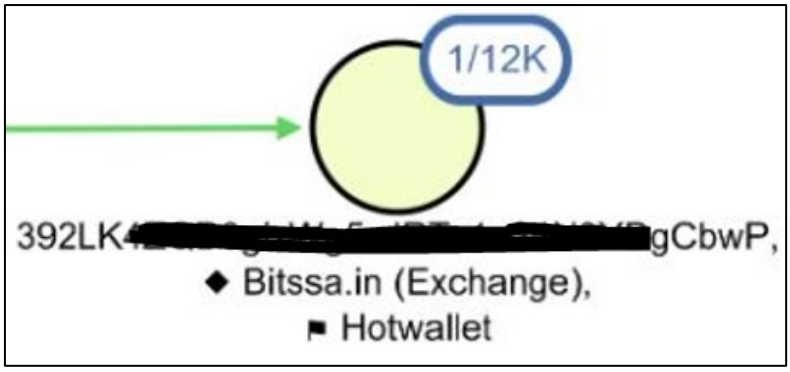

Figure 12: Bitssa.in – Hot wallet Address

It should be noted that the findings in this study were only linked to the two input addresses provided by the plaintiff. It is also possible that the defendant hid more cryptocurrency investments obtained by other means during the marriage. These assets should also be declared by the defendant to the court during the divorce settlement case. However, this is outside the scope of this investigation.

This study and investigation illustrated that it is not impossible to trace funds on the blockchain. Various tools exist to assist in following funds and movements on the blockchain. With an investigation on the blockchain, the aim is to find links to an exchange. An exchange normally stores KYC information of members. The idea is to obtain personal information that could be linked to certain bitcoin addresses and transactions. Once personal information can be identified, the investigator could attempt to contact the person of interest. If no response is received, alternative OSINT investigation techniques will have to be followed to locate the person.

4. Conclusion

This paper gives an overview and introduction to white collar crime in the crypto space. Many people believe that crypto is anonymous and that they can use the technology to hide some of their assets from people such as a spouse, for example. However, as illustrated in this paper, that can be contrary to belief as every transaction on the blockchain is transparent and visible to the public. When one uses blockchain explorers and investigation tools such as Maltego or QLUE, it is possible to trace the flow of funds on the blockchain. An investigator simply needs a starting point to follow the funds to a destination that is linked to an exchange. Most exchanges collect personal information on all members. An investigator can issue a subpoena via an attorney to an exchange. This will instruct the exchange to reveal the required personal information on a target person linked to a crypto address within their platform.

This paper describes an investigative approach to a divorce settlement case. The defendant was accused of not declaring digital assets in the divorce settlement. The defendant had obtained bitcoins via bitcoin mining processes during their marriage. These mining computers had also been procured during the time they were still married. Two bitcoin addresses have been provided by the plaintiff as inputs and a starting point on the blockchain. From the high-level investigation on the flow of funds, it became clear that the addresses provided as inputs by the plaintiff showed a balance of 0 BTC. Further findings were that 3.916319358 BTC had been sent to a destination address that is linked to the Luno exchange. Only 3.88199398 BTC had left the Luno exchange, and these funds appear to have been cashed out. The remainder had been sent to another exchange. To get the proof of the cash-out and the remainder been sent to another exchange by the defendant, a subpoena is required to instruct the exchange to reveal more information such as all transaction details of the defendant. Thus, based on these findings, there is evidence that the accused obtained 3.916319358 BTC from the mining services while being married. The bitcoins had been hidden from the plaintiff during the divorce settlement. Half of value of these bitcoins should be paid out to the plaintiff.

Acknowledgement

The authors thank Thor Pederson from TCG Forensics for his continued support and advice.

References

Baker, B. (2023, Mar 27). *What is Bitcoin mining and how does it work?* Retrieved from www.bankrate.com: https://www.bankrate.com/investing/what-is-bitcoin-mining/

Barone, R., & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. *Eur J Law Econ 47* (pp. 233–254). Springer. doi:https://doi.org/10.1007/s10657-019-09609-6

Bitssa. (2023, Aug 11). *Bitssa Swap*. Retrieved from https://swap.bitssa.com/: https://swap.bitssa.com/

Blockchain.com. (2023, Aug 11). *Blockchain.com Explorer*. Retrieved from www.blockchain.com: https://www.blockchain.com/explorer

Botha, J., Botha, D., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. *18th International Conference on Cyber Warfare and Security* (pp. 36-48). Towson University, Baltimore County Maryland, USA: Academic Conferences International Limited.

Botha, J., Pederson, T., & Leenen, L. (2023). An Analysis of the MTI Crypto Investment Scam: Use Case. *European Conference on Cyber Warfare and Security* (pp. 89-99). Athens, Greece: Academic Conferences International Limited.

Chainalysis Team. (2023, May 4). *Monero: All About the Top Privacy Coin*. Retrieved from www.chainalysis.com: https://blog.chainalysis.com/reports/all-about-monero/#:~:text=Monero%27s%20privacy%2Denhancing%20features,-Monero%27s%20primary%20purpose&text=The%20Monero%20blockchain%20employs%20diverse,user%20generated%20a%20given%20signature.

CoinMarketCap. (2023, Aug 11). *Home Page*. Retrieved from https://coinmarketcap.com/: https://coinmarketcap.com/

Di Pierro, M. (2017). What is Blockchain. *Computing Prescriptions*. Retrieved from https://cse.sc.edu/~mgv/csce190f18/diPierro_mcs2017050092.pdf

Dore, K. (2021, Jun 1). *Spouses in divorce proceedings are using cryptocurrency to hide money. Here's how experts find it*. Retrieved from www.cnbc.com: https://www.cnbc.com/2021/06/01/divorcing-spouses-are-using-cryptocurrency-to-hide-money-how-experts-find-it.html

Gibson Miralis, N. (2023, Aug 11). *How is crypto crime becoming increasingly white collar?* Retrieved from www.lexology.com: https://www.lexology.com/library/detail.aspx?g=453fc875-be12-4701-b3ed-585aad9a2191

Hayward, A. (2021, May 31). *What Are Privacy Coins? Monero, Zcash, and Dash Explained*. Retrieved from https://decrypt.co: https://decrypt.co/resources/what-are-privacy-coins-monero-zcash-and-dash-explained

Luno. (2023, Aug 11). *Luno Home Page*. Retrieved from https://www.luno.com/en/za: https://www.luno.com/en/za

Maltego. (2023, Aug 11). *Maltego Home Page*. Retrieved from Maltego.com: https://www.maltego.com/

Maltego Technologies. (2023, Aug 11). *Tatum Blockchain Explorer*. Retrieved from www.maltego.com: https://www.maltego.com/transform-hub/tatum-blockchain-explorer/

Masa, W. (2022, Nov 24). *What Is Antminer? How Much Does A Antminer Make A Day?* Retrieved from https://bitkan.com: https://bitkan.com/learn/what-is-antminer-how-much-does-a-antminer-make-a-day-8792

Masters Law Group LCC. (2022, Nov 4). *CAN HIDING CRYPTO FROM YOUR EX GET YOU IN LEGAL TROUBLE?* Retrieved from www.masters-lawgroup.com: https://www.masters-lawgroup.com/cryptocurrency-and-divorce/can-hiding-crypto-from-your-ex-get-you-in-legal-trouble/

originstamp. (2023, Nov 11). *How to Trace Bitcoin Transactions [Full Guide]*. Retrieved from www.originstamp.com: https://originstamp.com/blog/how-to-trace-bitcoin-transactions/

QLUE. (2023, Aug 11). *QLUE Home Page*. Retrieved from www.qlue.io: https://qlue.io

Rockwallet. (2023, Aug 11). *Off-Ramp and On-Ramp Crypto, What You Need To Know*. Retrieved from Rockwallet.com: https://www.rockwallet.com/blog/off-ramp-and-on-ramp-crypto-what-you-need-to-know#:~:text=On%20the%20other%20hand%2C%20off,ramps%20allow%20you%20to%20exit.t=On%20the%20other%20hand%2C%20off,ramps%20allow%20you%20to%20exit.

Sigalos, M. (2023, May 20). *A husband hid $500,000 in bitcoin during a divorce — and got busted by a crypto hunter*. Retrieved from https://www.cnbc.com: https://www.cnbc.com/2023/05/20/bitcoin-in-divorce-how-spouses-hide-assets-crypto-hunters-find-them.html

TCG Forensics. (2023, Aug 11). *Most Prominent Investigations Into Fraud, Cybercrime And Violent Crimes*. Retrieved from www.tcgforensics.co.za: https://www.tcgforensics.co.za/

Trozze, A., Kamps, J., Akartuna, E., Hetzel, F., Kleinberg, B., Davies, T., & Johnson, S. (2022). Cryptocurrencies and future financial crime. *Crime Sci 11.* Springer. doi:https://doi.org/10.1186/s40163-021-00163-8

Vermeulen, J. (2022a, Apr 12). *Good news for Mirror Trading International scam victims*. Retrieved from https://mybroadband.co.za: https://mybroadband.co.za/news/cryptocurrency/440928-good-news-for-mirror-trading-international-scam-victims.html

Vermeulen, J. (2022b, Jan 7). *Finalmente Global shuts down, blames death of Mirror Trading International*. Retrieved from https://mybroadband.co.za: https://mybroadband.co.za/news/cryptocurrency/381646-finalmente-global-shuts-down-blames-death-of-mirror-trading-international.html