Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges

Anastasios Balaskas
University of Derby, Cyber Security Research Group
College of Engineering & Technology
DE22 1GB, Derby, United Kingdom
a.balaskas1@unimail.derby.ac.uk

Virginia N. L. Franqueira
University of Derby, Cyber Security Research Group
College of Engineering & Technology
DE22 1GB, Derby, United Kingdom
v.franqueira@derby.ac.uk

***Abstract*—Bitcoin has introduced a new concept that could feasibly revolutionise the entire Internet as it exists, and positively impact on many types of industries including, but not limited to, banking, public sector and supply chain. This innovation is grounded on pseudo-anonymity and strives on its innovative decentralised architecture based on the blockchain technology. Blockchain is pushing forward a race of transaction-based applications with trust establishment without the need for a centralised authority, promoting accountability and transparency within the business process. However, a blockchain ledger (e.g., Bitcoin) tend to become very complex and specialised tools, collectively called "Blockchain Analytics", are required to allow individuals, law enforcement agencies and service providers to search, explore and visualise it. Over the last years, several analytical tools have been developed with capabilities that allow, e.g., to map relationships, examine flow of transactions and filter crime instances as a way to enhance forensic investigations. This paper discusses the current state of blockchain analytical tools and presents a thematic taxonomy model based on their applications. It also examines open challenges for future development and research.**

Keywords— blockchain; cryptocurrency; bitcoin; tools; blockchain analytics; digital forensics; cybercrime investigation.

I. INTRODUCTION

Blockchain analysis is an entirely new field of research and development, which started to emerge in 2014 as a trend within the cryptocurrency ecosystem. This trend was mainly pushed by its transparent and decentralised nature.

Blockchain Analytics provide a useful tool for individuals to inspect the network of transactions in terms of, e.g., flaw analysis and transaction relationships [1]. Also, as cryptocurrencies thrive and grow as mainstream payment method, insights into how people are spending them become increasingly relevant. Not just in terms of which products or services are bought with them, but also knowledge of how long people are keeping cryptocurrency in their wallets, in a way to stimulate the worldwide adoption of cryptocurrency [2][3]. For law enforcement, identifying these type of activities is important in order to prevent money laundering and terrorism financing. Through the analysis of transactions, investigators try to match connections and interactions between addresses. Some tools have already started to index sets of transactions as a way to cluster them into specific groups [4][5].

The positive sides to blockchain analysis are not hard to find. Detailed analytics can answer questions like how the cryptocurrency is being spent, where are the new wallets coming from and how can we trace the money [6]. Nevertheless, beside the economic indicators and market trends, blockchain analysis can involve further parameters like the embedded metadata and their connection with smart contracts, which transfer the landscape to a wider field of applications apart from normal cryptocurrency [7].

In this paper, blockchain analytic tools are examined in terms of their applications within the research and developers' community, and their effectiveness in cybercrime investigation and analysis. Through study of related work, a thematic taxonomy is presented for the categorisation of blockchain analytic tools according to their applications. Specific tools are examined based on their features, efficiency and components, providing, this way, evaluation criteria for the selection of an appropriate solution in order to cover a set of investigation requirements. Furthermore, open challenges and practices are discussed as well as future areas of research and development.

The paper is organised as follows. Section II provides background information on the technical aspects of blockchain and bitcoin. Section III presents a thematic taxonomy of the blockchain analytic tools and examines available tools and how they fit within the above-mentioned taxonomy scheme. Section IV explores open challenges in this field, while Section V draws conclusions and elaborates on recommendations for future work.

II. BACKGROUND

Information that is available in a blockchain is considered as extremely valuable for both data analysis and crime investigation. This section presents the backbone concept of blockchain and how it applies to bitcoin transactions.

A. What is Blockchain

Blockchain is a distributed technology built under peer-to-peer network principles and cryptographic primitives, such as asymmetric encryption and digital signature. It allows trust-less users to exchange information and record transactions without external interference and coordination. Therefore, the blockchain infrastructure allows a secure and append-only database to be built that relies on a consensus protocol for deciding which of the valid information will be added in the distribution and propagated through the network of participants. As this technology can provide every member with a trusted and decentralised proof of work [8], the application part of it – like cryptocurrencies – can utilise what is usually referred to as *public ledger*. This means that all users have equal ledgers, ensuring, this way, transparency within the network.

Different applications use the blockchain technology as a way to store value exchanges through *transactions*. Every transaction generated by a node is digitally signed with the

previous transaction's hash and the destination node's public key; this scheme ensures that transactions are tamper-proof. Specific nodes in the blockchain network will validate a block containing transactions – which nodes depend on the type of consensus adopted by the network; this process is called *mining* [9, pp. 105-106]. For example, bitcoin adopts the proof-of-work consensus scheme where each node is presented with an intensive computational problem. Nodes which succeed in solving the problem will be able to incorporate the valid block into their version of the public ledger before it is broadcasted across the network. As it was shown in the original bitcoin induction [10], such a ledger will remain secure as long as more than the 50% of the computational power is controlled by honest users.

Having the blockchain acting like a public ledger facilitates the ability for any blockchain analytic tool to query for transactions associated with a particular address, e.g., search for wallet addresses and check for related transactions.

B. *Overview of Bitcoin*

Bitcoin is a network protocol based on blockchain, introduced by Nakamoto [11] which allows payments and coin transfers to be made among participating entities. No trusted bank is needed to maintain balances, coordinate money transactions or issue new currency.

The bitcoin network maintains a global distributed ledger of transactions which is public. In this case, each transaction represents a payment from one node to another. The payment address is generated after a set of irreversible cryptographic hashing functions of the sender's public key; every new valid block is broadcasted to all network nodes. Bitcoin currently uses SHA-256 for those hashing operations [12].

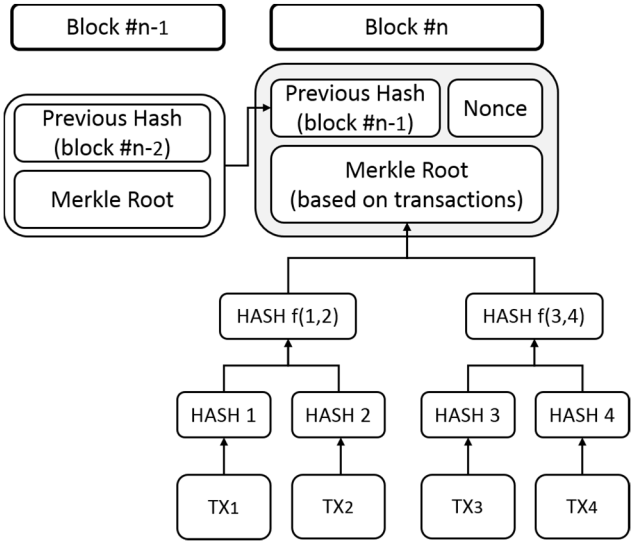

Fig. 1. Block construction of Bitcoin using Merkle Tree (TXn are application-specific transactions).

The transactions listed in a new block have been verified by miners who also check that no coins are spent twice. Transactions of a new block are processed into a single hash value which is the root of a Merkle Tree [13]. Such binary tree structure only contains transactions in the leaves. The hashing scheme, illustrated in Fig. 1, propagates transactions' hashes and combines them until a unique hash is obtained and added to a new block as the Merkle Root of transactions in the block. Also added to the new block is the hash of the previous block; both hashes and the replication of the ledger (among participants of the network) make the blockchain technology tamper-proof [14]. In case two miners broadcast a new block and one block is subset of the other, the block that has more transactions is kept [15].

Similar to cash change in physical transactions, bitcoin generates coin change, which is directed to a new (wallet) address rather than the original address. The main reason behind it is privacy. Maintaining privacy in blockchain depends on a strict separation between addresses and personal identities, a model referred to as *pseudonymity* [16]. For example, a bitcoin payment transfers coins from address #1 to #2 (from Bob to Alice), but directs change to address #3. Therefore, at first glance, it would be assumed that addresses #1 and #3 are associated with separate identities. The reality is, however, that addresses #1 and #3 might refer to the same identity, as illustrated in Fig. 2. These pseudonymous scheme makes the bitcoin graph very complex and ambiguous, therefore, extra information is needed to link wallet addresses to identities and perform different types of analysis – motivating the surge of blockchain analytic tools.

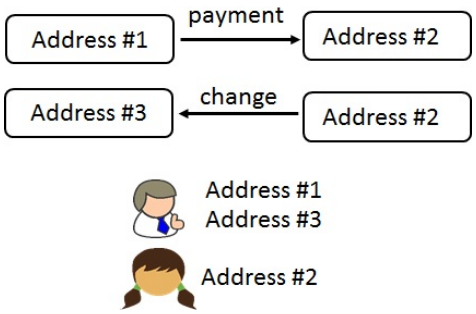

Fig. 2. Bitcoin: payment & change scheme.

III. Blockchain Analytic Tools

This section presents a taxonomy model by examining tools and practices within the area of blockchain analytic tools in detail. The taxonomy model presented in Fig. 3 leads to discussion regarding open challenges in the area of blockchain analytics, elaborated in Section IV.

A. *Thematic Taxonomy of Blockchain Analytic Tools*

Investigations of cybercrime, in general, and of ransomware in particular, are increasingly relying on blockchain analytic tools since many attacks typically use cryptocurrency for harvesting ransom. For example, CryptoLocker campaigns have been under examination using blockchain information [17] [18]. Researchers have been able to identify embedded digital footprints that could reveal relevant information about identities behind them [19].

As cryptocurrencies rely on cryptographic protection and a decentralised peer-to-peer system, money ownership is implicitly pseudonymous, while its flow is publicly available and visible. Blockchain analysis provides information about movements of cryptocurrencies. Several researchers have approached this topic with the help of blockchain analytic tools

in order to de-anonymise users [20] [21]. Reid and Harrigan [21] outlined the difficulty of the combined anonymity and user behaviour while tools which emerged later, like **Blockchain Inspector** [22], use artificial intelligence in order to profile blockchain users and track their behaviours. However, using blockchain analytics has two main drawbacks, namely the big data volume [23] and dealing with users with multiple wallet addresses, as a result of the coin change scheme (Section II-B).

Economic studies have been another area of interest which takes advantage of blockchain analysis. Moser and Bohme [24] focused on bitcoin transaction fees and tried to determine the agents' behaviour via analysis of their transaction fees using the publicly available blockchain records on bitcoin and exchange rates from **Coindesk** [25]. Lischke and Fabian [26] and Ron and Shamir [27] conducted market analysis using blockchain, combining network data and geo-locations to get insights into the cryptocurrency business distribution over time. Both studies used **blockexplorer.com** [28] – an open source web tool that allows visualisation of information regarding blocks and blockchain transactions as their main source of data.

Other areas of blockchain analysis include the study of the scripting language used by cryptocurrency protocols. Bartoletti and Pompianu [29] used blockchain analytics and developed a tool named **OpReturnTool** to investigate metadata related to the OP_RETURN instruction, a command that is included in bitcoin and provides a way to embed additional data into the blockchain [9, p. 193]. It is set to allow up to 80 bytes of data and, when a transaction that contains an OP_RETURN field is confirmed by mining, this content will be added into a block and will, therefore, remain within the blockchain forever.

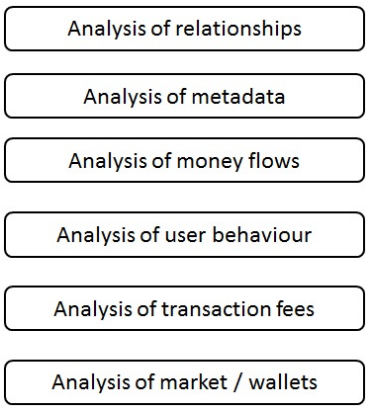

Fig. 3. Thematic taxonomy for applications of Blockchain Analytic Tools.

In a nutshell, such tools have been used for a variety of purposes. Figure 3 captures those applications and provides a thematic taxonomy of blockchain analysis tools in terms of areas of interest. The next section studies in more detail further tools with the goal of mapping them against the proposed taxonomy.

B. Additional Blockchain Analytic Tools

This section reviews a selection of additional blockchain analytic tools, both open source and commercial tools, in order to identify relevant features.

BitConeView [30] is a tool that can facilitate the examination of bitcoin flaws using visualisation of the blockchain. The tool also allows tracking of spending based on the stored transactions, enabling the identification of patterns of coin flow. **BitIodine** [4] is another tool to analyse blockchain; it parses information and provides a front-end which gives insights into a variety of information. Such information can be basic, like address account (i.e., wallet) balance and total number of transactions, up to more advanced information, like address clustering and address labelling using public information collected from the Internet. Both tools have been tested with success using different set of experimental work and scenarios, demonstrating to be an effective way to analyse and detect patterns within the blockchain and providing a way to improve security or privacy issues.

Blockchain.info [31] is among the most popular and frequently used blockchain analytic tool, having firstly appeared on the market back in 2011. This tool provides some fast and easy-to-use capabilities for tracing individual transactions, while also provides plenty of information, including charts and statistics, about the whole bitcoin network. Ortega [22] used the publicly information from blockchain.info within a certain period in order to de-anonymise addresses from Tor services and proxies. Blockchain.info also delivers information in a convenient way and allows the analyst to tag each transaction with an associated name. Applying clustering heuristics to data provided by blockchain.info and information available on a public bitcoin forum [33], Meiklejohn et al. [34] were able to classify a number of transactions in a user network and perform a traffic analysis on money movement.

Kinkeldey, Fekete and Isenberg [35] developed a system that can be used to recognise a bitcoin network entity based on its public address, regardless if that entity is an individual or an organisation. The tool is called **BitConduite** and utilises the network topology (with its billions of transactions) in order to provide an estimation of an address that could match an entity. Whereas bitcoin can be utilised in various ways – ranging from currency investment to illegal payments – BitConduite can become useful in order to explore and identify the rationality behind bitcoin usage. An analyst that works with BitConduite can perform grouping and filtering based on various attributes and visualise the results in a timeline.

The trade data from cryptocurrency platforms can give interesting insights into money inflows and outflows. The website **bitcoincharts.com** [36] provides financial and technical information linked with bitcoin and has been utilised for analysis of daily trading rates, trends and anomalies [26].

BlockSci [37] is an open-source tool for blockchain analysis which mainly differentiates itself in two-ways. Firstly, it does not use a transactional database. Instead, it uses an analytical built-in memory that promises faster processing. Secondly, while most of the blockchain analytical tools focuses on bitcoin, BlockSci is more versatile and can support multiple blockchains apart from bitcoin, such as Litecoin and ZCash.

Commercial software tools also exist in the market. **Chainalysis** [38] was proposed as an assessment tool allowing assessment of risks associated with bitcoin transactions. It is currently being used by law enforcement in cybercrime investigations involving bitcoin, as it is able to provide links between (a known) source and its recipients [39]. Similarly, **Elliptic** [40] offers software that can connect bitcoin activity to real world identity by utilising a proprietary database with millions of bitcoin addresses. Elliptic is often used by financial

institutions and law enforcement as it offers transactions monitoring capabilities and transparent documentary evidence (including a proprietary database which links bitcoins addresses to web entities) [41].

C. Mapping Tools against the Proposed Thematic Taxonomy

A common theme of the reviewed blockchain analytic tools is the provision of data to meet a range of analysis goals, delivered via different features. Most of the time, a full analysis requires combining data from the blockchain with external data obtained via blockchain analytics, wikis and/or discussion forums. Table I summarises all the tools covered against the taxonomy presented in Fig. 3.

TABLE I. ANALYSIS OF BLOCKCHAIN ANALYTIC TOOLS VS. THE PROPOSED THEMATIC TAXONOMY

Thematic Taxonomy	**Features**	**Tools**
Analysis of Relationships	Transaction Graph Utilised for Address Clustering	• BitIodine • Blockchain.info • BitConduite
	Wallet Explorer Proprietary Database	• Chainalysis • Elliptic
Analysis of Metadata	OP_RETURN	• OpReturnTool
Analysis of Money Flows	Transaction Graph Utilised for Address Clustering	• BitConduite • BitConeView
	Address Tagging	• Blockchain.info • Bitcointalk.org
Analysis of User Behaviour	Profile Rules	• Blockchain Inspector
	Risk Assessment	• Chainalysis
Analysis of Transaction Fees	Transaction Graph	• Blockchain.info • Coindesk.com • BitConeView • BlockSci
	Exchange Rate	• Blockchain.info • Coindesk.com • BlockSci
Analysis of Market / Wallets	Transaction Graph	• Blockexplorer.com
	Trade Data	• Bitcoincharts.com

D. Discussion about Blockchain Analytic Tools

Despite availability of several blockchain analytic tools as reviewed in Sections III-A and III-B, an analysis operation requires aggregation and correlation of different sources of information. Current tools provide very limited support for this and, therefore, analysts are usually required to implement additional tools to achieve their analysis goals. Additionally, to the best of our knowledge, there is a lack of generically-oriented analytic tools for blockchain. Even frameworks claiming to be "generic", such as [42], mainly focus on bitcoin analysis, leaving other cryptocurrencies and purpose-built blockchains outside of their scope.

The majority of the reviewed tools retrieves their underlying blockchain information with the use of BitcoinCore [43]. Thereafter, the data is encapsulated as Java object using Bitcoin J library APIs [44] before processing. However, neither Bitcoin Core nor Bitcoin J is a native tool to offer blockchain analysis. Therefore, a plethora of tools have been under development in order to extract blockchain information from, for example, the API from another existing analytic tool, or from the web page source code. Nevertheless, it seems that all these analytic tools have been consistently focusing on the same specifications and, as a result, their implementation has shown a significant amount of repetition while, at the same time, leaving behind the option of creating a blockchain parsing tool with more abstract objectives.

To summarise, despite the considerable development work to explore and gain wide access to information encoded in a blockchain, the effort has focused too much on bitcoin and a small set of features. Possibly that work could be more effective and efficient through the use of generic-purpose, real-time analytics tools, that would provide the required level of abstraction in order to process a wider range of blockchain data.

IV. OPEN CHALLENGES OF BLOCKCHAIN ANALYTICS

This section discusses challenges of blockchain analytics that are relevant in performing different forms of investigation, such as cybercrime-oriented or (business) economics-oriented. Taking as starting point the summary discussion of Section III-D, it further expands the discussion in different aspects.

A. Big Data Analytics & Real Time Analysis

Blockchain analytics could very well be combined with Big Data. In fact, blockchain could not only benefit data analytics, but also data management. Regarding data analytics, transactions encoded in blockchain could be used as a source for of information. For example, user trading patterns might be extracted with additional prediction of users' potential trading behaviours within the analysis. As for data management, blockchain could be used to store important data as it is distributed and secure. Data provenance is also something that blockchain could ensure. For instance, if blockchain is used to store patients' health information, the information could not be tampered, and it would be hard to steal that private information.

Additionally, blockchain can provide better transparency in data analysis. The difference here is that blockchain will reject an input which is not verifiable and seems to be suspicious. As a consequence, a data analyst will only be dealing with information that is fully transparent. Simply put, a customers' behaviour pattern identified within the blockchain will probably be more accurate compared to those currently being collected in typical databases.

One of the challenges that financial institutions often face is the difficulty to detect fraud transactions, especially on a real time basis [45]. Considering that the blockchain records every transaction and that all remain within the ledger, it could possibly provide a way for real time pattern check. In fact, some of the blockchain analytic tools, such as Chainalysis [38], utilise this real time intelligence for decision making regarding anonymous information. From a privacy perspective, however, questions may arise since it mainly conflicts with the primary motivation for the popularity of cryptocurrencies – anonymity.

B. The Inviolability Challenge & Hidden Suprises

In the archival world, a record could be considered as a trusted one, and provide provisional evidence, when the storage process results from: (1) a consequent routing work of record keeping, with regulations regarding altering or tampering, and (2) the existence of valuable metadata to outline the context and

relevant modification since its creation. However, a challenge exists to keep the records inviolable. In other words, how to protect a record from tampering or unauthorised access, deletion or alteration. Different practices have applied to achieve this over the years, from file content listing to user credentials for access control. However, sooner or later all methods would appear to have open threats for bypassing the rules.

On the other hand, blockchain as a ledger and distributed database can maintain a constantly increasing set of data records that is protected from alteration. What has been noticed though, is that while blockchain in mostly associated with the publication of application-specific transactions – e.g., financial data for bitcoin applications – it can also be used to publish other sort of information as well [46]. As a publishing platform, blockchain is inherently resistant to censorship; once information is published, it is nearly impossible to remove it. Bitcoin users can take advantage of this feature by encoding data into bitcoin transactions, which are then permanently added to the blockchain [47]. Since its very inception, the bitcoin blockchain has had a tradition of political, artistic, or even religious expression. A few examples listed by Shirriff [48] include a speech published in the very first bitcoin block of data, presumably from Satoshi Nakamoto as a political statement regarding it as a response to the weaknesses of centralised financial institutions [49]. The bitcoin mining pool Eligius [50] has also published religious prayer in the blockchain, while the security researcher Dan Kaminsky added an ASCII memorial for cryptographer and privacy advocate Len Sassaman to the blockchain after his death [51].

Possibly these examples can be read as an early stage of a future expansion of use of the blockchain. A way to work out the retrieval of those hidden messages and keep the blockchain independent of record keeping is a promising direction for data analysts to explore.

C. *Blockchain for Law Enforcement*

At the moment, law enforcement attention has mainly been focused on cryptocurrencies, as the other possibilities of application development (e.g., hidden data with criminal content; Section IV-B) do not seem to have reached the real world yet. The main question is how to identify criminal activity by overcoming the anonymity challenge. Indeed, the problem of attribution of identity is possibly the hardest challenge for those investigating cybercrimes and other types of crimes related with computer use and online activities. Decentralised payments, by definition, do not rely on any centralised point to facilitate law enforcement work. For example, a police investigation may result on the suspension of bank accounts, something that is not possible with decentralised payments. However, a company or institution that offers a service for decentralised payments could be under specific regulations, as a result of providing centralised access point. An example could be a currency exchange company that represents an intermediate layer between normal currency (cash) and cryptocurrencies (e.g., bitcoins). Such company could be enforced to comply with specific regulations, like anti-money laundering legislation. In fact, this is a key point regarding identity attribution. Besides the pseudonymity offered by cryptocurrencies, a physical identity is always involved in order to instantiate a wallet or for cashing crypto-coins out.

Blockchain analytic tools can offer law enforcement agencies considerable benefits. It provides the ability for tracing every transaction involved in a given cryptocurrency, including full address history starting from the very first transaction [52]. In that way, law enforcement could have all the needed records in order to trace transferred money, something that would not necessarily be feasible within the traditional economy. Notwithstanding the achieved anonymity that a cryptocurrency can offer, the address of a user's wallet is still a number that will follow the user, so if that can be connected with a particular individual, then the transactions could be identifiable and traceable using that address. However, the challenge of identifying a user is becoming increasingly complex, as a new generation of privacy-oriented cryptocurrencies, like Monero or Zcash [53], is now being used for illegal payments.

Data retention, achieved via blockchain, represents a benefit to law enforcement since it potentially allows a publicly available recording of transactions [54]. It is a continuous challenge for law enforcement the fact that phone and broadband providers apply diverse policies regarding customers' and their related transactions data. In the world of cybercrime, it typically takes a significant amount of time to observe and track someone after an illegal activity, as this might involve record retrieval from different providers, or event data from a range of residencies and jurisdictions. It may happen that the investigator identifies specific records that will match a criminal activity with the suspect, just to realise that their relevance would no longer exist. Such situation would not hold within the blockchain infrastructure, as the records remain in place and unchanged due to blockchain's append-only characteristic.

A challenge that will probably become more and more relevant for law enforcement, however, is the use of different cryptocurrencies for a criminal activity as an intended way to add another layer of complexity for tracking. This means that transactions would be logged in different blockchains. In this case, a universal collection of data from different blockchains would need to be incorporated to today's landscape of features provided by blockchain analytic tools.

D. *Anonymity vs. Pseudonymity*

It seems that the public in general misunderstands the concept of anonymity within virtual currencies. In other words, cryptocurrencies are mainly regarded as anonymous services. Nevertheless, considering the public and transparent nature of blockchain (such as bitcoin), it would be more accurate to describe such services as pseudonymous rather than anonymous. A deeper understanding on the difference in this context would benefit policy-making.

Bitcoin and other cryptocurrencies have introduced a new privacy perspective to financial transactions, compared to the traditional formats based on cash or cards. The key difference is that blockchain is public, although it makes use of pseudonymous identities. Something that creates the possibility of tracing and – theoretically - linking a transaction record with an identity [55]. The potential of linking a transaction with the public blockchain raises a challenge especially for the finance sector as it provides the potential of masking an identity behind transactions.

An interesting perspective regarding linking an entity to a transaction arises from the banking regulations. In traditional banking, there is a specific set of privacy related regulations concerning the sharing of information between banking groups and individuals [56]. No similar regulations apply to

cryptocurrencies yet. However, as they continue to evolve and adapt as an ordinary way of banking, there will be a time when crypto transactions will have to be registered [57], ending up with the same compliance requirements as traditional centralised institutions.

Another challenge facing government regarding cryptocurrencies is the use of anonymity in order to perform money laundering [58]. Money laundering could be broadly described as a part of financial-related activities manipulated to hide the source of the money. It is worth noticing that novel cryptocurrencies are focusing on true anonymity – rather than pseudonymity (such as bitcoin). For example, Zerocoin [59] adopts an anonymous structure, thus presenting a realistic money laundering threat. As a result, the recorded transactions could not be traced like they can for bitcoin, so an investigator will not be able to retrieve currency information regarding a wallet. If research and development of such novel anonymous cryptocurrencies keep evolving, that might trigger the development of regulations regarding bitcoin and other virtual currencies.

E. Mixers and Money Laundry Services

In order to preserve privacy, cryptocurrency users tend to use services called *mixers*. In a typical process, a mixing address receives coins from several different clients and forwards them in a random way to a fresh address for each client [60]. In other words, a cryptocurrency user is allowed to send coins from a certain address towards a mixing service and receive back from the service the same amount of money from a different address or addresses. In a nutshell, such services make the link with the original owner of the money even harder, acting as a "reset button" for wallets and bank accounts. Different approaches are adopted by different mixers.

CoinJoin [61] is a mixing service example where two transactions are joined together to establish a single transaction while input and output will remain unchanged. The concept behind that service is to build a shared transaction, signed from all the participating nodes.

Other mixing services are available like Coinmux [62], but it should be noted that if the service is built on a centralised model, then it might be possible to track and trace an exchange as the system will hold information from all inputs and outputs. A decentralised model is followed by CoinShuffle [63] which does not require a trusted third party.

An extensive study on mixing services was published by Balthasar and Hernandez-Castro [64]. They interestingly identified cases – like the Bitlaunder or Coinmixer – where security can by compromised, reducing the privacy expectations of those services. However, there were other services, like Alphabay or Helix, which showed a considerable level of deficiency. It seems that providing a secure mixing service is a challenging task and that might be evaluated as a positive fact from a law enforcement perspective. On the other hand, there are also legitimate users that are using those services and, in that case, the risk of exposing their anonymity can be quite high.

V. Conclusion & Future Directions

Bitcoin and other cryptocurrencies are adapting the blockchain protocol as peer-to-peer distributed electronic cash systems. Due to the way payment transactions operate over the Internet in a decentralised trust-less system, law enforcement agencies are seeking ways to aid their investigations, especially by tracking and monitoring money and data movements that are involved in cybercrime activities. The ability to use analytic tools on cryptocurrency transactions using blockchain tools is a promising way forward to fight cybercrime.

The goal of this study was to explore the state-of-the art and practice of blockchain analytics. By exploring a variety of tools and techniques available, a thematic taxonomy was proposed and matched against the tools as a way to provide a better understanding of their purpose, and capabilities. It is interesting to observe how a single tool can be utilised for different application purposes, and what kind of information can be revealed using a combination of tools.

The paper has also explored challenges related to blockchain analytics from different perspectives. One of them is the handling of high speed and huge volume of data which becomes increasingly demanding for blockchain analytic tools. Taking advantage of a predictive modelling as a result of big data capabilities, such tools can progress towards being more (pro) active instead of predictive. A merge between the topics of blockchain analytics and big data can layer into a reactive and predictive restructuring which is gradually undertaken in business intelligence science and allows automatic operations of wide areas of background tasks using smart contracts and financial data. In fact, the prognostic analysis from big data can promisingly fit together with the automated execution of smart contracts.

It was uncovered in this study that blockchain transactions can possibly be used to conceal hidden messages which are persistent in the sense that they cannot be deleted or modified. Traditionally, such messages have been used, e.g., to avoid censorship or to make a public statement. However, Matzutt et al. [65] have recently published a study which revealed that illegal material, including links to sites hosting indecent images of children (IIOC) in the dark web, are being published and distributed via the bitcoin public ledger. This development confirms warnings by Interpol [66] in 2015 that harmful content (such as IIOC and malware) could be permanently posted using the blockchain technology. It raises a number of questions since the ledger is downloaded to be processed by miners and then broadcasted for the entire network representing an efficient distribution channel but also a risk for innocent people not knowledgeable of what is happening. Therefore, the implementation of software tools that will be able to efficiently and scalably identify and soundly extract those illegal material as evidence will be an important asset for cybercrime investigation and a powerful forensics tool.

The development of intelligent real-time fraud transaction analytics, as a specialisation of blockchain analytic tools, could also be beneficial for financial institutions and law enforcement. Users of a blockchain-based systems would also benefit with the ability to inspect transactions in real-time with minimal cost. Besides that, an additional challenge will be to make a universal tool that is able to aggregate and correlate different sources of information and different custom-built blockchains.

Blockchain represents a revolution with vast potential for applications to different domains. Law enforcement agencies can adopt two main streams to follow for the investigation of cybercrimes involving this technology. Firstly, a "follow the

money" investigative approach [67], where supporting services such as mixers and currency exchange third-parties represent the centralised weak points. Secondly, as a repository and distribution platform for illegal and harmful material. In both situations, the attribution of identity remains a big challenge, although not impossible to overcome.

REFERENCES

[1] C. Dannen. "Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners." New York: Apress, 2017, p. 47.

[2] A. Heston. "Bitcoin Investing: An Introduction to Cryptocurrency and How to Invest in Bitcoin". PublishDrive, 2018.

[3] G. Hileman, M. Rauchs. "Global Cryptocurrency Benchmarking Study". [Online]. Available: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf [Assessed: 24-1-2018].

[4] M. Spanguolo, F. Maggi, S. Zanero. "BitIodine: Extracting Intelligence from the Bitcoin Network" in Christin N., Safavi-Naini R. (eds) Financial Cryptography and Data Security, FC 2014, Lecture notes in Computer Science, vol. 84347, Berlin: Springer.

[5] A. Doll, S. Chagani, M. Kranch, V. Murti. "Btctrackr: finding and displaying clusters in bitcoin". Princeton University, USA. 2014.

[6] J. Sammons. "Digital Forensics: Threatscape and Best Practices". Waltham: Sygress, 2015, pp. 12-13.

[7] IBM Corporation. "Forward Together: Three ways blockchain explorers chart a new direction". [Online]. Available: https://www-935.ibm.com/services/studies/csuite/pdf/GBE03835USEN-00.pdf [Assessed: 24-01-2018].

[8] R. Merkle. "A digital signature based on a conventional encryption function" in Advances in Cryptology, CRYPTO 87, Santa Barbara, California, USA, August 16-20, 1987, pp. 369-378.

[9] P. Franco. "Understanding Bitcoin: Cryptography, Engineering and Economics" Chichester: John Wiley & Sons, 2014.

[10] S. Nakamoto. "Bitcoin:A Peer-to-peer Electronic Cash System." [Online]. Available: https://bitcoin.org/bitcoin.pdf [Assessed: 14-Oct-2017].

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" [Online]. Available: http://bitcoin.org/bitcoin.pdf [Accessed: 1-Feb-2018].

[12] A. Antonopoulos. "Mastering Bitcoin: Unlocking Digital Cryptocurrencies". Sebstopol: O' Reilly Media, 2014, p. 191.

[13] R. C. Merkle, "A digital signature based on a conventional encryption function," in Advances in Cryptology — CRYPTO '87: Proceedings. Springer Berlin Heidelberg, 1988, pp. 369–378.

[14] D. Gerard. "Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts". David Gerard. 2017, p. 13.

[15] J. Wang, Z. Kissel. "Introduction to Network Security: Theory and Practice". Chichester: John Wiley & Sons, 2015, p. 158.

[16] Castells, M. "Another Economy is Possible: Culture and Economy in a Time of Crisis". Chichester: John Wiley & Sons.

[17] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for bitcoin," 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, 2017, pp. 9-16.

[18] K. Liao, Z. Zhao, A. Doupe and G. Ahn. "Behind Closed Doors:Measurement and Analysis of CryptoLocker Ransom in Bitcoin." in Electronic Crime Research, 2016 APWG Symposium on 2016 Jun 1, Toronto, ON. IEEE.

[19] G. Ahn, A. Doupe, Z. Zhao and K. Liao. "Ransomware and Cryptocurrency: Partners in Crime" in T. Holt (ed.) Cybercrime Through an Interdisciplinary Lens. New York: Taylor & Francis, 2017, pp. 105-126.

[20] M. Ober, S. Katzenbeisser and K. Hamacher. "Structure and Anonymity of the Bitcoin Transaction Graph". Future Internet, vol. 5, no. 2, 2013, pp. 237-250.

[21] F. Reid and M. Harrigan. "Analysis of anonymity in the Bitcoin System. Security and Privacy Social Networks" New York: Springer, 2013, pp. 197-223.

[22] Blockchain Inspector. "What is Blockchain Inspector." [Online]. Available: http://www.blockchaininspector.com [Assessed: 28-11-2017].

[23] Ben-Ari, A. "Outstanding Challenges in Blockchain Technology in 2017". [Online]. Available: https://appliedblockchain.com/outstanding-challenges-in-blockchain-2017/ [Accessed: 1-Feb-2018].

[24] M. Moser and R. Bohme. "Trends, Tips, Tolls:A Longitudinal Study of Bitcoin transaction Fees" in International Conference on Financial Cryptography and Data Security, 2015 Jan 30. Springer, Berlin, Heidelberg.

[25] Coindesk. "About." [Online]. Available: https://www.coindesk.com/about [Assessed: 28-11-2017].

[26] M. Lischke and B. Fabian. "Analysing the Bitcoin Network:The First Four Year". Future Internet, 2016, vol. 8, no. 1.

[27] D. Ron, A. Shamir. "Quantitative analysis of the bitcoin transaction graph." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-642-39884-1_2 [Assessed: 04-04-2018].

[28] Blockexplorer.com. "About block explorer." [Online]. Available: https://blockexplorer.com [Assessed: 28-11-2017].

[29] M. Bartoletti, and L. Pompianu. "An Analysis of Bitcoin OP_RETURN Metadata". arXiv preprint arXiv:1702.01024. 2017.

[30] G. Battista, V. Donato, M. Patrignani, M. Pizzonia, V. Roselli and R. Tamassia. "Bitconeview: Visualisation of Flows in the Bitcoin Transaction Graph" in 2015 IEEE Symposium on Visualization for Cyber Security, VizSec. IEEE Computer Society, 2015, pp. 1-8.

[31] Blockchain. "About." [Online]. Available: https://www.blockchain.com/about/index.html [Assessed: 28-11-2017].

[32] M. Ortega. "The Bitcoin Transaction Graph Anonymity." Master Thesis, Universitat Oberta de Catalunya. [Online]. Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23562/9/msantamariaoTFM0613memoria.pdf [Accessed: 28-11-2017].

[33] Bitcointalk. "Bitcoin Forum." [Online]. Available: https://bitcointalk.org/index.php [Assessed: 28-11-2017].

[34] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" in Proceedings of the 2013 Internet Measurement Conference. ACM: New York, NY, USA, 2013, pp. 127–140.

[35] C. Kinkeldey, J. Fekete and P. Isenberg. "BitConduite: Visualising and Analysing Activity on the Bitcoin Network" Eurographics Conference on Visualization (EuroVis), Posters Track (2017), 2017, pp. 1–3.

[36] Bitcoincharts. "About". [Online]. Available: https://bitcoincharts.com/about [Assessed: 28-11-2017].

[37] H. Kalodner, S. Goldfeder, A. Chator, M. Moser, A. Narayana. "BlockSci: Design and Applications of a BlockChain Analysis Platform". arXiv preprint arXiv:1709.02489. 2017.

[38] Chainalysis. "About." [Online]. Available: https://www.chainalysis.com/#about [Assessed: 02-Dec-2017].

[39] E. Cheng. "Dark web finds bitcoin increasingly more of a problem than a help, tries other digital currencies." [Online]. Available: https://www.cnbc.com/2017/08/29/dark-web-finds-bitcoin-increasingly-more-of-a-problem-than-a-help-tries-other-digital-currencies.html [Assessed: 02-Dec-2017].

[40] Elliptic. "Law Enforcemnet." [Online]. Available: https://www.elliptic.co/law-enforcement [Assessed: 02-Dec-2017].

[41] D. Samburaj. "Bitcoin Blockchain Surveillance Firm Elliptic Raises $5M in Series A Funding". [Online]. Available: https://www.ccn.com/bitcoin-blockchain-surveillance-firm-elliptic-raises-5m-series-funding/ [Assessed: 24-1-2018].

[42] M. Bartoletti, A. Bracciali, S. Lande, and L. Pompianu. "A General Framework for Bitcoin Analytics". arXiv preprint arXiv:1707.01021. 2017.

[43] BitcoinCore. "BitcoinCore: Helping you keep Bitcoin decentralised." [Online]. Available: https://bitcoin.org/en/bitcoin-core/ [Assessed: 28-11-2017].

[44] BitcoinJ. "Introduciton." [Online]. Available: https://bitcoinj.github.io [Assessed: 28-11-2017].

[45] Information Resources Management Association. "Artificial Intelligence: Concepts, Methodologies, Tools, and Applications" IGI Global, 2016, p. 664.

[46] Cox, T. "Blockchain and Potential Implication for International Book Publishing". [Online]. Available: https://publishingperspectives.com/2017/10/frankfurt-blockchain-potential-implications-publishing [Accessed: 1-Feb-2018].

[47] C. DeRose. "Why Blockchain Immutability is a Perpetual Motion Claim." [Online]. Available: https://www.coindesk.com/immutability-extraordinary-goals-blockchain-industry [Assessed: 28-11-2017].

[48] K. Shirriff. "Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software" [Online]. Available: http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html [Assessed: 30-Oct-2017].

[49] Bitcoinwiki. "Genesis Block." [Online]. Available: https://en.bitcoin.it/wiki/Genesis_block [Assessed: 6-Nov-2017].

[50] Bitcoinwiki. "Eligius". [Online]. Available: https://en.bitcoin.it/wiki/Eligius [Accessed: 1-Feb-2018].

[51] M. Hoffman. "The Proposed Virtual Currency Regulatory Framework" in: Comments to the New York State Department of Financial Services on BitLicense. [Online]. Available https://www.eff.org/files/2014/10/21/bitlicense-comments-eff-ia-reddit-hofmann-cover.pdf [Assessed: 28-11-2017].

[52] K. Bheemaiah. "The Blockchain Alternative: Rethinking Macroeconomic Policy and Economic Theory". New York: Apress, 2017, p. 63.

[53] O. Kharif. "Bitcoin is being dropped by criminals in favour of privacy coins like monero". [Online]. Available: http://www.independent.co.uk/news/business/analysis-and-features/bitcoin-latest-updates-price-privacy-coins-cryptocurrency-monero-digital-currency-price-a8137901.html [Accessed: 24-1-2018].

[54] D. Balaban. "How Law Enforcement Can Investigate Bitcoin Related Crimes and Why That's Good". [Online]. Available: https://cointelegraph.com/news/how-law-enforcement-can-investigate-bitcoin-related-crimes-and-why-thats-good [Assessed: 28-11-2017].

[55] S. Gomzin. "Bitcoin for Nonmathematicians: Exploring the foundations of crypto payments." Boca Raton: Universal-Publishers, 2016, p. 60.

[56] Bureau of Consumer Protection. "In brief: The financial privacy requirements of the Gramm-Leach-Bliley Act." [Online]. Available: http://zoo.cs.yale.edu/classes/cs457/backup/cache/www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm [Assessed: 28-11-2017].

[57] Financial Crimes Enforcement Netowrk. "Guidance FIN-2013-G001: Application of FinCen's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." [Online]. Available https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [Assessed: 28-11-2017].

[58] D. Bryans. "Bitcoin and money laundering: mining for an effective solution". India Law Journal, 2014, vol. 89, iss. 1, article 13.

[59] I. Mayers, C. Garman, M. Green and A. Rubin. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" in 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, pp. 397-411. IEEE.

[60] C. Tanas. S. Delgado-Segura, J. Herrera-Joancomartí. "An Integrated Reward and Reputation Mechanism for MCS Preserving Users' Privacy" in J. Garcia-Alfaro, G. Navarro-Arribas, A. Aldini, F. Martinelli, N. Suri (eds) Data Privacy Management, and Security Assurance. DPM 2015, QASA 2015. Lecture Notes in Computer Science, vol 9481, 2016, Springer, Cham.

[61] A. Van Wirdum. "CoinJoin: Combining Bitcoin Transactions to Obfuscate Trails and Increase Privacy" [Online]. Available: https://bitcoinmagazine.com/articles/coinjoin-combining-bitcoin-transactions-to-obfuscate-trails-and-increase-privacy-1465235087 [Assessed: 02-Dec-2017].

[62] Coinmux. "Coinmux." [Online]. Available: http://coinmux.com [Assessed: 02-Dec-2017].

[63] T. Ruffing, P. Moreno-Sanchez, A. Kate. "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin" in Kutyłowski M. Vaidya J. (eds) Computer Security - ESORICS 2014. ESORICS 2014. Lecture Notes in Computer Science, vol 8713. Springer, Cham.

[64] T. Balthasar and J. Hernandez-Castro. "An Analysis of Bitcoin Laundry Services" in H. Lipmaa, A. Mitrokotsa, R. Matulevičius (eds) Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science, vol 10674. Springer, Cham. 2017.

[65] R. Matzutt, J. Hiller, M. Henze, J.H. Ziegeldorf, D. Mullmann, O. Hohlfeld, K. Wehre. "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin" in Proceedings of the 22nd International Conference on Financial Cryptograpghy and Data Security (FC). Springer. 2018.

[66] Interpol. "INTERPOL cyber research identifies malware threat to virtual currencies". [Online]. Available: https://www.interpol.int/News-and-media/News/2015/N2015-033 [Assessed: 06-04-2018].

[67] J. MacRae and V. N. L. Franqueira. "On Locky Ransomware, Al Capone and Brexit" in Proceedings of the 9th EAI International Conference on Digital Forensics and Cyber Crime, LNICST 216, pp. 33-45. Springer, 2017.