2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) | 978-1-6654-3924-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/BRAINS52497.2021.9569824

Study of Blockchain Forensics and Analytics tools

Dinesh Srivasthav P
Cybersecurity and Privacy Research
TCS Innovation Labs
Hyderabad, India
dineshsrivasthav.p@tcs.com

Lakshmi Padmaja Maddali
Cybersecurity and Privacy Research
TCS Innovation Labs
Hyderabad, India
lakshmipadmaja.maddali@tcs.com

Vigneswaran R
Cybersecurity and Privacy Research
TCS Innovation Labs
Chennai, India
vigneswaran.r@tcs.com

***Abstract*—Cryptocurrencies have elicited tremendous interest in the recent past due to their ability to enable financial transactions without the need for a central authority. The most appealing aspect of cryptocurrencies that garnered significant attention is its potential to enable (pseudo) anonymous transactions on the blockchain ledger. Unsurprisingly, this has led to rapid adoption of cryptocurrencies for unlawful activities by malicious actors in several ways. Hence, to detect these unlawful activities, it is essential to analyze the blockchain ledgers to derive insights by investigating anonymous transactions and activities, which is where blockchain forensics comes in. In this paper, we present a taxonomy mapping the identified high-level forensics features with the supporting forensics tools that we surveyed. We provide a comparison of the surveyed tools using three practical parameters (number of cryptocurrencies supported, number of features provided and ease of accessing services) and give an overview of their theoretical effectiveness in general with some open challenges identified.**

***Index Terms*—Blockchain, Cryptocurrency, Analytics Tools, Blockchain Forensics Survey, Crypto Crimes**

I. Introduction

Cryptocurrencies rely on a transparent and immutable ledger, blockchain, that is maintained by a peer-to-peer network of nodes that do not require a central authority to process transactions. Cyber criminals are increasingly adopting and misusing cryptocurrencies to profit from unlawful/malicious activities such as darknet scams, illicit trading, money laundering, ransomware attacks, terrorism financing and so on. According to recent crypto crime report from Chainalysis [1], around 0.34% of total transaction volume is from illicit transactions which amounts to $10 billion dollars. Blockchain forensics investigates and analyzes the huge volume of blockchain data to identify fraudulent and anomalous crypto addresses, transactions, and entities. Several forensics tools, some of which are open-source, and some are proprietary, are available that investigate public ledgers and derive meaningful insights.

Notable works in literature [2] [3] limit exploration to general wallet, block explorers and simple graphical tools and a few basic blockchain analysis tools to a limited extent. However, our survey extends to certain highly functional blockchain forensics and analytical tools and presents a high-level taxonomy comprising of important forensics features which law enforcement agencies, banks and other organizations would need or use to identify deep patterns in the transaction data in order to detect anomalous and fraudulent transactions/entities.

978-1-6654-3924-4/21/$31.00 ©2021 IEEE

II. Taxonomy & Evaluation based on parameters

We explored a total of 13 feature packed forensics and analytics tools of which 6 are open-source; namely BlockSci [4], GraphSense [5], EthExplorer [6], Blockchain Analysis Tool of a Cryptocurrency (BATC) [7], Orbit [8], BlockTag [9], and 7 are proprietary tools; namely Dence Blockchain Investigator (DBI) [10], Cointel [11], ORS Cryptohound [12], CipherTrace [13], Chainalysis [14], Elliptic [15], Blockchair [16]. We categorized key forensics capabilities into four broad categories: in-depth investigation, identify high-risk activity, real-time analysis and strong audit trail as depicted in Table I.

Each of these tools has an individual focus area. For example, EthExplorer is specifically designed to analyze only the Ethereum blockchain and smart contracts, which most of the other open-source tools do not support. Similarly, BlockTag is developed as a tagging system to tag entities to real-world identities, and BlockSci focuses on providing a fast programming interface enabling users to run their own queries. In order to make a meaningful comparison, we identified three broad, practical, parameters that we believe are important considerations in choosing a tool: number of cryptocurrencies supported, number of high-level features provided (as depicted in Table I) and ease of accessing services (like REST APIs, integration feasibility, public deployments for testing etc.).

Considering these parameters, we identify GraphSense as a better open-source tool as it supports a good number of cryptocurrencies and maximum features among the explored tools. Though BlockSci is equally good, the support and development of this tool was terminated in November 2020 [17] while GraphSense has an active development team providing incremental features besides having REST API support.

GraphSense supports Bitcoin, Bitcoin Cash, Zcash, Litecoin, and Ethereum. It traces monetary flows, gives out detailed transaction history, and allows visual analysis through a web interface. It allows for path, graph pattern search to track interactions between crypto addresses to detect anomalous points. It uses techniques such as address clustering – to group related addresses, transactions, and address tagging – to link them to probable real-world entities (such as exchanges,

TABLE I
TAXONOMY OF HIGH-LEVEL FEATURES AND THE SUPPORTED FORENSICS TOOLS

Taxonomy	**In-depth investigation**					**Identify high-risk activity**					**Real-time analysis**		**Strong audit trail**
Features	**Block/ Transaction/ Address exploration**	**Flow of currency**	**Address clustering**	**Address tagging**	**Visualization analysis**	**Pattern finding**	**Anomaly detection**	**AML compliance**	**Risk assessment**	**Actionable insights**	**Alerts of suspicious activities**	**Monitor target entities**	**Generation of Full audit trail/ SAR/STR Investigation reports**
Opensource Tools													
GraphSense	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
BlockSci	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
BATC	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Orbit	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
EthExplorer	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
BlockTag	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗
Proprietary Tools													
DBI	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Cointel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ORS Cryptohound	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓
CipherTrace	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chainalysis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Elliptic	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Blockchair	✓	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗

gambling services, miners etc.) based on contextual information available from certain public data sources. It currently leverages Blocksci's address, transaction hash mapping with integer IDs and a component called "parser" for parsing blockchains. GraphSense helps to identify if a particular address/entity is illicit based on the predefined categories. However, if a legitimate address becomes illicit at a later point, it cannot notify the earlier interacted users or specifically track a blacklisted address and give alerts to the users if it gets involved in any suspicious activity. Being a steadily evolving system, it also has some unresolved limitations such as lack of support for real-time investigations as grouping of addresses and recomputing the address graphs with entities often takes several hours.

Open-source tools in general lack the high-level forensics functionalities available in proprietary tools that greatly influence the effectiveness of a tool such as making predictions using the past activities of an address, vulnerability detection, anti-money laundering (AML) compliance, real-time monitoring, risk analysis by calculating risk scores and subsequent categorization and provision of actionable insights, generation of complete audit trails and suspicious activity, transaction reports (SAR, STR) etc. Among the proprietary tools, Elliptic, Cointel, CipherTrace and Chainalysis are very much similar in functionalities and are better than any other mentioned tools.

We also identified certain open challenges of forensics tools, namely huge hardware requirements to parse and process massive blockchain data, difficulty of real-time analytics mainly in terms of speed and accuracy owing to the increasing blockchain's size, support for a variety of cryptocurrencies as they differ in their conceptual designs, complexity of cross-ledger analytics as tracking monetary flows and linking multiple transactions/addresses across different ledgers will be very difficult especially when privacy enhanced cryptocurrencies such as Zcash [18] are involved.

III. CONCLUSION

In this paper, we highlighted certain important forensics functionalities that are needed by law enforcement agencies, banks, and users but are lacked by existing open-source tools. This could be due to a variety of reasons such as the tool's agenda, funding etc. Although a few proprietary tools support these features, they may not be customizable and would be expensive. There are also certain open-challenges of forensics tools as stated. Hence, there is a need for more research in this direction to identify novel techniques addressing these gaps and challenges.

REFERENCES

[1] Chainalysis Crypto Crime 2021 Report: https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf. Retrieved July, 2021.

[2] Balaskas, *et.al*. Analytical tools for blockchain: Review, taxonomy and open challenges. In 2018 International Conference on Cyber Security and Protection of Digital Services (pp. 1-8). IEEE.

[3] Callum Eden. (2019). SherBlock Holmes: Digital Blockchain Forensics. Imperial College London. https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1819-ug-projects/EdenC-Sher(b)lock-Holmes-Digital-Blockchain-Forensics.pdf

[4] Kalodner, *et.al* (2020). BlockSci: Design and applications of a blockchain analysis platform. In 29th USENIX Security Symposium (pp. 2721-2738).

[5] Haslhofer, *et.al*. (2016, September). O Bitcoin Where Art Thou? Insight into Large-Scale Transaction Graphs. In SEMANTiCS (Posters, Demos, SuCCESS).

[6] Marchenko, *et.al* (2019, November). EthExplorer: A Tool for Forensic Analysis of the Ethereum Blockchain. In European Workshop on Performance Engineering (pp. 100-117). Springer, Cham.

[7] Werner, R., *et.al*. Blockchain Analysis Tool of a Cryptocurrency. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (pp. 80-84).

[8] Orbit: https://github.com/s0md3v/Orbit, Retrieved July, 2021.

[9] Boshmaf, *et.al*. BlockTag: design and applications of a tagging system for blockchain analysis. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 299-313). Springer, Cham.

[10] dence GmbH: https://www.dence.de/en/products/virtual_currencies.

[11] Cointel: https://cointel.eu. Retrieved July, 2021.

[12] ORS Cryptohound: https://www.orsretail.ai/cryptohound/, Retrieved July, 2021.

[13] CipherTrace: https://ciphertrace.com/. Retrieved July, 2021.

[14] Chainalysis: https://www.chainalysis.com/. Retrieved July, 2021.

[15] Elliptic: https://www.elliptic.co/. Retrieved July, 2021.

[16] Blockchair: https://blockchair.com/. Retrieved July, 2021.

[17] BlockSci: https://github.com/citp/BlockSci#blocksci. Retrieved July, 2021.

[18] Zcash: https://z.cash/. Retrieved July, 2021.