BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2017
http://excel.fit.vutbr.cz

Activity alarm for cryptocurrency blockchains

Lukáš Vokráčko*

Abstract
Cryptocurrencies are becoming increasingly popular and demand for monitoring transactions inside them increases alongside with it. In this article, I will discuss existing solutions for monitoring transactions and describe application Cryptoalarm designed for monitoring transactions in systematic manner. Cryptoalarm scans blockchains of cryptocurrencies such as Bitcoin, Bitcoin Cash, Litecoin, Ethereum, Zcash, DASH and sends notifications about address activities in real-time.

Keywords: Cryptocurrency — blockchain — transaction

Supplementary Material: Downloadable Code

*lukas@vokracko.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

Cryptocurrencies are distributed and pure virtual alternative to fiat currencies issued and backed by governments. Unlike any fiat currency, cryptocurrencies are based on distributed network and do not require trust among its users. They are secured by strong cryptography, which prevents potential attackers from forging new coins. They are also immune to regulations and do not allow authorities to freeze funds or to disallow transactions for specific people or groups. So far most users of cryptocurrencies have been people interested in the underlying technology or people seeking refuge from the old-fashioned banking system or even the governments for various reasons. Demand for tracking transactions grows alongside with cryptocurrencies' popularity as it is standard feature available to all cashless transactions in fiat banking. Blockchain (the technology behind majority of cryptocurrencies) is by its nature transparent, meaning everyone can see details of every transaction, and thus allows such tracking.[1]

[1]There are several cryptocurrencies that by default obscure transaction details with another layer of cryptography. They are not included in this work.

This work's focus is placed on real-time transaction monitoring within few of the most popular cryptocurrencies, namely Bitcoin, Bitcoin Cash, Litecoin, Dash, Zcash and Ethereum. The result of this work are an application *Cryptoalarm* for real-time transaction monitoring and web application providing user interface to manage address watchlists. This application can be useful for tracking movements of illegal funds for governments, financial institutions or law enforcement agencies.

This application is developed as part of project TARZAN [1], a set of tools for forensic analysis of cryptocurrencies.

2. Cryptocurrency

Cryptocurrencies are relative new field that was started by a work of Satoshi Nakamoto, who published paper about the first cryptocurrency called Bitcoin [2], a currency that most other cryptocurrencies are built on top of. Cryptocurrencies are based on distributed peer-to-peer model, where participants do not need to trust each other. Cryptocurrencies are not governed by a single authority but rather by a network consen-

sus. They are not affected by artificial inflation (or have exactly defined inflation) and prevents potential disputers to forge new coins by using cryptographic principles. None of above-mentioned properties are present in a fiat-based banking system. There is also a downside to cryptocurrencies. It is not possible to deal with misplaced transactions, lost account credentials or theft without an authority. It is possible only to track movements of stolen coins. Ability to recover coins would undermine the core idea of cryptocurrency - no central authority. All cryptocurrencies supported by *Cryptoalarm* are built on top of blockchain.

2.1 Blockchain

Blockchain is a data structure used by majority[2] of cryptocurrencies to store transaction data. Blockchain consists of connected blocks, where each block references its direct predecessor. Every new block is attached to the blockchain and is secured by a proof-of-work[3], or so-called mining (a process of solving a cryptographic puzzle that secures the blocks integrity).

Everything stored on blockchain is transparent. It is a property wanted in some use cases (e.g. public funding) and unwanted in others (e.g. personal finance). There is a protocol built on top of blockchain that manages anonymization of transactions and their respective amounts: CryptoNote. CryptoNote [3] provides another layer on top of blockchain to achieve it. In this work, I will place focus only on cryptocurrencies that use blockchain without obscuring transaction details.

2.2 Identity pairing

Cryptocurrencies are by nature anonymous (pseudonymous - identified by pseudonym). There is no requirement for users to pair their real or virtual identity with addresses. Unlike in banking system. One way how to pair user's address with the real identity is to request user information from exchange. This can be applied only for exchanges that require user verification. For some exchanges, it is not needed at all. Other require verification only after certain volume of trades is exceeded. Exchanges can also be outside of state jurisdiction and do not need to comply with court orders.

To get at least partial identity, one can find information about users at web pages, where users have public profiles. The best place to look for user identities is where cryptocurrencies are discussed. In some cases, users provide their cryptocurrency addresses in their profiles. From this information, one can obtain usernames paired with cryptocurrency addresses. And as users tend to use the same username across several services those profiles can be linked together. This can give out user's possible identity in case service shows (most likely) real user information. Facebook can be used as an example. Some users have their username same set as custom URL their profile (http://facebook.com/<username>).

Another way to get more information about user's identity is to find given user on website that operates inside a state's jurisdiction. Authorized law enforcing personal can request information with court order from service's provider. This way authority can get an IP addresses associated with user. Next, network traffic of given IP address can be inspected for cryptocurrencies transactions.

3. Existing solutions

There are already two types of existing tools for analyzing the content of cryptocurrencies: blockchain explorers and transaction notificators. They are described in following paragraphs.

Blockchain explorers can be used to browse cryptocurrency blockchain in a web browser. They allow users to search for the specific transaction or address by hash. They provide a list of all transactions for a given address. This can useful for user who wants to know details about transactions of single address. It is not possible to search for multiple addresses simultaneously and user must perform one search for each address. There is also no possibility to send notifications when transaction (or any other event) occurs. Each cryptocurrency has own blockchain explorer, which makes systematic transaction monitoring more fragmented. One of many Bitcoin's blockchain explorers is Blockchain.info[4].

Another set of existing tools is based on sending notifications when specified address is recipient of transaction. It can be useful for user, who wants to be notified about incoming transactions, but is far from ideal solution for tracking a large number of addresses across multiple cryptocurrencies in systematic manner. User can not specify type of involvement he wants to be notified about (sender/receiver). Notifications are sent as emails. There is not an API for push notifications which would be better suited for effective processing. Another problem is that these services provide monitoring only on small set of cryptocurrencies. Majority of them supports only Bitcoin thus, there is

[2] Some cryptocurrencies use Hashgraph or Tangle

[3] There is also another way how to secure blocks called proof-of-stake

[4] https://blockchain.info/

no way for user to monitor transactions in other cryptocurrencies. BitNotify[5] is one of these services.

Both types of these tools have several problems that are solved in new application developed for transaction monitoring — *Cryptoalarm* 4.

4. Cryptoalarm

New application *Cryptoalarm* is designed to solve problems of both above mentioned sets of tools while keeping their advantages. Cryptoalarm can monitor activities in broad spectrum of cryptocurrencies in real-time and on large sets of addresses. Cryptoalarm also supports multiple notification types with customized filters.

4.1 Features

Cryptoalarm enables user to perform a real-time transaction monitoring. Currently, there are six supported cryptocurrencies: Bitcoin [2], Bitcoin Cash, Litecoin, Ethereum [4], Zcash [5] and Dash [6].

User can set-up unlimited number of watchlists for each of these cryptocurrencies with specific filtering. Watchlist can be set to trigger notification, when address is involved in transaction as sender, recipient or in both cases. Notifications can be sent as emails or as REST call. REST notifications are especially designed to connect with another processing tools as they are easily parsed. Application connected to REST notification only needs to listen on specified URL and does not have to make repeated requests. Notifications are sent in bulk after customizable time period. This will save user's inbox in case of email notifications. Notification interval can be set to zero making notifications instant. Link to blockchain explorer is provided for every hash in email notification.

Cryptoalarm can recover in case of network issues. Failed requests are repeated in specific delay when connection problems are detected. This delay is doubled after every unsuccessful connection until it reaches maximum threshold. Subsequent delay becomes constant after reaching maximum threshold until successful connection is established.

Cryptoalarm iterates over every block until it reaches the last processed block. This can be effectively used to scan every block of blockchain by setting last processed block to genesis block.

4.2 Operations

Cryptoalarm is connected to cryptocurrencies underlying network nodes. The node provides RPC API and defines set of operations to obtain information about blockchain. This node is pooled by Cryptoalarm for information about a new block. The pooling is done in intervals that correspond to block time of given cryptocurrency which means new block can be detected almost immediately. Transaction information are obtained when a new block is detected. Transaction's input and outputs are then determined and normalized to unified format. For Ethereum, input and output of transaction is obtained directly from transaction data structure. It is necessary do additional processing to get input addresses for Bitcoin based cryptocurrencies. Bitcoin stores transaction inputs as pointers to previous transaction's outputs. To determined input address for a given transaction, another RPC request must be performed. Exact process is shown in algorithm 1. Inputs and outputs are then compared to a set of watched addresses and notifications are sent in case of a match.

Algorithm 1 Determine input addresses for transaction in Bitcoin based cryptocurrencies

Require: block - transaction's block
Require: N - transaction's index in given block
  $txid \leftarrow block[\text{"}vin\text{"}][N][\text{"}txid\text{"}]$
  $index \leftarrow block[\text{"}vin\text{"}][N][\text{"}vout\text{"}]$
  $tx \leftarrow get\_raw\_transaction(txid)$
  $tx\_out \leftarrow tx[\text{"}vout\text{"}][index][\text{"}scriptPubKey\text{"}]$
  return $tx\_out[\text{"}addresses\text{"}]$

4.3 Design

Cryptoalarm is designed to monitor each cryptocurrency in separated thread. Reason for this design is variety of block times and processing time required for every block. This is especially important for Bitcoin as it is currently the most used cryptocurrency. Bitcoins blocks are generally full (there is a limit of how much transactions can fit into one block) and given the way Bitcoin stores transaction inputs, it requires significantly more time to process single block (also depends on network delays).

Cryptoalarm is split into several classes:

Cryptoalarm handles threading and is responsible for block and transaction processing.
Coin implements communication with RPC API of cryptocurrency network node.
Notifier handles watchlists (that are periodically updated) and sending notifications.

There is a class derived from *Coin* for each supported cryptocurrency. Class diagram is shown in figure 1. Application can be easily extended to monitor activities in another cryptocurrencies. Following

[5] http://bitnotify.com

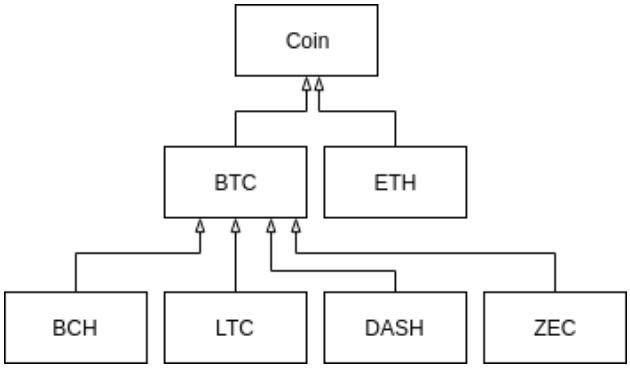

Figure 1. Coin inheritance diagram.

methods need to be implement for every new cryptocurrency:

- `get_last_block_number`
- `get_block`
- `get_block_transactions`
- `get_transaction_io`

Only block time and URL of RPC node is required to specify for majority of cryptocurrencies based on Bitcoin. Most of Bitcoin based cryptocurrencies only differ in following attributes:

- block time
- block size
- mining algorithm
- block rewards

There are 227 cryptocurrencies based on Bitcoin (and another 346 already abandoned) according to MapOfCoins [7] at the moment of writing this article.

5. Web application

Web application is primarily designed as user interface for *Cryptoalarm*. There are two another parts implemented in web application:

- Address matcher
- Identity parser

In web application, users can specify watchlists and is used as receiver for REST notifications by default. Dashboard view shows latest transactions of every address that user set-up a watchlist for. Dashboard view is shown in figure 2. Watchlist represents a single address. In watchlist, users can specify type of notification (email, rest, both), involvement type (input, output, both) and email template. Watchlist view also shows latest transactions on given address and all paired identities obtained by Identity parser 5.2. Each hash in web application (address, transactions) points to a blockchain explorer of given cryptocurrency. Watchlist view is shown on figure 3.

5.1 Address matcher

Address matcher is a tool for identifying which cryptocurrency address belongs to. Address matcher is to enhance user experience when creating new watchlists. This way, cryptocurrency is identified from address format and user does not have to selected it manually. Another utilization is in Identity parser 5.2 where it is used to create identity in correct cryptocurrency.

Address identification is ambiguous in some cases. Those cases are addresses of Bitcoin, Bitcoin Cash, Litecoin and other cryptocurrencies based on Bitcoin as they have the same address format. In this case all possible cryptocurrencies are returned.

5.2 Identity parser

Identity parser is used to find users associated with cryptocurrency addresses. Bitcointalk[6] parser is developed for this exact purpose. Bitcointalk is one of the most popular website by cryptocurrencies's users. It is a place where users discuss development of existing cryptocurrencies or new ones.

Identity parser works by visiting all user profiles and parses username and everything that fits the format of cryptocurrency address. For this address matcher is utilized. Users' identities are then shown in watchlist if they match with watched address. Identity parser uses selenium library to obtain page source. Identity parser can be set-up as a cron job that parses new profiles since the last run. Another use case is to parse all profiles each run. This way, the most accurate database of identities can be built as users can update their profile with new addresses.

Cryptoalarm comes with all identities obtained from Bitcointalk forum by default.

6. Conclusions

To satisfy increasing demand for transaction monitoring inside cryptocurrencies' blockchains I've developed application *Cryptoalarm*. *Cryptoalarm* can perform transaction monitoring in several cryptocurrencies and send real-time notifications about address activities. *Cryptoalarm* is designed for large scale monitoring in a systematic manner. It can be used by government, banking institutions or information agencies to monitor movements of funds on problematic addresses. Addresses of ransomware or malware crypto miner are good examples for *Cryptoalarm's* usage.

[6] http://bitcointalk.org

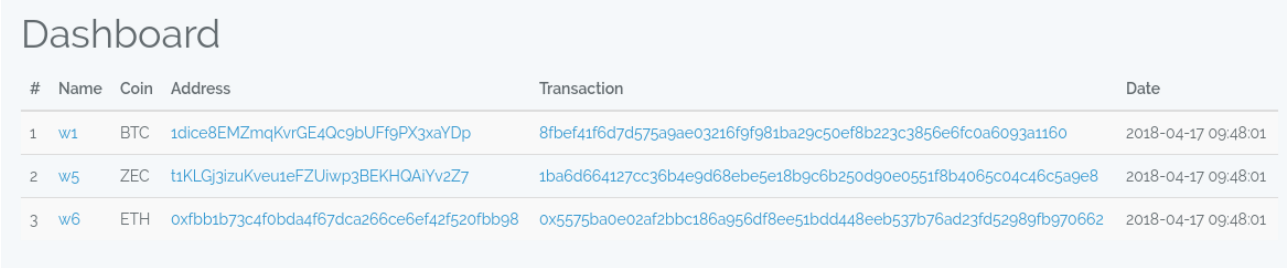

Figure 2. Preview of web application - dashboard

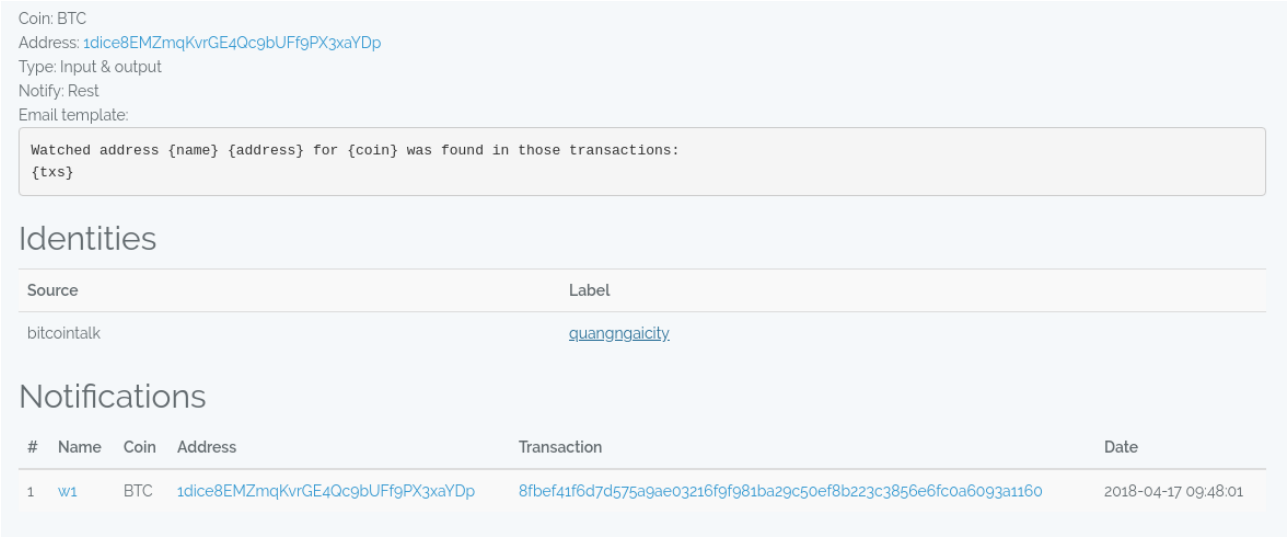

Figure 3. Preview of web application - watchlist

6.1 Following work

I will focus on monitoring transactions inside Ethereum smart contracts as there can be performed transfer of tokens in following work. Another feature to be implemented is chain split detection and recovery. RPC node can be out of synchronization with the main chain but all main chain transactions must be processed when node becomes synchronized again.

Acknowledgements

I would like to thank my supervisor Ing. Vladimír Veselý, Ph.D. for his help.

References

[1] *Integrated platform for analysis of digital data from security incidents*. [Online; visited 20.4.2018].

[2] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online; visited 10.12.2017].

[3] Nicolas van Saberhagen. *CryptoNote v 2.0*. [Online; visited 10.12.2017].

[4] Vitalik Buterin et al. *A Next-Generation Smart Contract and Decentralized Application Platform*. [Online; visited 10.12.2017].

[5] *Zcash: Technology*. [Online; visited 19.12.2017].

[6] Evan Duffield and Daniel Diaz. *Dash: A Privacy-Centric Crypto-Currency*. [Online; visited 11.12.2017].

[7] *MapOfCoins - View the Bitcoin cryptocurrency specifications in detail*. [Online; visited 20.04.2018].