From Innovations to Prospects: What Is Hidden Behind Cryptocurrencies?

Ang Jia  
jaiaang@stu.xjtu.edu.cn  
Xi’an Jiaotong University  
School of Cyber Science and Engineering

Ming Fan  
mingfan@mail.xjtu.edu.cn  
Xi’an Jiaotong University  
School of Cyber Science and Engineering

Xi Xu  
xx19960325@stu.xjtu.edu.cn  
Xi’an Jiaotong University  
School of Cyber Science and Engineering

Di Cui  
cudi@stu.xjtu.edu.cn  
Xi’an Jiaotong University  
School of Cyber Science and Engineering

Wenyiing Wei  
wwyhphr@163.com  
Xi’an Jiaotong University  
School of Cyber Science and Engineering

Zijiang Yang  
zijiang.yang@wmich.edu  
Western Michigan University  
Department of Computer Science

Kai Ye  
kaiye@stu.xjtu.edu.cn  
Xi’an Jiaotong University  
School of Electronics and Information Engineering

Ting liu  
tingliu@mail.xjtu.edu.cn  
Xi’an Jiaotong University  
School of Cyber Science and Engineering

ABSTRACT

The great influence of Bitcoin has promoted the rapid development of blockchain-based digital currencies, especially the altcoins, since 2013. However, most altcoins share similar source codes, resulting in concerns about code innovations. In this paper, an empirical study on existing altcoins is carried out to offer a thorough understanding of various aspects associated with altcoin innovations. Firstly, we construct the dataset of altcoins, including source code repositories, GitHub fork relations, and market capitalizations (caps). Then, we analyze the altcoin innovations from the perspective of source code similarities. The results demonstrate that more than 85% of altcoin repositories present high code similarities. Next, a temporal clustering algorithm is proposed to mine the inheritance relationships among various altcoins. The family pedigrees of altcoins are constructed, in which the altcoin presents similar evolution features as biology, such as power-law in family size, variety in family evolution, etc. Finally, we investigate the correlation between code innovations and market capitalization. Although we fail to predict the price of altcoins based on their code similarities, the results show that altcoins with higher innovations reflect better market prospects.

KEYWORDS

Altcoins, Innovations, Relation, Prospects

ACM Reference Format:

1 INTRODUCTION

The great influence of Bitcoin has promoted the rapid development of blockchain-based digital currencies (cryptocurrency) since 2013. There are three critical features for existing cryptocurrencies: 1) Large variety, in August 2019, the number of available cryptocurrencies is over 2300 and it is still growing quickly[3]. 2) Fast delivery, the number of ICOs2 (initial coin offering) newly increased per month is more than 60 since 2018. 3) Huge price change, a drastic fluctuation occurred in Bitcoin when it reached a peak of more than 20000$ on Dec 17, 2017, and fell to 3830.04$ on Dec 30 2018[5]. The three features have raised concerns about the quality of the cryptocurrencies and the real value of them.

The cryptocurrency world has experienced a complicated evolution since its birth. Bitcoin is the first cryptocurrency and now accounts for nearly 70% of the market[7]. The later cryptocurrencies can be divided into two categories: Alternative Cryptocurrency Coins (Altcoins) and Tokens[4]. Altcoins refer to the coins that are alternatives to Bitcoin. Usually, they have their own chains. However, tokens serve the blockchain and they are often built on top of another blockchain such as the Ethereum blockchain. In this study, we only focus on altcoins. According to the source of

1https://bitcoin.org/
2https://en.wikipedia.org/wiki/Initial_coin_offering
altcoins, they can be divided into two groups: the variant of Bitcoin and the cryptocurrency with self-developed Blockchain[4]. The majority of altcoins are variants (forks) of Bitcoin, built using Bitcoin’s open-sourced, original protocol with changes to its underlying codes, therefore conceiving an entirely new coin with a different set of features. Other altcoins are not derived from Bitcoin’s open-source protocol. Rather, they have created their own blockchain and protocol that supports their native currency.

To determine whether a cryptocurrency should be invested, one key point is the code innovation. According to a report[1] released in September 2018, there exist great similarities between altcoins, i.e., "the code underpinning more than 90% of the projects shared a similarity score of at least 80%". The severity of code clone raises concerns about the innovation of altcoins. However, investors only focus on market trends and ignore the implementation details of the codes. Moreover, existing studies that analyze the cryptocurrency only focus on the technical issues, and they would ignore the code innovation. In addition, what is amazing for technologists is that the value of a technology product seems to have nothing to do with the technology’s most direct vehicle, i.e., the code. Therefore, it is non-trivial to gain an understanding of the altcoin innovations, so well as their relation with the market prospects.

In this work, we aim to offer a thorough understanding of the various aspects associated with innovations of different altcoins. Specifically, we first construct our dataset by crawling three different types of data from GitHub and CoinMarketCap[3], including source code repositories, GitHub fork relations of repositories and market capitalization (market cap) of altcoins. To conduct a thorough analysis, we empirically study the altcoin codes by answering three research questions listed below.

**RQ1:** To what extent the codes are shared by altcoins?

**Innovations.** Many altcoins describe themselves with identical and innovative features and the ability to serve as better alternatives to Bitcoin. This ability actually lies in innovations of their implementation, i.e., source codes. However, it remains unknown what extent they share codes with other existing cryptocurrencies. Therefore, at the first step, we would like to offer an overview of the duplication in altcoin codes implemented in C++ (the largest part) to solve the RQ1.

**RQ2:** What is the relation between altcoins?

**Relations.** Software developments mostly do not start from scratch. Altcoins may also stem from one or many templates. Therefore, many altcoins may share similar source codes. However, the similarities between them cannot reveal the process of their inheritance. Although existing clustering algorithms offer clustering analysis of similar individuals, they ignore the sequence of input instances and cannot be applied in our work directly. In the second step, we aim to conduct the familial analysis of altcoins to further explore their inner relation by answering RQ2.

**RQ3:** What is the correlation between prospects and innovations?

**Prospects.** Same with rules of nature that similar organisms will compete for the same resources, altcoins implemented with the same codes are more likely to suffer the same competitions. Therefore, innovations may play an important role in affecting the prospects of altcoins. However, the complicated environment in the cryptocurrency world makes it hard to understand it directly. At the last step, we are willing to offer a deep insight into the correlation between prospects and innovations by answering RQ3.

**Contributions:** Our main contributions are list below:

(i) To the best of our knowledge, our empirical study for the first time investigated the innovations of altcoins from the view of source code, and we proposed a novel temporal clustering algorithm to mine the inner relations between altcoins by constructing family pedigrees.

(ii) We investigate the correlations between the altcoin innovations and their market capitalization from the view of code similarity. The results show that the altcoins with high innovations reflect better market prospects and, the cryptocurrency world is moving toward diversity.

(iii) We release the dataset of altcoin including the source code repositories, GitHub fork relations, and market caps. The dataset can be accessed from GitHub[5].

**Overview of the paper:** Section 2 presents an motivating example. Section 3 presents the construction of our dataset and its statistic result. Section 4 introduces the study results by answering the three research questions. After the discussing of the related work and threats to validity in Section 5 and Section 6, we conclude our paper in Section 7.

2 MOTIVATING EXAMPLE

This section motivates our research using a real-world example. StrikeBitClub[4] and HollyWoodCoin[3] are two altcoins, where StrikeBitClub is a hybrid scrypt PoW + PoS based one and HollyWoodCoin is a PoS-based one[7]. Table 1 shows the collected information of this two cryptocurrencies. They are both released in December 2017, they both suffer a huge price loss from December 2017 to September 2018.

<table>
<thead>
<tr>
<th>Table 1: StrikeBitClub and HollyWoodCoin</th>
</tr>
</thead>
<tbody>
<tr>
<td>currency</td>
</tr>
<tr>
<td>release time</td>
</tr>
<tr>
<td>price(release)</td>
</tr>
<tr>
<td>price(2018/4)</td>
</tr>
<tr>
<td>status(2019/8)</td>
</tr>
</tbody>
</table>

The source code repositories of these two altcoins and their GitHub fork information are crawled on 28 March 2018. They do not indicate GitHub fork relation between their repositories or to other repositories. However, using textual code clone detection, the two repositories share about 97% of codes.

The ‘coincidences’ in their codes, their release times, and their price loss inspire us to carry out studies to further mine the hidden phenomena. Altcoins are running based on similar techniques, and these two altcoins have similar source codes, which inspire us to explore the innovations of other altcoins and the relation between these altcoins. Companies with the same technology in the same

---

industry will compete for the same resources and these two similar altcoins suffer a decline in the price, which raises our exploration about the relation between code innovations and market prospects in the cryptocurrency world. To illustrate our approaches to solve these questions, we introduce our dataset in section 3, and our study in section 4.

3 DATASET
This section presents details of the dataset. We crawl source code repositories, Github fork relations, and market caps of all altcoins from GitHub and CoinMarketCap.com to construct our dataset. The process of dataset construction and statistics of the dataset will be illustrated in the following subsections.

3.1 Dataset Construction
Source Code Repositories: By 4 April 2019, more than 3000 cryptocurrencies have emerged. Bitcoin has about 20,000 commits and more than 200 release versions. We collect all versions of the cryptocurrencies (including Coin and Token) to construct our dataset. Source code repositories of these cryptocurrencies were accessed through the following steps. First, we accessed the website of each cryptocurrency on CoinMarketCap.com and got their GitHub links. Then we accessed the GitHub links and identified if it is a repository or repositories. If it is a repository, we will download this repository; otherwise, we will download the pinned repositories or (if the pinned repositories do not exist) the first three repositories.

Market Capitalization: We obtained the historical closing prices and the market capitalization of all cryptocurrencies by crawling the website coinmarketcap.com. We use Node.js to crawl the information and store them in JSON format.

GitHub Fork Information: The distinction between GitHub fork and blockchain fork needs to be explained. A fork in GitHub is a copy of a repository. A fork in the blockchain is when a change is made to the software of a cryptocurrency to create another version of the blockchain, technically [2]. Bitcoin hard forks (blockchain fork) leads to the creation of many altcoins, such as Bitcoin Cash, Bitcoin Gold, etc. When an altcoin is a product of Bitcoin hard forks, there may be fork relation (in GitHub) between their repositories. We would like to collect the fork relation between all altcoins before analyzing their code similarity relation. We query the GitHub API to obtain information of their repositories. Results are structured in JSON format, and the fork relation can be obtained from its "parent" node.

3.2 Statistics of Dataset
By 4 April 2019, there come up 3338 cryptocurrencies (including coin and token). Among them, 1253 have opened their code links and 1230 cryptocurrencies set GitHub repositories as their links. Using the method in Section 3.1, we successfully access 1698 repositories belonging to 1023 cryptocurrencies (some links are invalid or unable to open). Among them, more than 40% (693 in 1698) have only one release and the repository bitcoin/ bitcoin of Bitcoin has the largest number of releases as 216 times.

We try to crawl the information (created time, language, and fork) of these 1698 repositories using GitHub API, but information of 989 repositories are successfully accessed. Among these 989 repositories, 865 repositories are labeled with a specific language. Figure 1 shows the proportion of languages used in these repositories. Among the labeled 865 repositories, 440 repositories are labeled that its primary language is C++, and 185 repositories’ main language is JavaScript. Other languages used in more than 20 repositories are C, Go, HTML, Java, Python, and TypeScript.

We also analyze their created times from our obtained statistics. Figure 2 shows the number of repositories written in different languages during different periods. It indicates enthusiasm for creating repositories (including coin projects and token projects) since 2017. While the creating of all repositories arrives at its peak during 2017/11/30 to 2018/6/1, creating of C++ written repositories reaches its peak during 2019/6/1 to 2018/11/30. Moreover, from 2017/11/30 to 2018/6/1, there arise 239 repositories, which means a repository are created every 1.5 days.

Figure 3 shows changes in total market capitalization and the number of cryptocurrencies. The market capitalization of cryptocurrency experience a pull-up from 2017/1 to 2018/1 and a plunge after 2018/1. Besides, the number of newly-created repositories indicates a similar experience with a slight delay. The cryptocurrencies spring up like mushrooms after the rain of market expansion, which may introduce some hidden troubles in the way to maturity.

4 STUDY DESIGN AND RESULTS
The overview of our study is presented in figure 4. First, we acquire market caps and source code repositories of different cryptocurrencies from CoinMarketCap.com and GitHub. Then, we select repositories written in C++ (the largest part) and then calculate the similarities between them. Next, we propose a novel clustering algorithm combined with temporality to construct families of cryptocurrencies based on code similarities. Finally, we compare the market and prospects with their code similarities and relations. This section elaborates on the details of the dataset.

We present the study results by answering three research questions. For each question, we present the motivation behind the research question, the approach, and a discussion of our findings.

4.1 To what extent the codes are shared by altcoins?

Motivation: Altcoins serve for a common purpose—exchange. They demonstrate their features in offer, decentralization, immutability,
anonymity, etc. However, even though an altcoin describes it has many innovative and meaningful creations in its new release, there may be little difference in its source code and others. To verify the true innovations of an altcoin, the analysis of their codes and the similarities with others are needed.

**Approach:** Our study measures the global situation of cryptocurrencies’ innovation from two aspects. First, we obtain their fork relation through the GitHub API. The GitHub API provides endpoints for users to consume GitHub data as well as make changes on a user’s behalf[6]. We send requests through GitHub API and obtain a thorough description of this repository. With the query results structured in JSON, we are able to access the fork related information of a repository from the ‘parent’ (directly fork) and ‘source’ (original source) nodes. We finally crawl the fork information of 1698 repositories belonging to 1023 cryptocurrencies deployed in GitHub.

Second, we implement code clone detection to calculate the similarities between repositories of different cryptocurrencies. It is unnecessary and difficult to calculate the similarities between every repository in every version of each cryptocurrency. We cut two snapshots from our dataset on 28 March 2018 (D1) and 28 September 2018 (D2). In each snapshot, we select repositories of altcoins in their latest version at that time. As comparing repositories written in different languages is out of our scope and the C/C++ written repositories account for the largest (see Figure 1), the repositories whose main language is C/C++ are preserved. Table 2 shows the statistics about these C/C++ written projects of these two snapshots. Time, number of altcoins, and minimum, maximum, and average of LOCs (lines of code) are presented in this table.

**Table 2: Statistics for projects written in C++**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Time</th>
<th>Number</th>
<th>MinLOC</th>
<th>MaxLOC</th>
<th>AvgLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>Mar</td>
<td>485</td>
<td>15804</td>
<td>392312</td>
<td>60937</td>
</tr>
<tr>
<td>D2</td>
<td>Sep</td>
<td>566</td>
<td>13495</td>
<td>2560877</td>
<td>60443</td>
</tr>
</tbody>
</table>

To calculate the similarities between these repositories, we first remove configuration files, readme documents, and files implemented in other languages. Then we treat remaining source code files as text and use RKR-GST (Running-Karp-Rabin Greedy-String-Tilling [26]) algorithm to find the same code snippets in two projects. This algorithm, first carried out by Wise, uses the GST (greedy string tilling) algorithm, which aims to find similar code snippets in two projects. In this process, these similar code snippets are one-to-one mappings in A and B. Finally, considering that even though a large repository may contain codes of a small one, the similarity between them should not be high due to the difference in their size, we use the following formula to calculate the similarity between repository A and B:

\[
\text{similarity} = \frac{2 \times |A \cap B|}{|A| + |B|}
\]

We regard the codes of A and B as two sets. \(|A \cap B|\) represents the size of matched code snippets between A and B, \(|A|\) and \(|B|\) respectively represent the size of A and B, which can be measured by the length of character.
For cryptocurrencies with one repository, we set the similarity of this one repository as the similarity of this altcoin. For cryptocurrencies with more than one repository, we merge the similarities of repositories by selecting the highest similarities.

**Findings: About 15% of repositories shows fork relation with other repositories.** We crawl the fork information of 1698 repositories belonging to 1023 cryptocurrencies deployed in GitHub and successfully get the information of 989 repositories belonging to 983 cryptocurrencies. In this 989 repositories, 146 repositories have a fork relation with other repositories. Among them, bitcoin/bitcoin is the most forked repository forked by 12 other cryptocurrencies. The second is PIVX-Project/PIVX which is forked by 7 cryptocurrencies. Besides, bitcoin/bitcoin is also the most sourced repository. It is the source of 34 repositories, indicating that apart from 12 repositories which directly fork this repository, the repositories forked by the other 22 repositories also come from bitcoin/bitcoin. From this point, the implementation of Bitcoin has a great influence on other cryptocurrencies.

**More than 85% of the repositories share 80% of codes with the other existing repositories.** Figure 5 shows the distribution of maximum similarity of a repository with other existing repositories appearing before it. The similarities of these two experiments have a similar distribution that similarities between 90% and 100% account for the largest part, and the second are similarities between 80% and 90%.

**33.92% cryptocurrencies have a similarity of 80% with more than 50 cryptocurrencies.** According to the results of D2, five cryptocurrencies have a similarity of more than 90% with Bitcoin and 12 of more than 80%. However, the number of cryptocurrencies whose similarities with PIVX more than 90% and 80% is 11 and 48. Besides, there are 55 cryptocurrencies of which each has a similarity of more than 90% with more than 50 cryptocurrencies. Moreover, there are 192 cryptocurrencies (33.92%) of which each also has a similarity of more than 80% with more than 50 cryptocurrencies.

**4.2 What is the relation between altcoins?**

**Motivation:** Conducting a thorough analysis of the relationship between different cryptocurrencies is critical. However, while the statistics show a high degree of duplication in the cryptocurrency world, it’s hard to get a deeper understanding about their extended connections such as the vulnerability caused by their shared code snippets, the technology trends distributed in different groups and the inheritance of their codes during software development. In our study, we propose a temporal clustering algorithm to construct family pedigrees of cryptocurrencies.

**Approach:** To gain a deep insight into the relationship between cryptocurrencies, clustering them by similarities is a shortcut to acquiring an analyzable representation. However, existing clustering methods are insufficient to reflect the development of cryptocurrencies as they do not take temporality into account. We propose a novel clustering algorithm to present their similarities in chronological order.

---

Figure 4: Overview of our approach

Figure 5: Distribution of maximum similarities with existed repositories

While few repositories show fork relation with others, more than 85% of the repositories share 80% of codes with the other existing repositories.
Before the description of the algorithm, we introduce two rules to simplify the relationship between cryptocurrencies:

Rule 1. When the similarity between two cryptocurrencies is high, it is more likely to find that later-released cryptocurrency follows early-released cryptocurrency, which means the similarity is more like a directed relation.

Rule 2. When a cryptocurrency has high similarities with more than one cryptocurrency released early than it, it is more likely to follow the cryptocurrency with maximum similarity.

Based on the aforementioned rules, we only pay attention to the altcoin most similar to this altcoin. Besides, we distinguish the different relation of two cryptocurrencies with different occurrence time intervals. With long-time intervals, we consider one cryptocurrency is a follower of the other one. With short time intervals, we consider they are in the same group. Finally, we propose our algorithm, as shown in algorithm 1.

Algorithm 1 The Temporal Clustering Algorithm

Input: altcoin[n], time[n], similarity[n][n]
{n is the number of altcoins and altcoin[n],time[n] are sorted in chronological order}

Output: Family-Pedigrees

```
1: i = 1;
2: while i <= n do
3:  put altcoin[i] in Family-Pedigrees;
4:  MaxSim[i] = \max\limits_{1 \leq x \leq n} similarity[x][i];
5:  if i == 1 or MaxSim[i] < \Theta_s then
6:     set altcoin[i] as a initial node of a new tree;
7:     continue;
8:  end if
9:  j = \arg\max\limits_{1 \leq j \leq n} similarity[j][i]
10: if node[j] exists then
11:    if |t(node[i]) - t(node[j])| > \Theta_t then
12:      altcoin[i].fathercoin = altcoin[j];
13:    else
14:      altcoin[i].brothercoin = altcoin[j];
15:    end if
16:  end if
17: end while
```

Algorithm 1 illustrates a way to construct family pedigrees for cryptocurrencies. At first, we sort cryptocurrencies by the chronological order of their occurrence time for convenience. Then, in line 2-8 in Algorithm 1, we define that a new tree is created as a coin is selected without high similarities with early-released cryptocurrencies. Next, in line 9-16, we classify the relation between cryptocurrencies with maximum similarity based on the interval of their occurrence time. Finally, a forest composed of many family pedigrees will form.

To have a graphic impression about the relations between hundreds of cryptocurrencies, we propose a way to present them in a tree diagram. The father coin will be the father node of this coin, while its brother coin will be in the same horizontal position. Figure 6 shows part of one family pedigree as our graphic representation of D2 (setting \(\Theta_s = 70\%\) and \(\Theta_t = 3\) months). A horizontal arrow represents brotherhood, and an upright arrow indicates a father-son relationship. For example, Zetacoin is the father node of Skeincoin and e-Gulden is the brother node of Skeincoin.

Findings: Most altcoins congregate in few groups. We use our proposed algorithm to construct family pedigrees on D2 by setting \(\Theta_s = 70\%\). Figure 7 shows the distribution of the numbers in different families. The distribution has a big head and a long tail, which indicates an unbalanced distribution of altcoins in families. The phenomenon of this power-law distribution in altcoins is actually similar to the species richness in clades of organisms[60]. To be accurate, 72.4% (410 in 566) of altcoins congregate in 8.8% (5 in 57) of family pedigrees. It obeys the 80/20 principle, which indicates a more tight aggregation in the more technically-close groups.

Early-released altcoins are more likely to form large families. Figure 8 shows the time of the first altcoin in families. Every node represents a family pedigree. The horizontal axis shows the number of altcoins in this family, while the vertical axis shows the release time of the first altcoin in this family. There are eight
4.3 What is the correlation between prospects and innovations?

**Motivation:** Charles Darwin has observed that due to the limited resources, there is a struggle for existence among individuals - often with only a fraction of offspring surviving through each generation to reproduce successfully. In the cryptocurrency world, there is also a rat race between different kinds of cryptocurrencies. Many factors may influence the prospect of a cryptocurrency, including but not limited to overall market trends, government policies, competitors with the same functionality, and its technology implementations. Especially, mining the relation between their technology implementations and their prospects are useful to see the importance of technology in the cryptocurrency market.

In our previous study, we try to predict their price change from their codes (details in section 6.1). However, it is the same as common knowledge that the correlation between code similarity and market cap is weak. In this study, we carry out the following two questions to further analyze their relation:

1. What is the correlation between prospects of cryptocurrencies and code similarities?
2. What is the correlation between prospects of cryptocurrencies and family pedigrees?

**Approach:** To solve question 1, we select D1 and D2 used in section 4.1 as our research case to explore the relationships in the environment with dropping prices and stable prices, respectively. We crawl market caps of these cryptocurrencies to calculate their market prospects. We define three classes of cryptocurrencies, which are cryptocurrencies without code link, cryptocurrencies with high similarities, and cryptocurrencies with low similarities. We calculate the prospects of cryptocurrency classes during two periods as half one year later and one year later. For D1, we calculate the change of their numbers and market caps from 28 March 2018 to 28 September 2018 and from 28 March 2018 to 28 March 2019. Similarly, we set the periods of D2 as from 28 September 2018 to 28 March 2019 and 28 September 2018 to 28 September 2019. We define the rate of number change (NCR) and market cap change (MCCR) as follows:

\[
NCR(T) = \frac{\text{Number}(T_0 + T)}{\text{Number}(T_0)}
\]

\[
MCCR(T) = \frac{\text{MarketCap}(T_0 + T)}{\text{MarketCap}(T_0)}
\]

From the prospects of different classes, we can discover some differences between cryptocurrencies with different similarities and with or without code.

To solve question 2, we use family pedigrees (FP) of D1 and D2 generated by the algorithm 1 in section 4.2. First, we match the two sets of family pedigrees using algorithm 2. As the maximum similarities (edges of family pedigrees) may change during this period, we only focus on the attributes of their nodes to establish their matches. In algorithm 2, we match all pairs of FP1 and FP2 as long as there exist nodes of trees of FP1 appearing in trees of FP2. The consequence is that one tree in FP2 may match more than one tree in FP1. To avoid this embarrassment, we then select the match with most nodes in common. We search trees in FP1 (earlier) to match trees in FP2 (later) based on our assumption that one tree in the earlier family pedigree is likely to break up into two trees in the later family pedigree while two trees in the earlier one are not likely to unite into one tree in the later one. Then, same as the aforementioned approach, we calculate number change and prospects of family pedigrees from 28 March 2018 to 28 September 2018. From the statistics we processed, we present our research findings.

**Findings:** Alcoins with code links are more likely to have better prospects than alcoins without. Table 3 shows changes in the number and market cap of different classes of cryptocurrencies. We classify "with code" and "without code" through their websites on CoinMarketCap.com. When there is a "Source Code" link in its main page, we classify it as "with code". Otherwise, it will be classified as "without code". To be more accurate, we make our best effort to verify the alcoins without code link through searching on Google and GitHub. To analyze the prospects of different classes, we collect their numbers and market caps at the occurrence time, half a year later, and a whole year later. NCR/MCCR rate (HA) in Table 3 represents NCR and MCCR of this class in half a year. From the statistics, we can see that the number change rates of alcoins with code links are all higher than those without, which indicates that alcoins with code implementation as their technical support are more likely to survive both in environments with dropping prices and stable prices. Also, in most cases, the market cap rates of alcoins with code are higher than those without. All suggest that alcoins with code links are more likely to have a better prospect.
Alcoins with low similarities are more likely to have better prospects than altcoins with high similarities. Table 3 shows one example that we set 80% as the threshold to distinguish altcoins with high similarities and altcoins with low similarities. The similarity of altcoins is defined as their maximum similarity with each other. Here, altcoins with low similarities have fewer members but own larger market caps. This is because Bitcoin dominates the market and is the first cryptocurrency. In all cases, altcoins with low similarities have a higher NCR rate than altcoins with high similarities. Also, in most cases, altcoins with low similarities have a higher MCCR rate than altcoins with high similarities. All suggest that altcoins with low similarities are more likely to have a better prospect.

Small families are likely to have better prospects than big families and the cryptocurrency world is moving toward diversity. Figure 9 presents families in D1 and D2. Table 4 shows details of the families comprised of more than ten members. The last row “single” represents families comprised of only one altcoin. Families in the right (D2) indicate evolution from families in the left (D1). The links are constructed through algorithm 2. Numbers and market caps are listed for each family of two snapshots, and the last column shows the number of altcoins both appearing in two families. The evolution of altcoins is similar to the evolution of species, such as a species may emerge, become extinct, or split into two species. For example, family Bitcoin and Terracoin in D2 all come from family Bitcoin in D1, and they share 20 and 38 altcoins with family Bitcoin in D1. Moreover, families of different size are experiencing different evolution. Among 11 columns except for the second, families whose members are less than 40 experience an increasing or constant process in their numbers, while families whose members are more than 40 experience a decreasing process both in their numbers and market caps. Although most families experience a loss in their market cap, families of more members seem to suffer more. In this way, small families are likely to have better prospects than big families. Due to the reduction of big families and the growth of small families, all families are moving to medium size. It is the same with biological development as this ecosystem is moving toward diversity.

5 RELATED WORK

We discuss related works in two areas: analyses of cryptocurrencies and code clone detection.

Analyses of Cryptocurrencies. There are many researches that measures properties of cryptocurrencies from several aspects including but not limited to the peer-to-peer networks [14, 29, 30, 47], data encryption [17, 40], attack [11, 25, 52] and scam identifications [13, 15]. In this paper, we only focus on papers most related to our own. Reibel et al. [39] carried out research to identify the extent of innovation in the cryptocurrencies landscape using the open-source repositories. They focused on the code reuse of Bitcoin and used hash to calculate the similarities between repositories and analyze their relations through graphs. And they illustrated 8 clusters with directory structure similar relations and file similar relations. Azouvi et al. [12] conducted a study to analyze the centralization in the existing governance structures of Bitcoin and Ethereum. They collected discussions of the contributors and their contributions to...
Table 4: Number change and prospects of cryptocurrencies in different families

<table>
<thead>
<tr>
<th>Family*</th>
<th>Number</th>
<th>Market Cap</th>
<th>Family*</th>
<th>Number</th>
<th>Market Cap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bitcoin</strong></td>
<td>63</td>
<td>$1.27E+11</td>
<td><strong>Bitcoin</strong></td>
<td>40</td>
<td>$1.19E+11</td>
</tr>
<tr>
<td><strong>Terracoin</strong></td>
<td>69</td>
<td>$2.85E+09</td>
<td><strong>Terracoin</strong></td>
<td>69</td>
<td>$2.85E+09</td>
</tr>
<tr>
<td><strong>Dashcoi</strong></td>
<td>5</td>
<td>$3.09E+06</td>
<td><strong>DigitalNote</strong></td>
<td>10</td>
<td>$2.85E+07</td>
</tr>
<tr>
<td><strong>Deutsche eMark</strong></td>
<td>45</td>
<td>$1.44E+08</td>
<td><strong>Deutsche eMark</strong></td>
<td>41</td>
<td>$3.72E+07</td>
</tr>
<tr>
<td><strong>Digitalcoin</strong></td>
<td>14</td>
<td>$1.28E+08</td>
<td><strong>Freicoin</strong></td>
<td>15</td>
<td>$2.85E+09</td>
</tr>
<tr>
<td><strong>ExclusiveCoin</strong></td>
<td>22</td>
<td>$2.76E+08</td>
<td><strong>ExclusiveCoin</strong></td>
<td>26</td>
<td>$1.21E+08</td>
</tr>
<tr>
<td><strong>Frako</strong></td>
<td>33</td>
<td>$6.77E+08</td>
<td><strong>Bullion</strong></td>
<td>87</td>
<td>$2.54E+08</td>
</tr>
<tr>
<td><strong>Freicoin</strong></td>
<td>238</td>
<td>$1.46E+09</td>
<td><strong>Peercoin</strong></td>
<td>173</td>
<td>$5.54E+08</td>
</tr>
<tr>
<td><strong>Monero</strong></td>
<td>3</td>
<td>$2.79E+09</td>
<td><strong>Monero</strong></td>
<td>14</td>
<td>$2.11E+09</td>
</tr>
<tr>
<td><strong>Novacoin</strong></td>
<td>17</td>
<td>$7.74E+07</td>
<td><strong>Novacoin</strong></td>
<td>17</td>
<td>$2.45E+07</td>
</tr>
<tr>
<td><strong>Zcash</strong></td>
<td>8</td>
<td>$7.42E+08</td>
<td><strong>Zcash</strong></td>
<td>10</td>
<td>$8.06E+08</td>
</tr>
<tr>
<td><strong>Single</strong></td>
<td>29</td>
<td>$5.81E+10</td>
<td><strong>Single</strong></td>
<td>38</td>
<td>$3.43E+10</td>
</tr>
</tbody>
</table>

* We use the first coin of a family to represent that family. For example, Bitcoin represents a family in which the first released coin is Bitcoin.

** As altcoins evolve from D1 to D2, the first altcoin of a certain family may change as some altcoin may die. Also, the code of a certain altcoin may change, too. So the presentation of a certain family and the member of a family will change according to their survival state and code similarity.

Figure 9: Families in D1 and D2

In our work, we further analyze the relationship between innovation and prospects and find many significant findings that can provide suggestions for investors and developers.

Code Clone Detection. Tools and techniques of code clone detection can be classified as six categories [8]: textual approaches [10, 23, 27, 34, 37, 51, 56, 58], lexical approaches [35, 44, 45, 50, 55, 59], tree-based approaches [16, 36, 57], metric-based approaches [38, 48, 49], semantic approaches [18, 19, 22, 24, 43, 54] and hybrid approaches [9, 20, 21, 31, 32, 41, 46, 53]. In particular, we introduce several works closely related to our work. Nakamura et al. [33] introduce an approach to detect inter-language clones for web applications. As web applications contain source code written in co-dependent multiple programming languages, they merged co-dependent code clones detected from each programming language to further detect code clones. Yu et al. [58] propose a multi-granularity code clone detection method based on Java bytecode to detect code clones at both method level and block level. Apart from the similarity calculation between instruction sequences, they also calculate the similarity between the method call sequences to improve its effectiveness in detecting semantic code clones. Liu et al. [28] propose VEDFECT, a system to detect vulnerable code clone based on fingerprint. The fingerprint is constructed by applying hash function to code blocks in the diff. Then the vulnerable code
clone is detected by matching the preprocessed code blocks in the target project with the fingerprint. In our work, we carry out further analyses based on the code similarities acquired by code clone detection.

6 DISCUSSION AND THREATS

6.1 Discussion

Vulnerability inheritance. Security is one of the most severe issues in cryptocurrencies. Last year, Tim Ruffing [42] suggests that there was a cryptographic denial-of-spending attack on the original Zerocoin protocol, which is used in several cryptocurrencies including Zoin, PIVX, SmartCash, Zoin, and HexxCoin. Although they handled this vulnerability through their ways, we believe that there may be some connections between them. As shown in Figure 6, HexxCoin is the father node of Zoin and SmartCash, and Zcoin is also a member of this family. Although the similarity relation between cryptocurrencies is not equal to the appearance of vulnerabilities, the family relation, which indicates a very high similarity relation is useful for discovering hidden vulnerability relationships to some extent. We did not carry out a strict process to examine the effectiveness of family pedigrees as it is not the focus of this research.

Price prediction. The interests are always what investors are chasing for in the cryptocurrency world. As we found high similar family pedigrees of altcoins, we wonder whether there is potential to predict their price change from code similarities. Then we use the similarities of an altcoin with others as its feature, define the range of its relative price change against Bitcoin (> 0.1, between 0.1 and 1, and > 1) as its label, and use multiple machine learning models such as decision tree, Naive Bayes, and multilayer neural network to predict the label of the newly-released altcoins by the model trained based on earlier-released altcoins. However, the accuracy shows a decline year by year, as the accuracy of predicting altcoins released in 2015 based on models trained using altcoins before 2015 is about 60% while the accuracy of 2017 and 2018 is about 40% and 33%. Though it may be partly due to reasons caused by the change of dataset size, it reveals a hidden truth that the technical implementation of altcoins has less and less impact on price changes.

6.2 Threats

Dataset. Our study focuses on altcoins written in C++. Altcoins implemented in other languages will be analyzed in our subsequent works. We select two snapshots on 28 March 2018 and 28 September 2018 to carry out our research. As the cryptocurrency world experienced a loss of market cap on 28 March 2018 while the cryptocurrency world on 28 September 2018 was in a stable state, we want to use these two states to represent the complex environment where cryptocurrencies live. But these two snapshots are limited, and we plan to give continuous analyses across several periods.

Code clone detection. We treat source code as text and use RKR-GST algorithm to calculate the similarities. It is simple, so it can’t resist some obfuscations. But we hold the opinion that obfuscations are modifications to the source code, and we are supposed to take that difference into account. And we can get a thorough graphic representation of the same snippets to support the similarity results as the ground truth. When applying it to cryptocurrencies whose codes are written in other languages, it is also suitable for similarity calculation.

Threat. We propose two thresholds as $\theta_0$ and $\theta_1$ to impose restrictions on family pedigree construction. In our results, we generate family pedigrees by setting $\theta_0 = 70\%$ and $\theta_1 = 3$ months. And we use these results to analyze the relationship between prospects and families further. We also set 80% as the threshold to distinguish cryptocurrencies with high similarities and low similarities. As we set the threshold by a certain value, the results may be different from the results obtained by other thresholds. However, the relation between innovations and prospects remains unchanged.

Correlation between prospects and innovations. We carry out a correlation analysis between codes and market caps in Section 4.3 and price prediction in Section 6.1, to investigate whether the code innovation of an altcoin is an essential factor of its market caps. It is the same as common knowledge that the correlation between code similarity and market cap is weak. However, our works show altcoins with high innovation tend to have better prospects, emphasizing the importance of innovation.

7 CONCLUSION

In this paper, an empirical study on existing altcoins is carried out to offer a thorough understanding of various aspects associated with altcoin innovations. Firstly, we construct the dataset of altcoins, including source code repositories, GitHub fork relations, and market capitalizations (cap). Then, we analyze the altcoin innovations from the perspective of source code similarities. The results demonstrate that more than 85% of altcoin repositories present high code similarities. Next, a temporal clustering algorithm is proposed to mine the inheritance relationship among various altcoins. The family pedigrees of altcoin are constructed, in which the altcoin presents similar evolution features as biology, such as power-law in family size, variety in family evolution, etc. Finally, we investigate the correlation between code innovations and market capitalization. Although we fail to predict the price of altcoins based on their code similarities, the results show that altcoins with higher innovations reflect better market prospects.

Our results emphasize the importance of code innovation and we suggest that newly-released cryptocurrencies need to carry out more technological innovations. Our work can be expended to several direction, such as the inheritance of code libraries, innovation analysis of token, relation between releases of highly-similar altcoins, and evolution of Cryptocurrency world form view of code innovations.

ACKNOWLEDGMENT

This work was supported by National Key R&D Program of China (2016YFB1000903), National Natural Science Foundation of China (61902306, 61632015, 61772408, U1766215, 61721002, 61532015, 61833015), Ministry of Education Innovation Research Team (IRT_17R86), China postdoctoral science special foundation (No. 2019TQ0251), and Project of China Knowledge Centre for Engineering Science and Technology. Ting Liu is the corresponding author.


