

Do you trade with your friends or become friends
with your trading partners?
A case study in the $\check{G}1$ cryptocurrency

Nicolas Gensollen * Matthieu Latapy

November 26, 2019

Abstract

We study the interplay between social ties and financial transactions made through a recent cryptocurrency called $\check{G}1$. It has the particularity of combining the usual transaction record with a reliable network of identified users. This gives the opportunity to observe exactly who sent money to whom over a social network. This social network is a key piece of this cryptocurrency, which therefore puts much effort in ensuring that nodes correspond to unique, well identified, real living human users, linked together only if they met at least once in real world. Using this data, we study how social ties impact the structure of transactions and conversely. We show that users make transactions almost exclusively with people they are connected with in the social network. Instead, they tend to build social connections with people they will never make transactions with.

Keywords— cryptocurrency, transaction, social ties, blockchain, stream graphs, link streams, temporal networks, time-varying graphs, dynamic graphs, dynamic networks, longitudinal networks, interactions, time, graphs, networks

*Contact author: Nicolas.Gensollen@lip6.fr

Contents

1	Introduction	3
1.1	Related Work	4
1.1.1	Inferring relations from interactions	4
1.1.2	Inferring interactions from relations	5
1.1.3	The case of financial transactions	5
1.2	Our contribution	6
2	The $\check{G}1$ cryptocurrency	7
3	Dataset and link stream modeling	8
3.1	Link streams	8
3.2	Modeling certifications and transactions using link streams	9
4	Overview of certification and transaction streams	11
5	How do new certifications and transactions appear between members?	13
5.1	Do social ties come before transactions?	13
5.2	Connection probability	16
6	Certifications and transactions neighborhoods	18
7	Conclusion	21
8	List of abbreviations	22

1 Introduction

When seeing two friends inviting each other, who could tell whether they are friends because they invite each other regularly, or if they invite each other regularly because they are friends? Such questions are common in systems where interactions occur over a social network. Obviously, interactions happen preferentially between socially connected individuals, but new ties are also created or reinforced through interactions. Understanding the mechanisms driving the evolution of these systems is an active field of research.

Most of the time, the social network is unknown and one can only record the interactions over time. In such settings, a classical problem consists in recovering the network from traces of interactions. Alternatively, one may also study the opposite problem where the network is known and one wishes to infer associated interactions.

In this paper, we investigate the interplay between social ties and financial transactions. Similarly to friends inviting each other, we wish to better understand whether transactions occur between individuals who were already socially connected, or if individuals build a new tie because they are involved in regular trades. Studying these questions is often challenging because of the lack of data. Indeed, financial transactions are considered as sensitive data, and rarely made public; even when they are, interactions are anonymized.

In 2008, the blockchain technology [1] opened the doors to new virtual currencies which do not rely on a central authority. Transactions are written in a public distributed ledger, such that anybody can obtain the full list of transactions. Since then, the number and diversity of applications relying on the blockchain has been continuously growing [2] [3]. Although Bitcoin is still a benchmark cryptocurrency [3] [4], many new currencies relying on different kinds of blockchains have been introduced since then [4]. Most provide (to some extent) anonymity to the entities making transactions. Indeed, users of these systems are often encouraged to create a new address when they want to make a new transaction, making the association of users and addresses a problem on its own [5] [6]. Some heuristics have been proposed to tackle this challenge but they mostly work for big users and they are difficult to assess. In addition, even if users were identified properly, underlying social ties would remain unknown.

The $\check{G}1$ [7] cryptocurrency under study in this paper relies on explicit social ties to strengthen the robustness of the system. It maintains an accurate network of identified users with reliable social ties, and uses it for monetary growth. This offers a unique opportunity to study the interplay between financial transactions and social ties between human beings.

1.1 Related Work

1.1.1 Inferring relations from interactions

Scientific works tackling the general problem of inferring a network of social relationships from a sequence of interactions span several domains from sociology to computer science. With the increase of geotagged data availability due to the popularization of smart phones and other GPS equipped devices, a large portion of these studies focuses on the inference of social ties from mobility traces. Indeed, social networks are embedded in geography such that it is commonly assumed that interacting probability increases with physical proximity. For instance, the authors of [8] use a call detail records (CDR) to explore the interplay between mobility and social ties. They show that our mobility is far more similar to the one of our social contacts than strangers. Moreover, by relying on temporal variations of similarity metrics, they exhibit different groups of social ties.

In [9], the authors rely on transactions made through student ID cards to build the students' social network. Indeed, student ID cards record students' daily behaviors such as dining, shopping, book borrowing, or library access history. The authors propose a hierarchical encounter model based on association analysis in order to recover not only intra-community social ties but also inter-community links. They show that their method can alleviate the homophily effect by also capturing weak social ties that would be missed by other threshold based methods.

It is well-known that all social relationships are not equivalent [10] [11]. Indeed, they can, among other things, be of different nature and have different strength. Being able to not only infer social ties from interactions, but also quantify their nature and strength is a key challenge within this line of work. In this direction, the authors of [12] study the interactions in a group of baboons in which they observe proximity and grooming as bounding activities. Comparing these interactions to a null model, they propose a method to construct a signed social network in which positive and negative interactions can occur. With the objective of studying the (in)stability of the network, they show that balanced triangles, representing stable structures in social balance theory, are over-represented in the network while unbalanced triangles were under-represented.

Similarly, the authors of [13] present a method to filter strong ties from temporal networks of interactions. Their method computes for each pair of nodes the distribution of their number of interactions in a null model based on node activities. Significant pairs of nodes are thus defined as those with a number of interactions that cannot be explained by the null model.

Slightly different studies aim at predicting missing links of a network from known links or other external features. For example, the authors of [14] use the proximity, in space and time, of geo-tagged photographs over the Flickr social network to infer the likelihood of a social tie between users. This paper shows that this probability increases by orders of magnitudes as the number of

co-locations increases.

Focusing on topological features, the authors of [15] explore the combined effect of multiple social networks for link prediction. More precisely, they represent social ties as a multiplex network where each layer represents a specific social platform, and they show how this additional information can be used to improve link prediction.

In [16], the authors investigate link strength prediction in a social network based on social transactions (likes, comments, etc). They propose a new type of multiple-matrix factorization model for incorporating a transaction matrix between users, and test their method on *Cloob* [17], a popular Iranian social network where users can rate their friendship relationships.

1.1.2 Inferring interactions from relations

If inferring the network of relationships (or missing links of this network) from traces of interactions is often studied, the inverse problem of simulating traces of interactions from the network is also an interesting area of research. In [18] for example, the authors propose a procedure to generate dynamical networks from any weighted directed graph. This graph is considered as the accumulation of paths between its nodes, and the proposed procedure unfolds these paths using random walks of variable lengths. The authors show that their approach is able to generate dynamical networks with bursty, repetitive, or correlated behaviors.

1.1.3 The case of financial transactions

Pioneering work studying both the nature and strength of social ties as well as the way people make transactions can be found in social sciences. In [19] for example, the authors propose to split payments into three categories: gifts, entitlements, and compensations, and show that each category corresponds to a specific set of social relationships and systems of meanings.

More recently, the authors of [20] use real but anonymized transaction records to infer a pseudo-social network of users in which two users are connected if they transferred money to the same entity. Then, they use this pseudo-social network for social targeting and obtain better performances than traditional models.

To the best of our knowledge, there is no previous work studying financial transactions and social interactions simultaneously from a reliable data source. The recent development of cryptocurrencies is creating new opportunities for this kind of studies. Contrary to transactions relying on usual payment methods, blockchain based transactions are public and can be analyzed freely as long as the blockchain itself is public. In [21], for instance, the authors extract the transactions from the Bitcoin blockchain and build the network of transactions. They provide a graph-based analysis of this network and show that linear preferential attachment drives its growth. In [22] the authors study the network of transactions of both Bitcoin and Litecoin, while the authors of [23] recently studied the structure of the Bitcoin users graph, exhibiting a bow tie like structure between its components. In [24], the authors analyzed user comments in

online communities of Bitcoin, Ethereum, and Ripple to predict the price and number of transactions in these cryptocurrencies.

The main limitation is often that, in most of these systems, most public keys (i.e wallets) are used only once such that there is no obvious way to link real users to the set of keys they used to make transactions [5] [6]. In addition, even if users were identified properly, underlying social ties would remain unknown.

1.2 Our contribution

In this paper, we study a specific cryptocurrency which offers both a recording of transactions and of social bounds between identified human beings. This means that we know exactly who sent money to whom and when. Our main objective is to understand the interplay between these transactions and social ties between users.

More precisely, we first explore whether users start making transactions before creating a tie, or if they tend to make transactions with people they are already friends with. Going further, we study the different neighborhood structures and their evolution over time. We tackle questions such as: Are my transaction partners the same as my friends? How do my friends exchange between them compared to my transaction partners? Are my friends and transaction partners more and more homogeneous over time?

As we will see in section 3, although the data is rather simple at first glance, the proper modeling of interactions is challenging and no unique, commonly accepted approach exists. We leverage here the recently introduced link stream model, which captures both the temporal and structural nature of data [25] [26]. We start our analysis with basic metrics targetting the questions above and we define link stream concepts as we need them in the analysis.

Therefore, our contribution is two-fold: it gives a modeling of the data that incorporates time and structure and it sheds lights on fundamental questions on the interplay between transactions and social ties, in the $\check{G}1$ system. These insights are important for progress in several areas, like in particular the inference of social networks from interaction traces.

This paper is organized as follows. Section 2 introduces the $\check{G}1$ cryptocurrency and explains the main ideas and mechanisms behind it. In section 3, we present the dataset under study and show how link streams model interactions from this dataset. In section 4, we use time series and static graph concepts to give a first insight on the global structure and dynamics of the system. In section 5 we consider time and structure together but stay at a basic link level in order to understand the interplay between social ties and transactions. Finally, in section 6 we use more complex stream concepts mixing time and structure in order to investigate this interplay further.

2 The $\check{G}1$ cryptocurrency

$\check{G}1$ [7] was introduced in France in March 2017 and relies on two kind of accounts: *member* and *anonymous* accounts. Both types are linked to a pair of cryptographic keys enabling them to make transactions. While there is no control over the ownership of anonymous accounts, identification of members is a key concern. Indeed, a member has to be equivalent to a real living human being with no other member account in the system. This constraint is linked to the monetary growth mechanism implemented within $\check{G}1$: each day the monetary mass increases and new units of the currency are injected in the system. These new units are distributed evenly between members such that each member receives exactly one share of the monetary growth.

This amount of money that members receive every day is called the *universal dividend* and is denoted by UD in the following. The growth rate of the monetary mass depends on the number of members in the system and is updated every six months in the current implementation [7]. The purpose of this inflation mechanism is two-fold: first, it ensures that all members of a given generation are equal in terms of currency creation. Second, it ensures that the relative value of a dividend is constant over time, and that no generation is privileged over another by the currency creation itself. These two concepts were developed in [27] as the *spatial* and *temporal symmetries* of a currency, and $\check{G}1$ is the first cryptocurrency implementing them.

It is easy to see that most currencies, independantly of their use of the blockchain, do not implement these rules: some individuals benefit from the monetary creation at the expense of others. In Bitcoin for example, early adopters managed to mine most of the finite monetary mass leaving only crumbs to other users [21] [28]. With fiat currencies, creation of new units is often a privilege given to states and banks and remains obscure to most citizens. One of the main objectives of [27] is to show that a currency can fulfill its purpose of enabling transactions of goods, while preserving fairness and equity in terms of monetary creation.

In order to identify its members, $\check{G}1$ maintains a *web of trust* (WoT) between them. A link from person a to person b in the WoT is called a *certification* and means that a certifies that b is a real living human being, with no other member account. Members of the system wishing to participate in the currency creation process must hold enough certifications at all time. Since certifications expire and have to be renewed, members have an incentive to build new connections in order to ensure their status. Moreover, building new connections is a way to reinforce the web of trust and protect the system against sybil attacks.

For these reasons, users are supposed to only give certifications to persons they know, which means that people actually meet in real life during social events to build these links. A certification is thus not necessarily a strong social tie per se, but it is supposed to exist only between human beings who have met at least once in real life, which might be more than one can expect in other online social networks. Therefore, we assume in this paper that certification

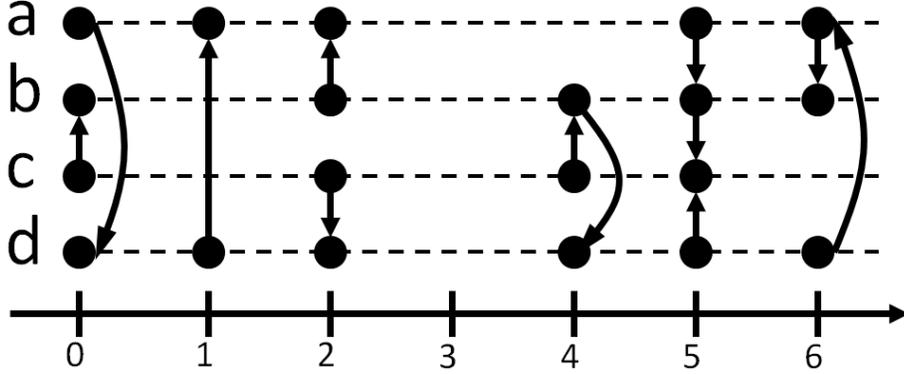


Figure 1: Example of a directed link stream $L = (T, V, E)$ with $T = [0, 6] \subseteq \mathbb{R}$, $V = \{a, b, c, d\}$, and $E = \{(0, c, b), (0, a, d), (1, d, a), (2, b, a), (2, c, d), (4, c, b), (4, b, d), (5, a, b), (5, b, c), (5, d, c), (6, a, b), (6, d, a)\}$.

links accurately reflect social ties between members.

3 Dataset and link stream modeling

All the data we consider here is extracted from the \check{C} 1 blockchain, which is publicly available [29]. It contains three key pieces of information: *identities*, *certifications*, and *transactions*. An *identity* associates a wallet to a user name and represents a member of the system.

Definition 1 (Certification) A certification is a directed link between two members and can be represented as a (t, u, v) triplet, meaning that entity u certifies entity v at time t .

Definition 2 (Transaction) A transaction is a directed weighted link between two public keys (member or not), and can be represented as a (t, u, v, a) quadruplet, meaning that entity u sends an amount a to entity v at time t .

This data has both structural and temporal components which make its analysis far from trivial. Classical methods such as static graphs or time series simplify data and information is lost in the process. In this paper, we use *link streams*, recently introduced in [25] and [26]. Below, we give basic link stream notations and we refer the interested reader to these papers for more details.

3.1 Link streams

Definition 3 (Directed Link Stream) A directed link stream L is a triplet (T, V, E) where T is a set of time instants, V is a finite set of nodes, and

$E \subseteq T \times V \times V$ is a set of directed links. Having $(t, u, v) \in E$ means that u is linked to v at time t .

Figure 1 displays an example with four nodes $a, b, c,$ and d (node labels are represented on the y-axis) over a time period going from $t = 0$ to $t = 6$ (time is represented on the x-axis). Each interaction (t, u, v) is represented as an arrow going from the horizontal line corresponding to node u to the one of node v at time t . For example, interaction $(2, b, a)$ appears as an arrow between a and b at time $t = 2$.

Since link streams encode both time and structure, it is natural to define the *graph induced* by a stream and the *activity* of a stream:

Definition 4 (Graph Induced by a Stream) *The graph induced by a directed link stream $L = (T, V, E)$ is $G(L) = (V, \bar{E})$ in which two nodes are linked if they interacted at least once in L , i.e. $\bar{E} = \{(u, v), \exists (t, u, v) \in E\}$.*

Definition 5 (Activity of a Stream) *The activity of a link stream $L = (T, V, E)$ is defined as the number of active links as a function of time, ie $a_L(t) = |\{(u, v), (t, u, v) \in E\}|$.*

3.2 Modeling certifications and transactions using link streams

We denote by V the set of all public keys involved in $\check{G}1$ certifications or transactions. A subset $M \subseteq V$ of these public keys belong to members and they are available through identities written in the $\check{G}1$ blockchain. The set $A = V \setminus M$ contains all public keys involved in transactions but not associated to any member, which we call *anonymous wallets* in the following.

Definition 6 (Certification Stream \mathcal{C}) *We denote by $\mathcal{C} = (T_{\mathcal{C}}, M, E_{\mathcal{C}})$ the stream of certifications between members:*

- $T_{\mathcal{C}} = [1488987127, 1555054577] \subseteq \mathbb{R}$ is the **time interval** going from the first certification (on 2017-03-08 15:32:07) to the latest one considered in this study (on 2019-04-12 07:36:17)
- $E_{\mathcal{C}}$ is the set of **certification links**: $(t, u, v) \in E_{\mathcal{C}}$ if u certifies v at time t (see definition 1).

Definition 7 (Transaction Stream \mathcal{T}) *We denote by $\mathcal{T} = (T_{\mathcal{T}}, V, E_{\mathcal{T}})$ the stream of transactions:*

- $T_{\mathcal{T}} = [1488990898, 1555052722] \subseteq \mathbb{R}$ is the **time interval** going from the first transaction (on 2017-03-08 16:34:58) to the latest transaction considered in this study (on 2019-04-12 07:05:22)
- $E_{\mathcal{T}}$ is the set of **transaction links**: $(t, u, v) \in E_{\mathcal{T}}$ if u sent a payment to v at time t (see definition 2).

Notice that \mathcal{T} is defined over the node set V and contains transactions between members and anonymous accounts. We can define the *substream* induced by a set of nodes as the stream of links between these nodes (see [25] for details). Transactions can thus occur between identified members (nodes belonging to $M \subseteq V$), between anonymous wallets (nodes belonging to $A \subseteq V$), or between members and anonymous wallets. Therefore, we split \mathcal{T} into four disjoint substreams:

Definition 8 (Member to Member Transaction Stream \mathcal{T}_{MM}) *The stream $\mathcal{T}_{MM} = (T_{\mathcal{T}}, M, E_{\mathcal{T}_{MM}})$, with $E_{\mathcal{T}_{MM}} = T_{\mathcal{T}} \times M \times M$ holds all transactions between identified members.*

Definition 9 (Member to Anonymous Transaction Stream \mathcal{T}_{MA}) *The stream $\mathcal{T}_{MA} = (T_{\mathcal{T}}, V, E_{\mathcal{T}_{MA}})$, with $E_{\mathcal{T}_{MA}} = T_{\mathcal{T}} \times M \times A$ holds all transactions from a member to an anonymous wallet.*

Definition 10 (Anonymous to Member Transaction Stream \mathcal{T}_{AM}) *Stream $\mathcal{T}_{AM} = (T_{\mathcal{T}}, V, E_{\mathcal{T}_{AM}})$, with $E_{\mathcal{T}_{AM}} = T_{\mathcal{T}} \times A \times M$ holds all transactions from an anonymous wallet to a member.*

Definition 11 (Anonymous to Anonymous Transaction Stream \mathcal{T}_{AA}) *Stream $\mathcal{T}_{AA} = (T_{\mathcal{T}}, A, E_{\mathcal{T}_{AA}})$, with $E_{\mathcal{T}_{AA}} = T_{\mathcal{T}} \times A \times A$ holds the transactions between anonymous wallets.*

Figure 2 shows the repartition of transactions between these four substreams as well as their repartition in terms of the total exchanged volume. As can be seen, transactions between identified members (i.e. belonging to \mathcal{T}_{MM}) represent only 30% of \mathcal{T} while transactions between an anonymous wallet and a member (i.e. belonging to \mathcal{T}_{AM}) represent almost 45% of \mathcal{T} and only 12.4% in terms of exchanged money, meaning that there are many small transactions from anonymous wallets to member accounts. A reason for this asymmetry is linked to the way miners are retributed in $\check{G}1$. Recall that money creation is done by the members themselves and that it has nothing to do with mining, such that miners are doing the work for free by design. In order to compensate the miners for this voluntary work, there is a special wallet in $\check{G}1$, called *Remuniter*, which receives donations and uses them to retribute miners. This very specific wallet is therefore a very large hub in \mathcal{T} and stands for almost 40% of all transactions.

Observation 1 *Almost 40% of all transactions are related to miner retribution.*

Removing all transactions involving *Remuniter* changes the transaction count repartition to: 49.2% for members to members, 28.4% for members to anonymous wallets, 10.3% for anonymous wallets to members, and 12.2% for wallets to wallets. Note that, thanks to this specific wallet, we can easily identify the miners of $\check{G}1$ as the outgoing neighbors of *Remuniter* in \mathcal{T}_{AM} (i.e. all members who received money from *Remuniter*). At the time we downloaded the blockchain, there were 158 miners.

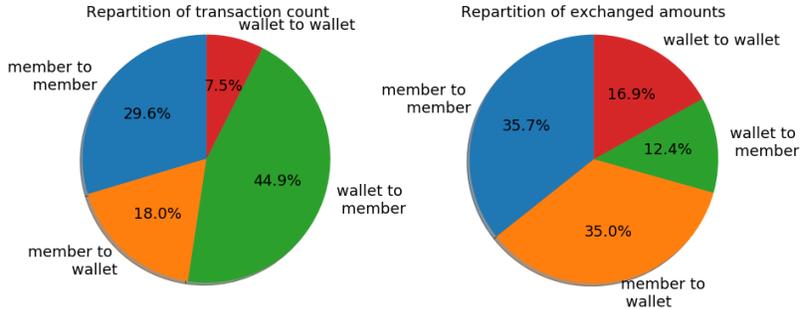


Figure 2: The transaction stream \mathcal{T} can be divided in four substreams: transactions between identified members \mathcal{T}_{MM} , between members and anonymous wallets \mathcal{T}_{MA} , between anonymous wallets and members \mathcal{T}_{AM} , and between anonymous wallets \mathcal{T}_{AA} (see definitions 8 - 11). **Left** - Repartition of the transactions between the different transaction substreams. **Right** - Repartition of the exchanged amounts between the different transaction substreams. Notice that, although \mathcal{T}_{AM} represents about 45% of \mathcal{T} in terms of number of transactions, it only adds up to 12.4% of the exchanged volume.

4 Overview of certification and transaction streams

In this section, we present general properties of \mathcal{C} and \mathcal{T} in order to gain a better understanding of their structure and dynamics. We start by studying the activities (see definition 5) of the certification stream \mathcal{C} , and of the transaction stream between members \mathcal{T}_{MM} . Figure 3 shows the 30 days rolling sum of these activities from March 2017 to March 2019. It appears clearly that they follow very similar trends over this period. A first growth period goes from March 2017 to April 2018 before a strong decrease in activity until early October 2018. Since then, both transaction and certification activities increase, with more volatility for transactions.

Observation 2 *The certification dynamics is strongly correlated to the number of transactions among members.*

By aggregating interactions into a static graph, we obtain two induced directed graphs $G(\mathcal{C})$ and $G(\mathcal{T}_{MM})$ (see definition 4). Figure 4 shows the in and out-degree distributions of each graph. The out-degree of a node in $G(\mathcal{C})$ is the number of certifications given by this member, while its in-degree is the number of certifications it received. In $G(\mathcal{T}_{MM})$, the out-degree of a node is the number of transactions initiated by this member, while its in-degree is the number of transactions it received. First, note that there is no node with an in-degree smaller than 5 in $G(\mathcal{C})$ because the minimum number of certifications



Figure 3: 30 days rolling sum of the activities (see definition 5) of the certification stream \mathcal{C} (red curve) and the transaction stream between members \mathcal{T}_{MM} (blue curve).

required to become a member is set to 5 in the current implementation of $\check{G}1$ [7]. Both graphs clearly display a heavy tailed degree distribution meaning that some members are involved in many more certifications or transactions than the majority.

Observation 3 *The certification graph and the member transaction graph have heterogeneous in and out degree distributions.*

Figure 5 displays correlations between node degrees in $G(\mathcal{C})$ and $G(\mathcal{T}_{MM})$. The top right subplot shows that members tend to give more certifications than they tend to initiate transactions, especially for high degree values. The bottom left subplot shows that nodes in-degree and out-degree values in $G(\mathcal{C})$

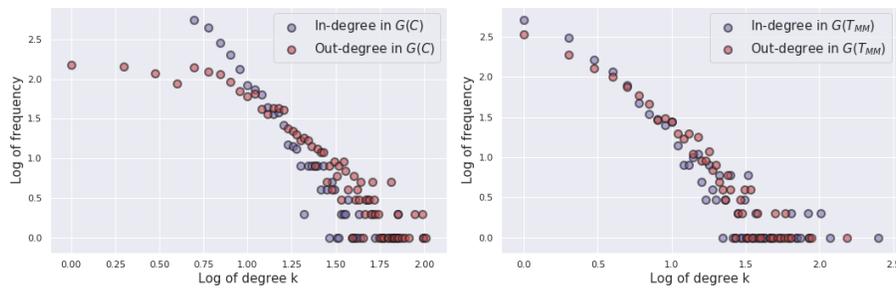


Figure 4: In-degree (in blue) and out-degree (in red) distributions. Left for $G(\mathcal{C})$, and right for $G(\mathcal{T}_{MM})$.

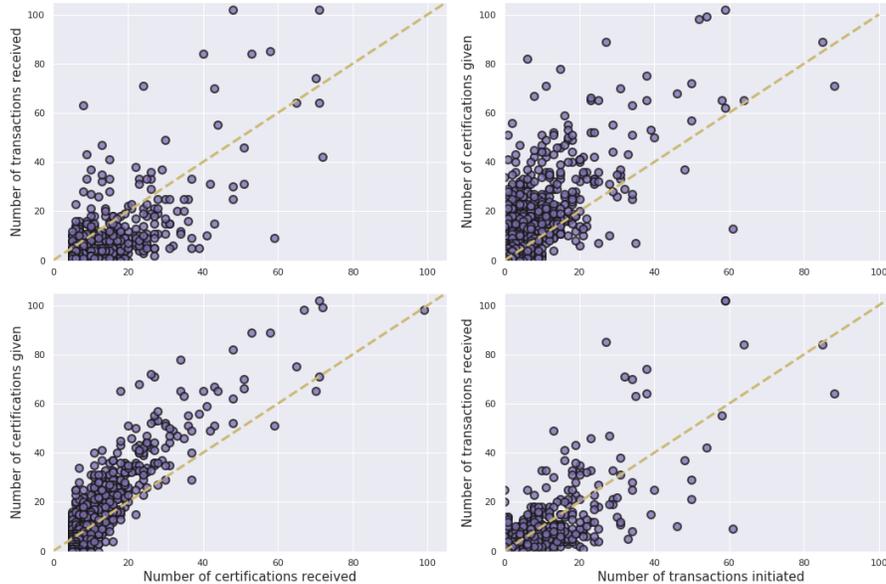


Figure 5: Scatter plots of in-and-out degree correlations in $G(\mathcal{C})$ and $G(\mathcal{T}_{MM})$.

are strongly correlated, meaning that people who receives a lot of certifications tend to also give a lot of them, and tend to actually give more certifications than they received.

Observation 4 *In-coming and out-going activities are strongly correlated both from certification and transaction points of views.*

5 How do new certifications and transactions appear between members?

A key goal of this paper is to gain insight on how certifications impact transactions and vice-versa. We therefore focus on the certification stream \mathcal{C} and the transaction stream restricted to identified members \mathcal{T}_{MM} . In this section we use a direct link-based approach to understand how new links appear in these two streams. More specifically, we wish to understand if a relationship between two members tends to exist in both streams and if it rather starts with a certification (seen as a social tie) or through transactions.

5.1 Do social ties come before transactions?

When a certification occurs between two previously disconnected nodes in \mathcal{C} we search for the first transaction between these two nodes. This transaction can

happen before the certification, after it, or never. For 73% of certifications, the two involved nodes never made a transaction. Instead, 16% of certifications have a pre-existing transaction, and 11% will make a transaction in the future. The top plot of Figure 6 shows the distribution of the delay between a certification (between two nodes in \mathcal{C}) and the closest matching transaction (between these two nodes in \mathcal{T}_{MM}). The delay is very small in most cases. One possible explanation is that new members are often involved in small transactions (welcome gifts or acknowledgments) shortly after (or before) being certified. The bottom plot of figure 6 shows the distribution of the number of transactions in \mathcal{T}_{MM} preceding a certification in \mathcal{C} for these certifications that occur after transactions. Almost all such certifications occur after only one or two transactions, but in a very few cases, a certification can happen after as many as 14 prior transactions.

Observation 5 *Most certification relationships in \mathcal{C} do not have a matching transaction in \mathcal{T}_{MM} , but when they do, most are close in time.*

Let us now investigate the other way round: When a transaction occurs in \mathcal{T}_{MM} , are the two involved nodes already linked by a certification or will they certify each other in the future? It turns out that 64% of all transactions from \mathcal{T}_{MM} occur between two members linked by a certification relationship in \mathcal{C} . More precisely, 42% occur between two already certified members, while only 22% occur between members who will certify themselves in the future. These numbers also mean that about 36% of all transactions from \mathcal{T}_{MM} occurs between members who never certify themselves directly in \mathcal{C} . We can also consider only new transactions in \mathcal{T}_{MM} , that is transactions between two members who never made a transaction before. The middle plot of figure 6 shows the distribution of time intervals Δt (in seconds) between a new transaction in \mathcal{T}_{MM} and the closest matching certification in \mathcal{C} . As can be seen, the majority of new transactions in \mathcal{T}_{MM} occurs shortly after a matching certification in \mathcal{C} .

Observation 6 *Almost two thirds of transactions between members occur between members linked by a certification.*

Because of the constraints imposed on the WoT, the undirected version of $G(\mathcal{C})$ is connected and we can compute a certification distance between any two members. Because the WoT results from social interactions, we expect that nodes lying far apart in $G(\mathcal{C})$ have a small probability of knowing each other, and therefore, of making transactions. About 78% of transactions between members not directly linked occur between members at distance 2 in $G(\mathcal{C})$, 19% at distance 3, 2.8% at distance 4, and 0.2% at distance 5, such that the more distant two nodes are in $G(\mathcal{C})$, the less likely they are to make transactions in \mathcal{T}_{MM} .

Observation 7 *Members who make transactions without being certified are linked by very short chains of certifications.*

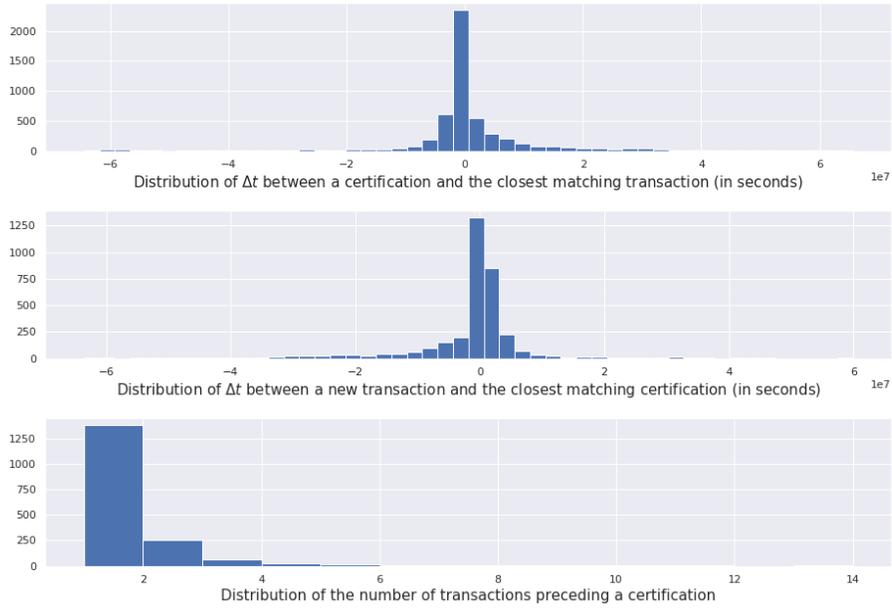


Figure 6: **Top** - Distribution of time interval Δt (in seconds) between a certification in \mathcal{C} and the closest matching transaction in \mathcal{T}_{MM} . **Middle** - Distribution of the time interval Δt (in seconds) between a new transaction in \mathcal{T}_{MM} (i.e. a transaction between two members who never made a transaction before) and the closest matching certification in \mathcal{C} . **Bottom** - Distribution of the number of matching transactions in \mathcal{T}_{MM} preceding a certification in \mathcal{C} for certifications occurring after prior transactions.

$ \overline{\mathcal{C}} / M \otimes M $	$ \overrightarrow{\mathcal{C}} / M \otimes M $	$ \overleftarrow{\mathcal{C}} / M \otimes M $
0.008	0.005	0.003
$ \overline{\mathcal{T}} / M \otimes M $	$ \overrightarrow{\mathcal{T}} / M \otimes M $	$ \overleftarrow{\mathcal{T}} / M \otimes M $
0.004	0.0039	0.0008
$ \overline{\mathcal{T}} \cap \overline{\mathcal{C}} / \overline{\mathcal{C}} $	$ \overline{\mathcal{T}} \cap \overrightarrow{\mathcal{C}} / \overrightarrow{\mathcal{C}} $	$ \overline{\mathcal{T}} \cap \overleftarrow{\mathcal{C}} / \overleftarrow{\mathcal{C}} $
0.318	0.271	0.389
$ \overline{\mathcal{C}} \cap \overline{\mathcal{T}} / \overline{\mathcal{T}} $	$ \overline{\mathcal{C}} \cap \overrightarrow{\mathcal{T}} / \overrightarrow{\mathcal{T}} $	$ \overline{\mathcal{C}} \cap \overleftarrow{\mathcal{T}} / \overleftarrow{\mathcal{T}} $
0.535	0.497	0.715

Table 1: Repartition of interactions among the sets defined by equations 1 - 6.

5.2 Connection probability

What makes two members more likely to be socially connected from a transaction perspective? Are two members more likely to know each other if they made several transactions with the same orientation or if they have made at least one reciprocal transaction? To answer such questions, we introduce:

$$\overline{\mathcal{C}} = \{(i, j) \in M \otimes M, \exists t : (t, i, j) \in E_{\mathcal{C}} \text{ or } (t, j, i) \in E_{\mathcal{C}}\} \quad (1)$$

$$\overrightarrow{\mathcal{C}} = \{(i, j) \in M \otimes M, \exists t : (t, i, j) \in E_{\mathcal{C}} \text{ and } \nexists t : (t, j, i) \in E_{\mathcal{C}}\} \quad (2)$$

$$\overleftarrow{\mathcal{C}} = \{(i, j) \in M \otimes M, \exists t : (t, i, j) \in E_{\mathcal{C}} \text{ and } \exists t : (t, j, i) \in E_{\mathcal{C}}\} \quad (3)$$

In other words, $(ij) \in \overline{\mathcal{C}}$ if there exists at least one certification between i and j at some point in time, $(ij) \in \overrightarrow{\mathcal{C}}$ if there exists only unidirectional links between i and j (either $i \rightarrow j$ or $j \rightarrow i$), and $(ij) \in \overleftarrow{\mathcal{C}}$ if there exists at least one bi-directional certification link between i and j . Notice that $\overleftarrow{\mathcal{C}} \subseteq \overrightarrow{\mathcal{C}}$ and $\overrightarrow{\mathcal{C}} \subseteq \overline{\mathcal{C}}$. We use the same notations for transactions between members:

$$\overline{\mathcal{T}} = \{(i, j) \in M \otimes M, \exists t : (t, i, j) \in E_{\mathcal{T}_{MM}} \text{ or } (t, j, i) \in E_{\mathcal{T}_{MM}}\} \quad (4)$$

$$\overrightarrow{\mathcal{T}} = \{(i, j) \in M \otimes M, \exists t : (t, i, j) \in E_{\mathcal{T}_{MM}} \text{ and } \nexists t : (t, j, i) \in E_{\mathcal{T}_{MM}}\} \quad (5)$$

$$\overleftarrow{\mathcal{T}} = \{(i, j) \in M \otimes M, \exists t : (t, i, j) \in E_{\mathcal{T}_{MM}} \text{ and } \exists t : (t, j, i) \in E_{\mathcal{T}_{MM}}\} \quad (6)$$

Table 1 gives the repartition of interactions among these sets. Although the number of certification links is higher than the one of transactions between members, i.e. $|\overline{\mathcal{C}}|/|\overline{\mathcal{T}}| = 2$, the fraction of bidirectional certifications is much higher than the one of bidirectional transactions: $|\overleftarrow{\mathcal{C}}|/|\overleftarrow{\mathcal{T}}| = 3.75$.



Figure 7: Fraction of member pairs linked by k transactions that are also linked by a certification. The blue plot shows $|\overleftarrow{C} \cap \overleftarrow{T}_k| / |\overleftarrow{T}_k|$ as a function of k , while the red curve shows $|\overleftarrow{C} \cap \overleftarrow{T}_k| / |\overleftarrow{T}_k|$ (see equations 1 - 8).

Observation 8 *Reciprocity of relationships in the social network is stronger than reciprocity in the transaction network.*

Table 1 also shows that the probability for two members to be linked in one stream increases a lot if they are connected in the other stream. More precisely, when two members are connected by a certification, they are almost eighty times more likely to make a transaction than two random members. Similarly, when two members made at least one transaction, they are 67 times more likely to be linked by a certification.

Observation 9 *The probability two nodes to be linked in one stream is orders of magnitudes larger if they are linked in the other stream.*

In addition, reciprocity of transactions seems to play an important role in the probability of having a social tie. Indeed, two members having done at least one reciprocal transaction are almost ninety times more likely to be connected in the WoT than two random members.

Observation 10 *Two members involved in reciprocal transactions are very likely to be socially connected.*

We now study how the number of transactions between two members influence their probability of having a social tie. We denote the number of transactions involving members i and j by:

$$|\tau_{ij}| = |\{(t, i, j) \in E_{\mathcal{T}_{MM}}\}| + |\{(t, j, i) \in E_{\mathcal{T}_{MM}}\}| \quad (7)$$

And we denote the set of member pairs linked by k transactions by

$$\bar{T}_k = \{(i, j) \in M \otimes M, |\tau_{ij}| = k\} \quad (8)$$

Figure 7 shows the fraction of member pairs linked by k transactions that are also linked by a certification. The blue plot shows $|\bar{T}_k \cap \overrightarrow{\mathcal{C}}| / |\bar{T}_k|$ as a function of k , while the red curve shows $|\bar{T}_k \cap \overleftarrow{\mathcal{C}}| / |\bar{T}_k|$. These fractions globally increase with the number of transactions k . More than 80% of members linked by more than five transactions are connected in the WoT.

Observation 11 *The probability for two members to be socially connected increases with the number of transactions they make.*

In conclusion, this section shows that certifications are often the first kind of link appearing between two $\check{G}1$ members, and that transactions occur afterwards. Moreover, these transactions do not happen randomly but constrained by the social network: they preferably take place between friends or between friends of friends. In addition, we showed that the existence of a social relationship between two members increases the probability of making a transaction. Conversely, the probability of being connected with a certification increases when members make transactions, especially when they are bidirectional. In the next section, we will investigate these questions further using more advanced concepts mixing time and structure.

6 Certifications and transactions neighborhoods

In previous section, we studied how new links occur in \mathcal{C} and \mathcal{T}_{MM} using a direct link-based approach. In this section, we go further using the topology of both streams to gain more insights.

A key concept in graph theory is the one of neighborhoods. For a directed link stream $L = (T, V, E)$ the definition of the neighborhood of node $v \in V$, as given in [26], is the following cluster:

$$N_S(v) = \{(t, u), (t, u, v) \in E \text{ or } (t, v, u) \in E\} \quad (9)$$

A neighborhood is thus composed of temporal nodes rather than simple nodes for static graphs. We also consider the neighborhood of the undirected induced graph $G(S)$:

$$\bar{N}_S(v) = \{u \in V, \exists (t, u, v) \in E \text{ or } \exists (t, v, u) \in E\} \quad (10)$$

In other words, $\bar{N}_S(v)$ contains all nodes which interacted with $v \in V$ at least once, while $N_S(v)$ keeps track of interaction times.

In addition to neighborhoods, we propose to study triangles in \mathcal{C} and \mathcal{T}_{MM} , which are a famous and very important concept in network theory. They intuitively convey the idea that *people I interact with tend to also interact between themselves*. A commonly used metric mixing triangles and neighborhoods in

graphs is the clustering coefficient. The clustering coefficient of a node is the density of its neighborhood, and the clustering coefficient of the whole graph is defined as the average value over its nodes.

The average clustering coefficient for $G(\mathcal{C})$ (resp. $G(\mathcal{T}_{MM})$) is 0.49 (resp. 0.31), while the average for $G(\mathcal{T}_{AA})$ is 0.13. Note that, by construction, the clustering coefficients for $G(\mathcal{T}_{AM})$ and $G(\mathcal{T}_{MA})$ are both equal to 0. In terms of triangles, $G(\mathcal{C})$ contains 6589 triangles, $G(\mathcal{T}_{MM})$ 1990 triangles, and $G(\mathcal{T}_{AA})$ only 393. These values are much higher than for random graphs with the same degree distributions (about 23 times higher for $G(\mathcal{C})$, and about 4 times higher for $G(\mathcal{T}_{MM})$), meaning that both $G(\mathcal{C})$ and $G(\mathcal{T}_{MM})$ are very clustered networks. Figure 8 shows the distributions of the node clustering coefficients in both networks. Note that, although their average clustering values are similar, the distributions over nodes are very different. Indeed, the distribution for $G(\mathcal{T}_{MM})$ exhibits two peaks around 0 and 1, meaning that most nodes make transactions either in a very clustered way or not at all, while the distribution for $G(\mathcal{C})$ has a majority of values in between those extremes.

Observation 12 *Both $G(\mathcal{C})$ and $G(\mathcal{T}_{MM})$ are strongly clustered. However, the clustering coefficient distributions have very different shapes. The distribution in $G(\mathcal{T}_{MM})$ exhibits two peaks around 0 and 1, meaning that members make transactions either in a very clustered way or not at all.*

Previous results are built on induced graphs and so they do not take time into account. Clustering coefficient has been extended to link streams [25], but provide little insight here. Indeed, the slow dynamics of \mathcal{C} make results very similar to the ones obtained for the induced graph $G(\mathcal{C})$, and \mathcal{T}_{MM} is a very sparse stream such that there is almost no time instant where transactions form triangles.

We propose another stream concept to study triangles with time: directed k -closure of links, where k is an integer larger than 1: the 2-closure, for example, is the time one has to go back to find a link between the same nodes but in the opposite direction. The 3-closure is defined as the amount of time required to find a triangle containing the considered link.

The left plot of figure 9 illustrates 2 and 3-closures in a simple case. The 2-closure of link $(6, a, b)$ for example is equal to 4 since we have to go back to $t = 2$ to find a link in the opposite direction, namely link $(2, b, a)$. The 3-closure of the same link $(6, a, b)$ is equal to 5 since, this time, we have to go back to $t = 1$ to find the triangle $(6, a, b), (4, b, d), (1, d, a)$.

Here we examine both the 2 and 3-closures for \mathcal{C} and \mathcal{T}_{MM} . The right plot of figure 9 shows the k -closure distributions for the two streams. The 2-closures for \mathcal{C} is generally smaller than for \mathcal{T}_{MM} , meaning that people tend to certify back faster than they make a transaction in the other direction. The 3-closures distribution of \mathcal{C} and \mathcal{T}_{MM} are very similar which seems to suggest that, although there are less triangles in \mathcal{T}_{MM} than in \mathcal{C} , they tend to appear within the same time frame.

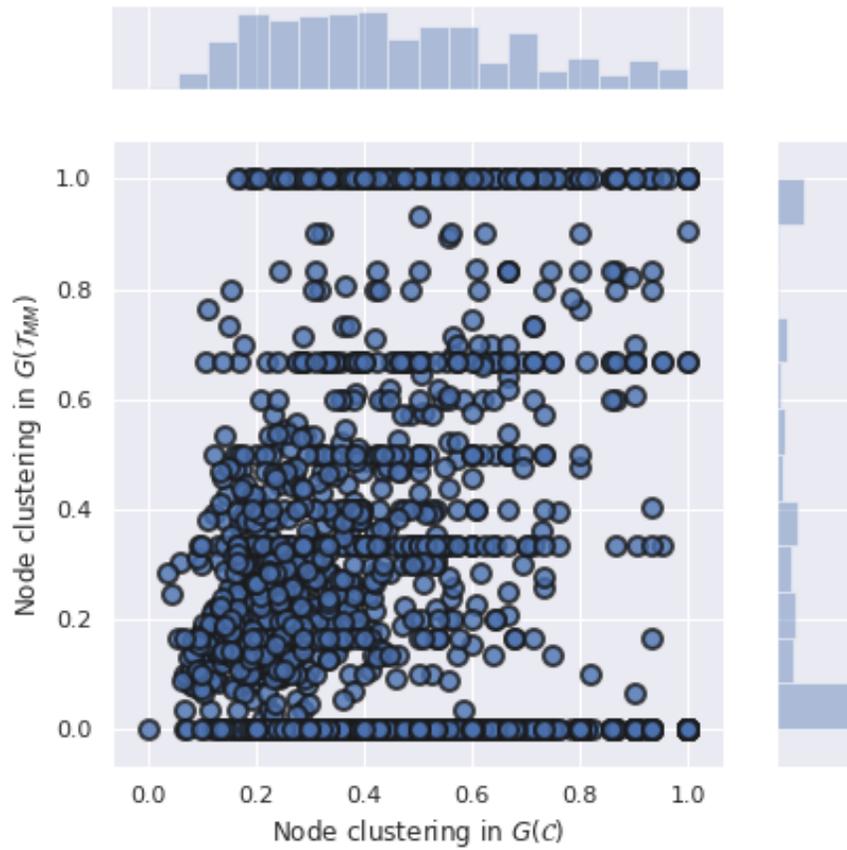


Figure 8: Node clustering coefficients distributions and correlations in $G(\mathcal{C})$ and $G(\mathcal{T}_{MM})$.

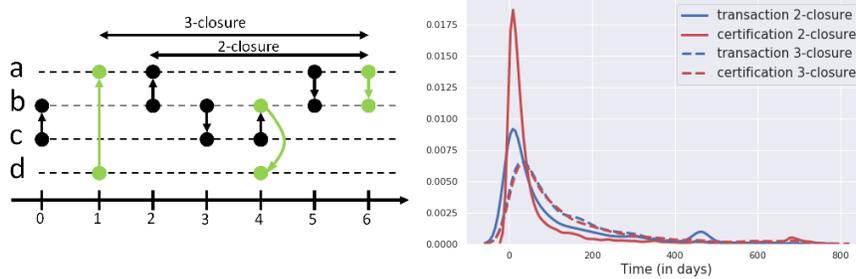


Figure 9: **Left** - Illustration of the 2 and 3-closures. The 2-closure of link $(6, a, b)$ is equal to 4 since we have to go back to $t = 2$ to find a reversed link $(2, b, a)$. The 3-closure of link $(6, a, b)$ is equal to 5 since we have to go back to $t = 1$ to close the triangle composed of $(6, a, b), (4, b, d), (1, d, a)$. **Right** - The distribution of 2- and 3-closures for all links in \mathcal{C} and \mathcal{T}_{MM} . Note that we only consider links with finite k-closures, links with infinite values being ignored.

Observation 13 *Users certify back faster than they make a backward transaction. On the other hand, triangles are built within similar time frames in \mathcal{C} and \mathcal{T}_{MM} .*

7 Conclusion

We studied a recent cryptocurrency which, despite its relatively small size, provides a very interesting and publicly available dataset to study transactions within a social environment. Because the data has both a structural and temporal component, neither a pure static graph nor a time serie based model are well suited for its study. We proposed here to rely on the link stream formalism to study the streams of certifications and transactions.

We showed that certifications are often the first type of link occurring between two previously disconnected nodes, suggesting that members of $G1$ start to meet at social events before making transactions. In this context, the social network shapes the way transactions occur: even when they occur between two members without a certification relationship, transactions have a much higher probability of occurring between two socially close nodes. Investigating further, we showed that members tend to have a transaction neighborhood included within their certification neighborhood.

We also studied clustering coefficient of certifications and transactions and discovered that their distributions have very different shapes. Members tend to make transactions either in a very clustered way or not at all, but rarely in between these two extremes. We also studied the k-closure of certifications and transactions and found that users certify back faster than they tend to make a backward transaction, meaning that certification relationships become

bi-directional faster than transactions.

These results might be specific to this particular cryptocurrency and call for further investigation to explore their generality, though. Indeed, $G1$ is still very young and used mostly by a limited number of currency-interested people. As the currency will age, we expect $G1$ usage to grow, and that time will play a more important role in the study of the interplay between social ties and interactions. Another interesting direction would be to compare the properties of $G1$ with other social systems with transactions, like for instance Steemit [30].

8 List of abbreviations

- **UD:** *Universal Dividend*
- **WoT:** *Web of Trust*

References

- [1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2009.
- [2] W. Al-Saqaf and N. Seidler, “Blockchain technology for social impact: opportunities and challenges ahead,” *Journal of Cyber Policy*, pp. 1–17, 11 2017.
- [3] G. Hileman and M. Rauchs, “Global cryptocurrency benchmarking study,” 4 2017.
- [4] S. G. Gohwong, “The state of the art of top 20 cryptocurrencies,” *Asian Administration and Management Review*, vol. 1, 1 2018.
- [5] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of bitcoins: Characterizing payments among men with no names,” in *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC ’13, (New York, NY, USA), pp. 127–140, ACM, 2013.
- [6] C. Remy, B. Rym, and L. Matthieu, “Tracking bitcoin users activity using community detection on a network of weak signals,” in *Complex Networks & Their Applications VI* (C. Cherifi, H. Cherifi, M. Karsai, and M. Musolesi, eds.), (Cham), pp. 166–177, Springer International Publishing, 2018.
- [7] B. L. et al., “Duniter G1 client.” <https://g1.duniter.fr/>, 2017–2019.
- [8] J. L. Toole, C. Herrera-Yaqué, C. M. Schneider, and M. C. González, “Coupling human mobility and social ties,” *Journal of The Royal Society Interface*, vol. 12, no. 105, p. 20141128, 2015.

- [9] J.-Y. Xu, T. Liu, L.-T. Yang, M. Davison, and S.-Y. Liu, “Finding college student social networks by mining the records of student id transactions,” *Symmetry*, vol. 11, p. 307, 03 2019.
- [10] R. Bapna, A. Gupta, S. Rice, and A. Sundararajan, “Trust and the strength of ties in online social networks: An exploratory field experiment,” *MIS Q.*, vol. 41, pp. 115–130, Mar. 2017.
- [11] R. Xiang, J. Neville, and M. Rogati, “Modeling relationship strength in online social networks,” in *Proceedings of the 19th International Conference on World Wide Web, WWW '10*, (New York, NY, USA), pp. 981–990, ACM, 2010.
- [12] V. Gelardi, J. Fagot, A. Barrat, and N. Claidière, “Detecting social (in)stability in primates from their temporal co-presence network,” *Animal Behaviour*, vol. 157, pp. 239 – 254, 2019.
- [13] T. Kobayashi, T. Takaguchi, and A. Barrat, “The structured backbone of temporal social ties,” *Nature Communications*, vol. 10, no. 1, p. 220, 2019.
- [14] D. J. Crandall, L. Backstrom, D. Cosley, S. Suri, D. Huttenlocher, and J. Kleinberg, “Inferring social ties from geographic coincidences,” *Proceedings of the National Academy of Sciences*, vol. 107, no. 52, pp. 22436–22441, 2010.
- [15] D. Hristova, C. Noulas, Anastasiosand Brown, M. Musolesi, and C. Mascolo, “A multilayer approach to multiplexity and link prediction in online geo-social networks,” *EPJ Data Science*, vol. 5, no. 1, p. 24, 2016.
- [16] H. Khosravi, A. Bozorgkhan, and O. Schulte, “Transaction-based link strength prediction in a social network,” in *2013 IEEE Symposium on Computational Intelligence and Data Mining (CIDM)*, pp. 191–198, April 2013.
- [17] “Cloob.” <https://www.cloob.com>. Accessed: 2019-08-20.
- [18] A. Barrat, B. Fernandez, K. K. Lin, and L.-S. Young, “Modeling temporal networks using random itineraries,” *Phys. Rev. Lett.*, vol. 110, p. 158702, Apr 2013.
- [19] V. Zelizer *Sociological Forum*, vol. 11, no. 3, 1996.
- [20] D. Martens and F. Provost, “Pseudo-social network targeting from consumer transaction data,” 09 2011.
- [21] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, “Do the rich get richer? an empirical analysis of the bitcoin transaction network,” *PloS one*, vol. 9, p. e86197, 02 2014.
- [22] M. Popuri and G. MH., “Empirical analysis of crypto currencies,” vol. 644, 2016.

- [23] D. D. F. Maesa, A. Marino, and L. Ricci, “The bow tie structure of the bitcoin users graph,” *Applied Network Science*, vol. 4, no. 1, p. 56, 2019.
- [24] Y. B. Kim, J. G. Kim, W. Kim, J. H. Im, T. H. Kim, S. J. Kang, and C. H. Kim, “Predicting fluctuations in cryptocurrency transactions based on user comments and replies,” *PLOS ONE*, vol. 11, pp. 1–17, 08 2016.
- [25] M. Latapy, T. Viard, and C. Magnien, “Stream graphs and link streams for the modeling of interactions over time,” *Social Network Analysis and Mining*, vol. 8, 10 2017.
- [26] M. Latapy, C. Magnien, and T. Viard, “Weighted, bipartite, or directed stream graphs for the modeling of temporal networks,” *CoRR*, vol. abs/1906.04840, 2019.
- [27] S. Laborde, “Relative theory of money,”
- [28] C. Rose, “The evolution of digital currencies: Bitcoin, a cryptocurrency causing a monetary revolution,” *International Business and Economics Research Journal (IBER)*, vol. 14, p. 617, 07 2015.
- [29] “G1 blockchain explorer.” <https://g1.duniter.fr/#/app/blockchain/search>. Accessed: 2019-08-20.
- [30] “Steem, an incentivized, blockchain-based, public content platform,” 6 2018.