Trust Asymmetry

Percy Venegas

Economy Monitor

Abstract

In the traditional financial sector, players profited from information asymmetries. In the blockchain financial system, they profit from trust asymmetries. Transactions are a flow, trust is a stock. Even if the information asymmetries across the medium of exchange are close to zero (as it is expected in a decentralized financial system), there exists a "trust imbalance" in the perimeter. This fluid dynamic follows Hayek's concept of monetary policy: "What we find is rather a continuum in which objects of various degrees of liquidity, or with values which can fluctuate independently of each other, shade into each other in the degree to which they function as money". Trust-enabling structures are derived using Evolutionary Computing and Topological Data Analysis; trust dynamics are rendered using Fields Finance and the modeling of mass and information flows of Forrester's System Dynamics methodology. Since the levels of trust are computed from the rates of information flows (attention and transactions), trust asymmetries might be viewed as a particular case of information asymmetries – albeit one in which hidden information can be accessed, of the sort that neither price nor on-chain data can provide. The key discovery is the existence of a "belief consensus" with trust metrics as the possible fundamental source of intrinsic value in digital assets. This research is relevant to policymakers, investors, and businesses operating in the real economy, who are looking to understand the structure and dynamics of digital asset-based financial systems. Its contributions are also applicable to any socio-technical system of value-based attention flows.

Keywords: Trust economics, Computational trust, Cryptocurrencies, Bitcoin, Behavioral finance, Web Analytics, Blockchain Analytics, Machine learning, Genetic programming, Markets disintermediation, Topological Data Analysis, Applied Quantitative Analysis, Fields Finance.

JEL Classification: G02, F63, B17, C53, C58

...reputation is a stock that is changed by the flow of good and bad actions... –Jay Forrester

The message is on the feedback –Gordon S.Brown

1 Introduction

The are various reasons why bitcoin (and to a lesser extent, other algorithmic currencies) are quickly capturing an increasing share of international flows: the US and the EU printed large amounts of money after the financial crisis, and because of nationalistic sentiment, now they are not in the mood for running large trade deficits to support the rise of the South and Asia Pacific; programmatic money is a superior settlement mechanism; volatility does not matter if the currency is only used as medium of exchange.

However, a common concern among finance professionals, who usually make money by having access to privileged knowledge and special relationships, is how is it possible to do business when information asymmetries are close to zero — in shared distributed ledgers and blockchains, data is either public or available given proper authentication. By using examples from actual economic activity (in international trade and digital commerce) we can illustrate how the intuition of a *trust imbalance* may serve as starting point in the analysis. We define the concept of "trust asymmetry" in terms of dissimilarities in metric entropy (e.g. Kolmogorov Entropy) or as in this case, using symbolic regression complexity – which can be described in terms of the shape of a data space, and, the dynamics of vector fields.

We define the concept of "trust asymmetry" as a form of metric entropy (e.g. Kolmogorov Entropy) which can be described in terms of the shape of a data space, and, the dynamics of vector fields.

At the theoretical side, one of the problems with the information asymmetry literature in economics is that rarely formal methods are offered to actually quantify the degree information asymmetry; this is in part because of methodological challenges for real-time behavioral economics data collection. Distributed ledger systems offer a distinct opportunity to overcome this issue, and actually, correlate financial and non-transactional data flows.

The paper will begin with a layman's introduction to behavioral traits of the trust-based decisions in the periphery of a trust-less financial system and will continue to define formal heuristics to measure trust-asymmetries using methods from several disciplines. From computational trust, behavioral finance and applied quantitative analysis we use trust evidence from blockchain, financial, and web analytics, as the experience based input of the direct interaction of the market participants. We also apply topology and symbolic regression to investigate the structure and shape of the data (information flows), as an input to the system dynamics and vector fields modeling. In the conclusions, we discuss the implications of this research to applications such as prediction markets.

Ultimately, we will be able to answer questions such as: are the nodes running blockchain software essentially a material expression of people's beliefs? Particularly, is the "belief consensus" the fundamental source of intrinsic value that can be measured by intangible attention flows and tangible transactional activity?

1.1 Trade finance

Trade between Latin America and Africa with India and China is set to grow [18]. But as those who operate a new small business in Latin America or Africa know, the traditional banking system is a major roadblock to their growth ambitions. Trade finance, or even business banking accounts, are difficult to access.

However, a small fish exporter in Uganda can do business with a Hong Kong broker that supplies the mainland China market using the new blockchain financial system. The delivery of goods takes 8 days by ship, 10 hours by plane. Settlement takes at least 5 days using the traditional banking system, and less than 30 minutes using bitcoin. Therefore, executing a cryptocurrency trade brings at least a comparable jump in efficiency to what aviation brought to supply chains after WWII when the transition from sea to air logistics materialized. But if the information is public in the blockchain, and the settlement near real time in the context of international trade, where are the asymmetries that will allow financial intermediaries to profit? Fishermen in Lake Victoria are good at catching fish and want to be paid in Ugandan shilling (UGX). Merchants in Hong Kong have access to Hong Kong dollars, USD or RMB. They are 9135 kilometers apart, and they do not know each other. No one really wants to remove the intermediary to save money, in detriment of efficiency in sourcing of goods or payment settlement. But they do need to do business with someone they trust. The price of trust is the cost of business lost (not realized) if trust is lost (not secured).

1.2 Digital commerce

Cross-border deposits are an inconvenience for the majority of humanity. It is easy if one lives within the walled gardens of the internet: Amazon takes your money if you live in the US/EU, Alibaba if you live in China. But as the teams at the MIT's Collective Learning group and the Harvard's Growth Lab point out, growth will not come from the West or even China, but from India and everywhere else. Nevertheless, consumers in the emerging world face great difficulties getting access to affordable credit cards that can work without problems all the time, everywhere — not even bitcoin debit cards are readily available because those are largely issued to European and North Americans, and also there, issuers are constantly limiting their use to purchase cryptocurrency. Meanwhile, a large share of freelancers (many of whom are bitcoin earners) live in the developing world, and the current KYC policies that traditional banks enforce really do not apply to them — it is unrealistic to understand the financial reality of emerging economies from an office in Basel, where the know-your-customer standards are issued.

International commerce runs a large deficit of trust. Merchants are wary of prospect customers, buyers have no confidence in sellers, and local regulators have no power over foreign merchants. However, demand for new payment methods (including cryptocurrencies) is growing across multiple markets. Figure 2 shows that search engine queries for "where can I spend bitcoins" and " " quadrupled from April to May 2017.

When even a weak signal shows strengthening demand (Russia's top search engine is Yandex, India's first language is Hindi) merchants know that something interesting is going on, and they begin supporting new payment methods such as digital currencies. The way it works is that users accumulate or buy cryptocurrencies to use them in exchange for services, goods, and entertainment. Deposits are handled by a payments processor and are put in custody in an exchange (for instance, to engage in trading activities), vault (cold storage), or similar.

Despite the decentralized nature of the medium of exchange, there is really no implicit animosity against financial intermediaries. Business people are pragmatic, they understand that specialization breeds prosperity. As a customer your primary motivation is not to remove service providers to save a few dollars, you just happen to have a relationship with your favorite brand, not with the seller on the other side – and you suffer great difficulties to access credit cards. As a seller, you do not want to worry about having to trust a buyer – and settlement speed is important because even in a cashless economy, cashflows are the lifeblood of a business. As a merchant, you simply need to be able to take the form of payment that your customers are using already, and that you can exchange later into whatever legal tender is appropriate. If the payment mechanism takes care of processing and fraud simultaneously, then the decision is straightforward.

1.3 Trust asymmetries

Note that in none of those two cases were there any "real banks" involved. And these are not fictional scenarios: today there is trading between Africa and Asia denominated in bitcoin (mainly via over-the-counter markets) [2], and digital currency denominated e-commerce grows [4] while brick and mortar retail shrinks. Money is already flowing for legitimate international commerce, largely without the banks. Figure 3 shows the intuition behind the concept.

Even if the information asymmetries across the medium of exchange are close to zero (as it is expected in a decentralized financial system), there exists a *trust imbalance*. And there are different levels of trust among trustful parties: naturally, a merchant will trust a local broker more than its foreign counterparty. In the middle, there is no need to trust a bank, a correspondent bank, or even a government. You just need to trust that people will pursue their own self-interest: miners will verify transactions while it is profitable to do so, and over-the-counter exchanges will maintain order books as long as there is demand. There is only the issue of on-ramping and off-ramping to fiat, but one could argue that this lies at the boundaries of the medium of exchange – it is a *trust coupling* problem. Therefore, whoever can level-up trust provides a valuable financial intermediation service — at least until the system becomes mature.

2 Literature

In their book "Beyond Smart Beta: Index Investment Strategies for Active Portfolio Management" Kula, Raab, and Stahn define Total return as the amount of value an investor earns from a security over a specific period when all distributions are reinvested [16]. While it is still early in the development of crypto assets to account for all distributions (dividends, coupons, capital gains), it is customary to use at least the price increase to measure the investment's performance. Typically, those historical returns would be the "goal" in a predictive model catered to "learn" (in an interactive fashion) what demand signals are also signs of value appreciation. However, in crypto economies prices are taken rather as a measurement of market sentiment, and related quantities such as on-chain transaction volume are difficult or impossible to assess in a trustworthy manner [6]. Therefore we may begin to characterize off-chain flows in terms of returns (a common success measure for investors), but soon we should move beyond prices, exchange volumes and transaction counts, and include hard metrics such as fees into our analysis.

An ideal scenario to study trust asymmetry is the case of a cryptocurrency fork, where at *t=0* one may assume equal conditions for the two chains (although in practice this is hardly the case, since the different fractions have already grouped around their preferred coin before the split, financial futures may have been trading already, and so on). In our paper on Crypto Economic Complexity [21], we argued that crypto economies tend to converge to the level of economic output that can be supported by the know-how that is embedded in their economy — and is manifested by attention flows. And, since a fork is really an event at the macroeconomic level (for instance, the economy of BitcoinCash vs the economy of Bitcoin), the aggregate demand for output is determined by the aggregate supply of output — there is a supply of attention *before* there is demand for attention. We also discussed the practicalities of quantifying economic complexity by ranking economies, focusing on the specific case of cryptocurrencies and tokens. Here we will demonstrate how to develop the heuristics of such an approach, from the perspectives of structure and dynamics of the combined system.

2.1 Trust equations

The socio-technical modeling of mass and information flow has usually been accomplished in econometrics, industrial, and, policy planning circles, using Jay Forrester's System Dynamics methodology [10]. The fact that continuous systems contain differential equations is hidden from the user by talking about levels, i.e., quantities that can accumulate (state variables), and rates, i.e., quantities that influence the accumulation and/or depletion of levels (state derivatives) [8]. A typical model for the traditional financial system is shown in Figure 4. However, real-life systems modeling in the context of a digital economy involves a different set of variables, notably, the inclusion of online activity and distributed ledger related records (either online or offline, if the architecture is based on mesh networks).

In the example, the level's rate equations have the form of the derivative of the level with respect to time, which equals the summation of inflows minus the summation of outflows. In the case of the decentralized financial system, the levels of trust are computed from the rates of information flows (attention and transactions); although the formulation is similar Forrester's, deriving the equations requires either analytical or machine learning modeling. In the Methods and Analysis sections, we provide additional literature covering such methodologies.

3 Methods

Data for this section includes digital assets historical monthly returns (Coincheckup.com), on-chain metrics (Coinmetrics.com), and off-chain web and social analytics (EconomyMonitor.com and clickstream data providers). The period of study is August 2017 to January 2018.

3.1 The characterization of flows

When a blockchain split event occurs, a race (competition) for attention begins. Demand stars flowing from search engines, price trackers, faucets, wallets, educational sites, and the many services that support a crypto economy. One such event occurred on August 1st 2017, when the Bitcoin blockchain forked, creating two competing digital assets, BTC and BCH [3]. We obtained monthly data for 177 of those web services, specifically, the share of usage of each service towards two of the official communities in both networks; this off-chain activity acts as an inferential sensor, an indication of interest and trust. The sources were the largest contributors in the six-month period, their share is weighted by contribution. The resulting arrays (Figures 5 and Figure 6) depict the time period in the vertical axis, and the source variables in the horizontal axis; the target variable (returns) are included in the last column. Red tones encode incomplete data.

In the case of Bitcoin (digital asset ticker BTC), we observe an active economy, with creative destruction (services that come online or stop contributing, as time progresses).

3.1.1

As for BitcoinCash (digital asset ticker BCH), the economy is less developed, with many incomplete data points or weak strength of the attention flows (orange tones). Signals that are expected to build-up over time (e.g. search engine traffic) are naturally stronger when the economy is more mature, and there are a few dominant sources –but a great number of smaller sources make up for the bulk of the flows.

There is also specialization since some services that are relatively inactive in the Bitcoin economy are larger contributors to the economy of BitcoinCash. For instance, any given month Google search contributes between 41% and 49% to the group of economies, and the share of Bitcoin is between 85% and 94% of those flows. But in turn, early supporters of the new coin focused on BCH (for instance Bitcoin.com, operator of a popular wallet supporting BCH, went from contributing 87% in August 2017 to 91% in January 2018 – although its total contribution to the group was marginal).

3.2 Results

Due to its ability to identify and focus on driving variables, Symbolic Regression can build models from data sets that have more variables than records (these are commonly known as *fat arrays*, and most non-evolutionary machine learning techniques find issues to deal with them) [19]. Therefore, we apply genetic programming for dimensionality reduction purposes, and to build the predictive models that can provide insight into the shape of the *trust data space*.

3.2.1 Bitcoin

In total, 532 models were generated, with the majority of those (55.1%) containing at least three variables. The modeling process explores the trade-off between model complexity and model error (1-R^2). This is illustrated in the ParetoFrontLogPlot which displays each of the returned models' quality metrics, *complexity*, and *accuracy*. The models denoted by red dots are all optimal in the sense that for a given level of accuracy there is no simpler model or, conversely, for a given level of complexity there is no more accurate model [15]. Notably, there are 3 models at an order of magnitude materially better than the rest (error on a scale under 10^{-15}), and one of those is an optimal model.

3.2.2 BitcoinCash

In the BitcoinCash case it is more difficult to determine what the dominant best models are, this is confirmed by the number of models with relatively high error, and the higher dimension and larger number of possible variable combinations (50 models use 5 variables, wherein the Bitcoin case no model had more than 4 variables).

4 Analysis

The first thing that we need to understand is the meaning of the models obtained. A trivial observation would be of the kind that one could find in the financial press, for instance, that because an increasing share of Google searches brings people to Bitcoin-related sites, then the market might be validating the positive sentiment expressed by higher prices. Rather, what we would like to understand from the *shape of the data* is what are those factors which variability has a noticeable impact on actual investor expectations changes, as measured by *price returns*–even if those sources are not among the largest traffic contributors to the crypto economy. This is because prices act similarly as a confounding factor (prices are tracked by both actual investors and enthusiasts, they may increase because there is more demand of informational resources and actual transaction activity, but because there is more transactional activity there might be more demand of informational resources as well). Instead, price returns are more likely to be used by professional investors as a success metric.

We would also prefer to focus on the models in the knee of the Pareto front since those represent the better trade-off between complexity and accuracy.

For Bitcoin, the model with complexity equal to 22 becomes informative. It contains a metavariable (*laser.online * vKontakte*) that appears in 6.6% of the models, and one of the variables from that specific metavariable construct (*laser.online*) appears in some form in 4 of the 6 finalist models. This is notable because while the other two variables in the model are a proxy for demand (the largest social network and search engine in Russia), usage of laser.online actually has investment implications – that service was a famous bitcoin scam and Ponzi scheme, where BTC holders actually invested and lost funds [5]. The p-value for the metavariables considered in the analysis is under 0.03, as shown in Figure 9 and Figure 10.

In the BitcoinCash economy, the drivers are notably different, and the complexity of the models tends to be higher. The fact that the independent variables are different than those that drive BTC returns speaks for the structurally different constitution of both economies: users of different services both consume investment information and have a preference to trade in different exchanges, such as Korea-based Bithumb. Some are even different people, as demonstrated by the fact that they seek information in Yahoo and social validation in Facebook, not in Yandex and vKontakte. The higher information content of higher complexity models may also induce over-fitting in the presence of noise.

What is notable is that the flows are diverse in terms of data sources, with everything from due diligence resources to entertainment — in other words, the idea that cryptocurrency market formation is only fueled by financial speculation is misleading. Bitcoin and derivatives based on this underlying are not financial products with a purely arbitrary value, as some commentators argue [17]. Each of these economies is a living organism that has a distinctive evolution that can be measured from the inception, or, from the time of the fork. And as complex organisms, they may have different levels of viability depending on the connectedness, influential actors, and risk present on their associated networks.

4.1 Trust asymmetry: the quantitative approach

4.1.1 Shape

The comparison of the development of symbolic regression expressions over generations provides the first proof of dissimilarity between the crypto economies; consistent with the nascent stage of the BitcoinCash economy, twice as many generations are required to model the returns as a function of inflows when compared to the more mature Bitcoin economy (see Figure 11).

Furthermore, it is possible to map the asymmetry of trust using a combination of multidimensional scaling, a statistical technique, and topological data analysis [11], a new type of econometric analysis which complements the standard statistical measures and has been used to detect early warning signals of imminent market crashes.

We begin by selecting functions from the Model Selection Report with complexity at the same accuracy level (e.g. 10^{-4}). Secondly, we draw a graph where a set of vertices ($v_1, \ldots, v_N$) is an element of V connected by M edges ($e_1, \ldots, e_M$) that are elements of E, where the length of each edge, ($l_1, \ldots, l_M$) are elements of L. The edges mirror complexity values, giving rise to a complexity space (in our case, a *trust space*, since at least one model included in the subset contains a variable that is a direct expression of investor's financial commitment – such as the use of a cryptocurrency exchange).

Figure 12 shows a tangible representation of the trust imbalance concept represented in Figure 3. By comparing the edge lengths (Euclidean distance) and complexity values using a ratio of the form distance/complexity, we find that the median distance is 0.00235542 for Bitcoin and 0.000860686 for BitcoinCash. The counterintuitive finding is that although the Bitcoin economy is more complex in macroeconomic complexity terms (diversity, and ubiquity of services), during the stage of formation of the competing BitcoinCash economy the complexity of models required to describe it is higher, given a similar level of accuracy. That is, even in terms of structure, the older economy is in a relatively steady state in relation to the new entity.

4.1.2 Dynamics

To model the dynamics we make use of Forrester's System Dynamics approach, a tool familiar to econometricians and policymakers. If we simplify to obtain the form of a two-sided system (what one economy loses the other gains) and focus on the flows in one direction, the schematic is as shown in Figure 13. The "goal" is an implicit input to the top component, and the flow of attention (with a gauge that implies a variable rate of action) is an input to the stock component at the bottom; the feedback loop represents information about the state of the level of trust.

In analytical form, the general equation that describes the stock component is (1).

$$level = \int_n^m \Sigma\,(in\_flows) - \Sigma\,(out\_flows).$$

Where n, m denote the complexity boundaries; we integrate over time, since we are measuring usage per month. The outflows are implied, and not shown in the graph, but we assume that whatever attention BitcoinCash is losing, Bitcoin is gaining –although in practice there might be as well leakages towards other competing forks.

So, at complexity level 11 (the worst error is what matters) BCH returns are driven by inflows into the BitcoinCash economy (2).

$$BitcoinCash_1 = (-0.13 + \frac{4.27 \cdot 10^{-6}}{github}).$$

And outflows can be described by the Bitcoin economy gains (3).

$$Bitcoin_1 = (4.80 + \frac{2.90 \cdot 10^{-2}}{duckDuckGo}).$$

At the same level of complexity the error measure associated to the Bitcoin model (0.04) is lower than for the BitcoinCash model (0.283); again, the result demonstrates the behavioral traits of the economic agents, as you would expect attention flows towards a software code repository (Github) become a factor for the newer coin, while the more established coin has higher visibility in organic channels (in this case, duckDuckGo, a search engine popular among developers).

This formulation encapsulates tacit knowledge since the model includes information in people's heads (e.g search patterns are revealed preferences, but are private to the user until the data is mined). It also contains explicit knowledge: blockchain unprecedented advantage is the public availability of transactional data. But from an investment perspective, the reason why modeling the level of trust is important is because the shape of the trust surface has a relationship with the probability of gain or loss [14] ; this extends as well to the domain of computational trust [12] a discipline in information security that deals with the analysis of trust structures such as those of a PKI (Public-Key Infrastructure) .

Fields finance. Another way to analyze the condition of asymmetry is by looking at trust imbalances among the same set of variables. In this way, we force the evolutionary algorithm to choose the best model that simultaneously contains both variables, and that allows for the flow to be visualized on a higher dimensional space (e.g. a vector field). To make the streams fully descriptive of the path to material economic activity (not simply market sentiment) we use blockchain fees rather than returns, and time series of daily usage data rather than share of inflows; the off-chain data expressively includes variables related to transactional activity (e.g. cryptocurrency exchanges, cryptocurrency payment platform for merchants). This allows for a better description of the causal relationship, and facilitates additional verification using forecasting methods such as bivariate Granger causality [20].

The resulting inflow equations are arranged into a field of the form given by (4).

$$\{Fees_{BCT}\ ,\ Fees_{BCH}\} = \{f\,(X_1,\ X_2)\,,\ g\,(X_1,\ X_2)\}.$$

Where X_1 refers to huobi.pro, a Chinese exchange; X_2 refers to coinpayments.net, a payments platform.

We slice the data by month (from September to November), to focus on the periods of analysis that are of interest – where we want to study the persistence or the break of trust symmetry. We obtain 6 equations in total, 2 for each month (each one describes how usage of the services under study may predict the movements in BTC or BCH fees). To obtain the rate of change of inflows levels (rather than levels themselves) we use the expression (1) applying a derivative at both sides and without other modification than assuming outflows equal 0; this requires that we compute the gradient of the field. The results are plotted in Figure 14, where X_1 is the component in the horizontal axis.

The flows give rise to a field. The f term (blue) and the g term (brown), each is expressed by vectors with components X_1 and X_2. We see how in September the vectors almost cancel out each other, however, the effect of consumption on BTC is leading –in fact, that month neither the exchange or the shopping cart solution show flows that are meaningfully correlated to the BitcoinCash economy. The economy of BitcoinCash actually becomes relevant to these services in October; as for Bitcoin, fees behavior is better described by the rate of exchange usage in October and by the rate of merchant service usage in November. The flows are mapping the belief consensus of the users of each coin.

The transition from September to October marks the phase change in trust dynamics (when the new coin adoption actually kicks off among the general public).

These observations are confirmed by the sensitivity metrics of the models (Figure 15). We see how in October, and especially in November, the relative impact that variables have on the target variable becomes material. We calculate sensitivity as the product of the mean of the absolute value of the partial derivative of X_2 with respect to X_1 , and, the ratio of the standard deviation of X_1 and the standard deviation of X_2. The % positive or negative represents the likelihood that increasing this variable will increase the target variable.

5 Conclusions

Digital assets detractors usually say that there is no proven demand for cryptocurrencies, but it has been demonstrated that demand not only can be measured but that crypto-economies and their driving variables can be ranked as demand evolves [**?**]. Perhaps the exercise of comparing Bitcoin and BitcoinCash is not entirely fair (after all BTC had the first mover advantage, by several years), but the heuristics that we have learned from the data have relevant implications nonetheless. For instance, one could identify what are the sources of systemic importance, or what traffic is overpriced or underpriced. And since in blockchains transaction count and exchange volume can be manipulated by batching transactions and other artifacts, one of the viable measures of value might be actual supply and demand of attention.

Furthermore, if crypto assets defy the “Efficient Market Hypothesis” and the idea that all available information is encoded in prices, something more profound may be going on here: beyond any of the traditional definitions of utility, *disintermediation of trust* by itself might entail a premium. In that case, the value of the chain may reside on the chain itself: the nodes running the software are simply an expression of people’s beliefs — being that the belief that the market can be manipulated for personal gain; that it is about time to challenge the government monopoly on money; that algorithmic money might be the more convenient utilitarian artifact to conduct transactions if you have already digitized a large part of your day-to-day activities; or else. This belief consensus is a human-machine construct, and perhaps this is why economists who are not trained as technologists have a hard time grasping the implications of a blockchain financial system.

But what is more intriguing is that what the quantitative analysis reveals is not conflicting at all with the definition of intrinsic value — value is, after all, a matter of perception. So the argument that cryptocurrencies have no intrinsic value is without merit, and as we have demonstrated, not backed by data. Furthermore, even regulators stances are evolving; according to FinCEN, a digital currency can represent a “value” that “substitutes for currency” [1] – this value representation is what is encoded in the off-chain network flows that we have quantified as trust metrics builders. And a more fundamental question about value arises: as the trust asymmetries between crypto economies reveal a structural divergence in value perception, could this paradigm provide incontestable proof of value in digital assets, including those with enhanced privacy features which by default make key transactional data opaque or unavailable?

Immediate applications of this research include Discreet Log Contracts [9], which have the potential to enhance the use cases of Bitcoin and other cryptographic currency networks by allowing users to discreetly enter into futures contracts for a wide variety of assets, trusting oracles only to sign the correct price. Possible next steps include the formalization of evaluation frameworks for the trust metrics and trust models. For instance, the share of flows is in principle a probability, therefore it could also be analyzed using formalisms from logic. Subjective logic [13] is a type of probabilistic logic that explicitly takes uncertainty and source trust into account, and could be used for this purpose. Also, topology concepts such as persistent homology could be implemented to study the robustness of the trust metrics obtained [7]. Finally, one may argue that in essence, trust asymmetries are a particular case of information asymmetries. In this view, we could use the rich literature of information theory, signal processing, complex networks, and, econophysics to develop on the methods here described.

References

[1] Beyond Best Practices: Regulatory Compliance Now a Necessity in the Cryptocurrency Sector — Money Laundering Watch. https://www.moneylaunderingwatchblog.com/2017/12/beyond-best-practices-regulatory-compliance-now-a-necessity-in-the-cryptocurrency-sector/. Accessed on Sun, February 25, 2018.

[2] Bitcoin & Crypto Enthusiasts in Africa - Leading ICO Marketing, Legal & Technical Support. https://ibcgroup.io/jobs/bitcoin-crypto-enthusiasts-africa/. Accessed on Mon, February 26, 2018.

[3] Bitcoin Cash. (n.d.). In Wikipedia. Retrieved February 21, 2018, from https://en.wikipedia.org/wiki/Bitcoin$_Cash.$

[4] BitPays Bitcoin Payments Volume Grows by 328Yearly. https://blog.bitpay.com/bitpay-growth-2017/. Accessed on Mon, February 26, 2018.

[5] Laser Online Retrieved February 21, 2018.

[6] On the difficulty of estimating on-chain transaction volume - Coin Metrics. https://coinmetrics.io/difficulty-estimating-chain-transaction-volume/. Accessed on Mon, February 26, 2018.

[7] Mickal Buchet, Frédéric Chazal, Steve Y. Oudot, and Donald R. Sheehy. Efficient and robust persistent homology for measures. *Computational Geometry*, 58:70–96, oct 2016.

[8] François E. Cellier. Basic Principles of Continuous System Modeling. In *Continuous System Modeling*, pages 23–50. Springer New York, 1991.

[9] Thaddeus Dryja. Discreet Log Contracts Thaddeus Dryja. *MIT Digital Currency Initiative*.

[10] Jay W. Forrester. System dynamics—the next fifty years. *System Dynamics Review*, 23(2-3):359–370, 2007.

[11] Marian Gidea and Yuri Katz. Topological data analysis of financial time series: Landscapes of crashes. *Physica A: Statistical Mechanics and its Applications*, 491:820–834, feb 2018.

[12] Audun Jøsang. Computational Trust. In *Artificial Intelligence: Foundations Theory, and Algorithms*, pages 243–270. Springer International Publishing, 2016.

[13] Audun Jøsang. Subjective Networks. In *Artificial Intelligence: Foundations Theory, and Algorithms*, pages 303–326. Springer International Publishing, 2016.

[14] Audun Jøsang and Stéphane Lo Presti. Analysing the Relationship between Risk and Trust. In *Lecture Notes in Computer Science*, pages 135–145. Springer Berlin Heidelberg, 2004.

[15] Mark Kotanchek, Guido Smits, and Ekaterina Vladislavleva. Pursuing the Pareto Paradigm: Tournaments Algorithm Variations and Ordinal Optimization. In *Genetic Programming Theory and Practice IV*, pages 167–185. Springer US.

[16] Gkhan Kula, Martin Raab, and Sebastian Stahn. *Beyond Smart Beta*. John Wiley & Sons Ltd, may 2017.

[17] John Quiggin. Opinion — What Bitcoin Reveals About Financial Markets. https://www.nytimes.com/2018/02/08/opinion/bitcoin-financial-markets.html. Accessed on Wed, February 21, 2018.

[18] Cesar A. Hidalgo Ricardo Hausmann. The Atlas of economic complexity: mapping paths to prosperity. *Choice Reviews Online*, 51(11):51–5931–51–5931, jun 2014.

[19] Rick Riolo, W.P. Worzel, Mark Kotanchek, and Arthur Kordon, editors. *Genetic Programming Theory and Practice XIII*. Springer International Publishing, 2016.

[20] Anil Seth. Granger causality. *Scholarpedia*, 2(7):1667, 2007.

[21] Percy Venegas. Crypto Economy Complexity.