

Asymmetric Trust and Causal Reasoning in Blockchain-based AIs

Percy Venegas¹

¹Economy Monitor

ABSTRACT

We use genetic programming evolved networks, vector fields, and signal processing to study time varying-exposures where trust is implied (e.g. a conversion event from attention flow to financial commitment). The datasets are behavioral finance time series (from on-chain data, such as fees, and off-chain data, such as clickstreams), which we use to elaborate on various complexity metrics of causality, through the creation parametric network graphs. We discuss the related methods and applications and conclude with the notion of social memory irreversibility and value by memory as useful constructs that take advantage of the natural fact of the existence of trust asymmetries, that can be operationalized by embedded AIs that use distributed ledgers both as the substrate of their intelligence and as social computers. By being context-aware, those intelligent agents are able to intervene in problematic stressors and contribute to minimizing network fragility.

Keywords: systemic risk, behavioral finance, economic complexity, evolutionary computation, computational trust, the blockchain, cryptocurrencies, market microstructure, reality mining.

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

There is none *deceived* but he that *trusts* –*Benjamin Franklin*

Introduction

Given the current state of knowledge, it is relatively easy to have artificial intelligent agents to find patterns and to formulate predictions following some objective criteria. But to get become useful in comparison with human intelligence, it is crucial that those agents are able to ask: Why? Posing the question is an exercise on causal reasoning, a realization of the awareness of cause and effect. It is also a matter beyond logic formalisms– the interface matters. That is because once the intelligent agent is able to ask why?, it will be also in a position to ask counterfactual questions, such as how an intervention may change the output, or even the causal relationship itself.¹ This is particularly important in the case of blockchain-based AIs because directionality matters (causation works in one way) and because the substrate of the AI is a fully or partially immutable ledger.

One may attempt to reduce the proposed solution to the problem to the application of well-known methods, such as Bayesian networks; since blockchain systems are deterministic and it is desirable that the constructs operating on top of them (e.g. smart contracts) behave with some degree of predictability, establishing an appropriate intuition of the priors by access to on-chain data and some sort of data integrity-verified artifacts (e.g oracles) may at least partially achieve this purpose. However, such a simplistic approach would deprive the AI of context: the world is not presented to us as a data feed, but rather as a dynamical experience in which the embeddedness into a social context² dictates the response, especially in the forming stages of intelligence. Particularly, the repeated use of metaphors such “circles of trust” in industry and personal relations hints at the tendency that humans have to at least implicitly compute similarity metrics (to define the boundaries of that circle or space) and to elaborate mechanisms to detect violations to certain social laws and descriptive models of economic behavior.³ In a way, to engage in the world we require that other agents are “trust verified”.

Trust is fundamental to the human experience, yet it is little understood. But AI, web analytics, and blockchain technology have come to change that. For the first time in history, we have real-time data to map how attention flows, and understand how people actually assess risk and commit resources. And with AI we can augment our own intellect,⁴ to understand complex

socio-technical systems. In some cases, this is a full departure from the prevailing economic theories, that were developed using experiments conducted on small groups, incomplete and delayed macroeconomic data, or theoretical models which are completely dissociated from reality. There is no reason why economics and the social sciences have to be called “soft” anymore; there is no such thing as hard and soft sciences, a scientist should always operate in the realm of facts and quantitative evidence, otherwise, he is only a commentator.

Computationally, biologically, and socially, humans “need” to trust.⁵ And even when dealing with “trust-less” systems such as distributed ledger technology, everyone (including AIs) need to trust “on the design”. This work is concerned with the role of trust asymmetry⁶ in the causal reasoning process of blockchain-based AIs. We will approach it from the perspective of the machine, of the method and apparatus needed for the intelligent agent to make consequential decisions in the world: is there an asymmetry, then why? And, where and when trust asymmetry breaks?

Related work

Integrating social information with traditional network layers

A blockchain-based AI becomes aware of the environment via off-chain data. To conceptualize this using the OSI model as a reference, we use a cross-layer stack (layer 7 and layer 6). In practice, the financial activity logged in the blockchain is the expression (e.g. a conversion event) of the consumption, flow of attention, and commitment of resources in adjacent networks such as the web and mesh IoT. For instance, when a web browser creates a request (e.g. GET / HTTP) a Java-based application could log the hits, detect the device type (mobile or desktop), and other features included in the user-agent header. Also by looking down in the stack to the routing level, ISP data is used to obtain geographical origin, redirect path and destination. This sort of “alternative data” becomes especially useful when studying permissioned and semi-centralized networks, since not all data is publicly available and suitable proxies are required.

Ripple

Formally, Ripple is not a blockchain, but a common ledger based on a proprietary technology to cater to the privacy needs of the banking industry –therefore, some transactional and network activity details are unavailable to the public. We tracked daily usage for the 100 most popular services among prospect Ripple users over the course of 18 months (548 days in total). We use daily prices as target variable since a general audience-prospect user will be inclined to look at the daily prices, while professional investors usually focus on daily returns. The services included those directly related to cross-border payments operations (e.g. gateways) and other peripheral to the economy, including price information services, wallets, and the like. We investigate the long-term market structure, specifically the demand signals from that segment of newcomers. We started with one hundred services, and after many rounds of elimination making different formulas compete with each other for accuracy (using symbolic regression), the simplest and most meaningful relationship expresses price as a function of two constant values and the demand for the services of a particular exchange. In other words, the simpler predictive model to provide any insight traces back the rise of Ripple among this segment to the popularity of one of the prominent exchanges (of the centralized type) that listed the coin. One such predictive model can be expressed as $Price = a * exchange1 - b$

A more complex model has the form $Price = a + b * sma(wallet_users, 21) * sma(wallet_users, 37) + c * wallet_public^2 - d * exchange - e * gateway * sma(wallet_users, 21) * sma(wallet_users, 37)$

According to this, from May 2017 to December the use of a particular *wallet* created support levels of 21 and 37 days (using simple moving averages) and it had the bigger impact of all variables discovered (increasing the use of this wallet has a positive impact on price 100% of the times). This means that the usage of this service serves as a “canary in the mine”, i.e a prolonged decrease in usage (being all conditions equal, such as not having a similar alternative replacing the use of the wallet) will indicate weakening demand fundamentals.

The first negative term is a *gateway*, which in Ripple’s architecture means “businesses that provide a way for money and other forms of value to move in and out of the XRP Ledger”. This particular issuing gateway supports both Yuan/XRP and Yuan/Stellar pairs and provides services mainly in China, and to a lesser extent in Japan and the US. This same gateway’s popularity increased following the crackdown on bitcoin exchanges in China.

The second negative term is a Chinese *exchange*, of the centralized type. That is, as demand for the exchange of CNY/digital asset increases, this may be exercising some downward pressure on price. The negative effect is slightly larger when people use the centralized exchange, rather than a Ripple gateway. This may suggest that some operatives turned to Ripple as a haven when the Bitcoin exchanges were hit, although prices are still susceptible to movements of XRP assets in and out of the economy via a gateway. But strong demand from the middle market supersedes the fears of those uncomfortable with all-time-highs, and this is why the usage of the Ripple wallet exploded on Dec 13–14th, in tandem with the spike in price volatility of XRP — alongside with attractive dynamics of the BTC/XRP pair. It is also important to note what the AI does not see: the lack of any oscillatory term in the formula (sin, cos) hints at the lack of strong regularities (periodicities) during the eight months of the analysis. The other valuable observation here is that in the absence of access to many of the Ripple ledger statistics that will normally allow identifying large holders, the usage of the wallet allows to single out the mid-market as a force driving the market (and this wallet service is predominantly accessed from the US).

Time series analysis and prediction

The application of genetic programming to the study of behavior and causation in cryptocurrency markets is not only an analytic artifact, but it is fundamentally aligned to the nature of the problem.

Taleb and Douady⁷ explain that the natural selection of an evolutionary process is particularly antifragile since a more volatile environment increases the survival rate of robust species and eliminates those whose superiority over other species is highly dependent on environmental parameters. In the context of cryptocurrencies, we could use temporal correlations in blockchain traffic to gauge the response of a given object (e.g. fees) to the volatility of an external stressor that affects it, but another approach is to simply study the response of the market (as measured by a common risk metric, such as volatility) to the actual market behavior (with the consumption of services and information measured by HTTPs requests, including endogenous variables such as the activity at the customer service channels of the wallet and the exchange itself, mining pools, mining profitability feeds, and so on; in this toy example we use just a subset of those variables). The driving variables are modeled using symbolic model ensembles, as in Figure 1, which is based in daily time series for the period of November 1st, 2016 to May 9th, 2018.

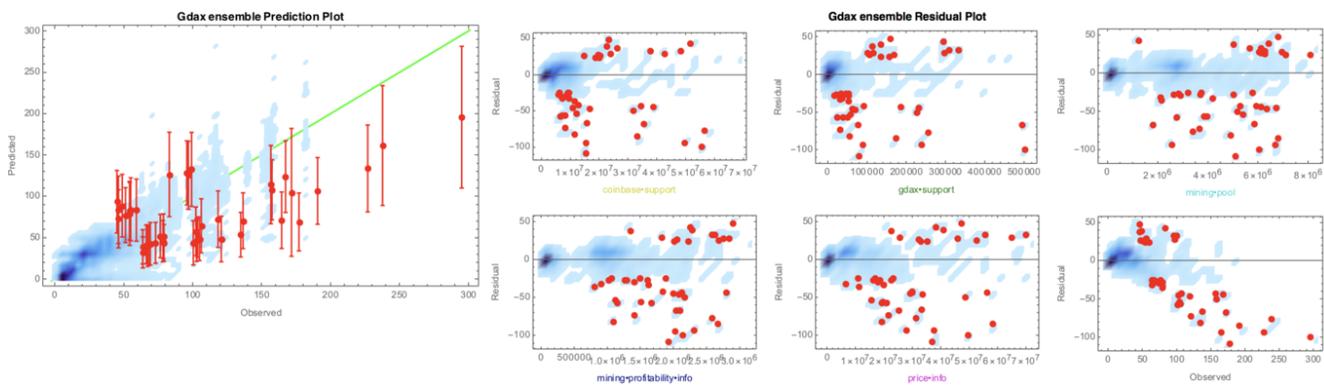


Figure 1. Volatility of BTC price in cryptocurrency exchange and environmental (demand) signals

The nonlinearity in a source of stress is necessarily associated with fragility. This is perhaps why low-quality coins fail —marketing activity is an environmental variable only, while actual installed capacity and operational infrastructure (i.e bitcoin’s) is a robustness contributor factor. Once we have established the driving variables, we need to study the volatility of those variables (and the non-linear relationships). We see how with high volatility the predictor performs poorly, at least with this small subset of variables, which are also all highly correlated. A possible fragility test would be to derive the “volatility of volatility” where the price volatility prediction becomes a traffic prediction problem. But the key realization, in alignment with Taleb and Douady, is that to be fragile the system has to be non-linear to harm (has to be accelerated to harm). Since fragility that comes from linearity is immediately visible, the hidden risks and potential harm come from non-linearity. In this example, the AI notes that the activity in a particular mining pool frequented by the users of the exchange has a low correlation to volatility, and will use the second derivative of volatility respect to the mining pool (usage per day is the event size) as a “trust” distance metric. The formula is obtained using symbolic regression as well, computing a smoothing

spline for volatility with respect to mining pool, and then, computing the symbolic derivative of the spline functions (cubic polynomials), and evaluating the expression at various data points. One of the possible models has the form $D(\text{Volatility}, (\text{Mining pool}), 2) = (\sin(1.27652458974758 + 1.63551681837977e-5 * (\text{Mining pool})) + \cos(3.2702109619178e-5 * (\text{Mining pool}) + \sin(2.14970699758616e-5 * (\text{Mining pool})))) / (\text{Mining pool})$

Of course, the data set can be enhanced with multiple data sources, and the prediction error reduced by combining additional methods (e.g. de-noising with recurrent neural networks and convolutional neural networks). But by providing a context of the environment to the intelligent agent, the AI is in a better position to reason on the trustability of the result.

Spatio-temporal patterns in blockchain networks

Space of Production

In one of the first studies of the disciple of Human Geography into distributed shared ledgers, Blankenship⁸ conceives blockchains as production spaces where developers are the dominant class within the social and technical spaces of the technology, have ultimately leveraged their knowledge and power dynamics to accumulate wealth via the token value, and then shifted into the role of investors. This necessarily involves automation (exploitation of automated robot labor) and obfuscation of the mechanisms of production – geographic borders are defined via conflicting abstract conditions (social, political, and economic), and put within the qualitative context of social dynamics. Humans not only trust in the source, but they also trust the structure – you generally do not care about who wrote a diet article (even if a change in lifestyle can have a lasting impact on health) as long as “structure” suggest the writer is not a charlatan. A similar behavior is observed in crypto markets, where traders and investors keep lists of Twitter accounts that they trust on to relay accurate information about the state of the market, and that is facilitated by other traders: it does not count only who is saying it, but who is following – this is part of the social fabric of crypto markets, the structure of the network encodes tacit knowledge and reflects abstract conditions and boundaries. The distance trust metrics have very tangible implications for individual and corporate purposes; “a member of my group said” (even if he had materially different attributes) is generally better than what an outsider says. The implications in terms of the theory of the firm:⁹ you do business in the proximity of your circle (your trust space) where trust is secured, even if it is more expensive to produce in your inner circle, and it is cheaper to acquire in the boundary (e.g. potential partners) – but going beyond that will require a significative leap of faith and the associated risk should be priced-in. The AI will understand this human inclination (as shown in Figure 2), as a trust differential in terms of metric entropy.

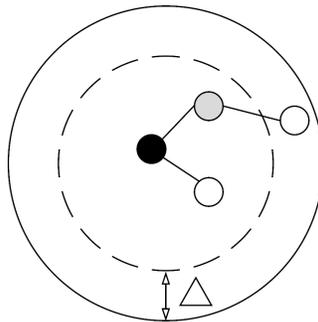


Figure 2. Trust spaces

Circles of trust and Kolmogorov entropy

Entropy is the price of structure.¹⁰ While the models obtained using genetic programming (Figure 1) have an associated complexity which is strictly related to leaf tree structure (genotype), as seen in Figure 3, the phenotype (the expression of the genotype in mathematical formulae) itself serves as an indication of the level of complexity.

The Kolmogorov complexity measures the length of the shortest program required to reproduce a pattern. We approximate the Kolmogorov complexity using a lossless compression technique. In this way, we found that model 1 and 2 have both an

			volatility
Complexity	1-R ²	Function	
1	11	0.319	$10.33 + (3.02 \times 10^{-6}) \text{coinbase} \cdot \text{support}$
2	15	0.285	$1.46 + 0.24 \sqrt{\text{gdax} \cdot \text{support}}$
3	19	0.257	$3.04 + (2.44 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (5.44 \times 10^{-6}) \text{mining} \cdot \text{pool}$
4	23	0.252	$-2.21 + (1.96 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (7.77 \times 10^{-3}) \sqrt{\text{price} \cdot \text{info}}$
5	26	0.243	$-0.79 + (2.92 \times 10^{-6}) \text{coinbase} \cdot \text{support} + \frac{10.57 \text{price} \cdot \text{info}}{\text{coinbase} \cdot \text{support}}$
6	30	0.234	$0.43 + (2.21 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (2.89 \times 10^{-6}) \text{price} \cdot \text{info} - (8.55 \times 10^{-13}) \text{mining} \cdot \text{profitability} \cdot \text{info} \text{price} \cdot \text{info}$
7	31	0.226	$0.97 + (2.10 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (2.33 \times 10^{-6}) \text{price} \cdot \text{info} - (2.91 \times 10^{-14}) \text{price} \cdot \text{info}^2$
8	34	0.221	$1.64 \times 10^{-13} + (2.12 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (2.10 \times 10^{-6}) \text{price} \cdot \text{info} - (9.65 \times 10^{-21}) \text{mining} \cdot \text{profitability} \cdot \text{info} \text{price} \cdot \text{info}^2$
9	38	0.212	$1.74 \times 10^{-13} + (2.75 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (1.48 \times 10^{-6}) \text{price} \cdot \text{info} - \frac{(1.82 \times 10^{-15}) \text{price} \cdot \text{info}^3}{\text{mining} \cdot \text{pool}}$
10	42	0.207	$10.71 - (1.15 \times 10^{-5}) \text{mining} \cdot \text{pool} + (5.95 \times 10^{-13}) \text{coinbase} \cdot \text{support} \text{mining} \cdot \text{pool} + (4.99 \times 10^{-6}) \text{price} \cdot \text{info} - (7.17 \times 10^{-14}) \text{price} \cdot \text{info}^2$
11	45	0.200	$2.20 \times 10^{-13} + (1.55 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (7.27 \times 10^{-19}) \text{coinbase} \cdot \text{support} \text{gdax} \cdot \text{support} \text{mining} \cdot \text{pool} + (2.82 \times 10^{-6}) \text{price} \cdot \text{info} - (4.17 \times 10^{-14}) \text{price} \cdot \text{info}^2$
12	46	0.198	$2.24 \times 10^{-13} + (1.32 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (6.02 \times 10^{-21}) \text{coinbase} \cdot \text{support}^2 \text{mining} \cdot \text{pool} + (3.03 \times 10^{-6}) \text{price} \cdot \text{info} - (4.66 \times 10^{-14}) \text{price} \cdot \text{info}^2$
13	48	0.193	$1.67 \times 10^{-13} + (2.13 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (1.46 \times 10^{-18}) \text{coinbase} \cdot \text{support} \text{gdax} \cdot \text{support} \text{mining} \cdot \text{pool} + (1.67 \times 10^{-6}) \text{price} \cdot \text{info} - (1.77 \times 10^{-19}) \text{gdax} \cdot \text{support} \text{price} \cdot \text{info}^2$
14	59	0.183	$1.86 \times 10^{-13} + (1.56 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (1.80 \times 10^{-18}) \text{coinbase} \cdot \text{support} \text{gdax} \cdot \text{support} \text{mining} \cdot \text{pool} + (2.73 \times 10^{-6}) \text{price} \cdot \text{info} - (1.66 \times 10^{-13}) \text{mining} \cdot \text{pool} \text{price} \cdot \text{info} - (1.80 \times 10^{-19}) \text{gdax} \cdot \text{support} \text{price} \cdot \text{info}^2$
15	60	0.181	$1.79 \times 10^{-13} + (1.78 \times 10^{-6}) \text{coinbase} \cdot \text{support} + (1.85 \times 10^{-18}) \text{coinbase} \cdot \text{support} \text{gdax} \cdot \text{support} \text{mining} \cdot \text{pool} - (9.55 \times 10^{-20}) \text{mining} \cdot \text{pool}^3 + (2.33 \times 10^{-6}) \text{price} \cdot \text{info} - (2.09 \times 10^{-19}) \text{gdax} \cdot \text{support} \text{price} \cdot \text{info}^2$

Figure 3. Models (BTC volatility in GDAX)

approximate byte count of 416 (despite the delta in evolutionary model complexity), and model 15 has a byte count 768. That is, in (metric) information theoretical terms the first two simplest models present invariance with respect to affine transformations in the trust space. This is a disambiguation aid that the AI uses for decision making: a description of the world with a lower error (model 2) can be encoded at the same level of computational complexity as an inferior alternative.

Configuring blockchain protocols' parameters based on the networks' topology analysis

Authors have explored graph-based techniques to automatically detect realistic decentralized network growth models from empirical data¹¹ and to study systemic risk in cryptocurrency markets.¹² The causal inference network in Figure 4 uses a parametric approach based on symbolic regression to derive the relationship between nodes, starting from a sample of 2000 price and consumption of services in the cryptocurrency markets during the period of August 2016 to January 2018.

This approach is based on empirical data, is robust to error, and has high explanatory power (all sensitivity and error-complexity figures are accessible via the description of the symbolic regression evolutions). However, to capture the full scope of causality, the “inherited fragility”, the AI makes use of signal processing and other techniques. Figure 5 depicts the use of the wavelet coherence method, which has been previously applied to the study commodities and financial time series^{13, 14} to understand when and how strongly an off-chain signal (in this case, the usage of a popular Ethereum web wallet service) affects the price of the cryptocurrency, ether. The AI uses this not only for disambiguation but to actually map the causal relationship in time and frequency domain (i.e. learn when one signal lags or leads the other).

Here the wallet signal leads the price signal, on day 120 in a cycle of approximately 4-6 days, where both signals are also strongly correlated. In the case of unruly distributions, the results are enhanced in combination with other methods (e.g. Granger causality,¹⁵ Bayesian structural time series models,¹⁶ among others). The key realization is that although market behavior (network dynamics) is not the same as market conditions (market structure), the intelligent agent can use the same

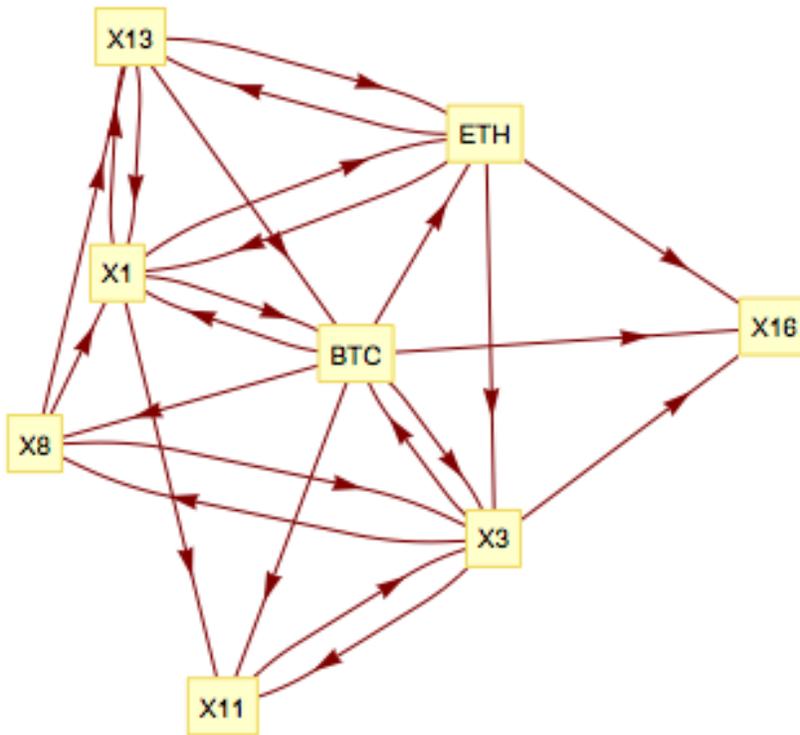


Figure 4. Causal inference network (BTC-ETH)

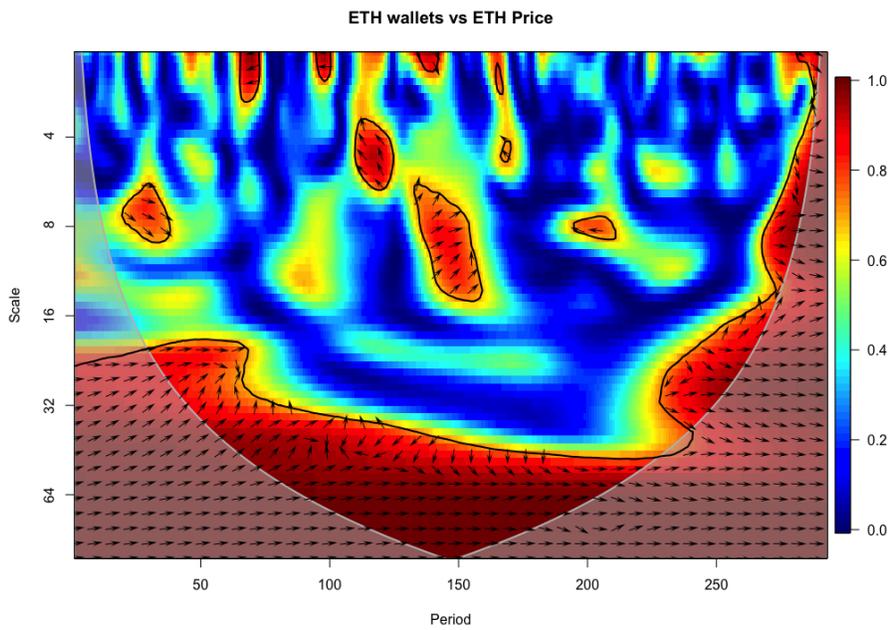


Figure 5. ETH wallet vs ETH price. July 7th 2016 to June 30th 2017.

Robust Models Ensemble [ref = 47.81]

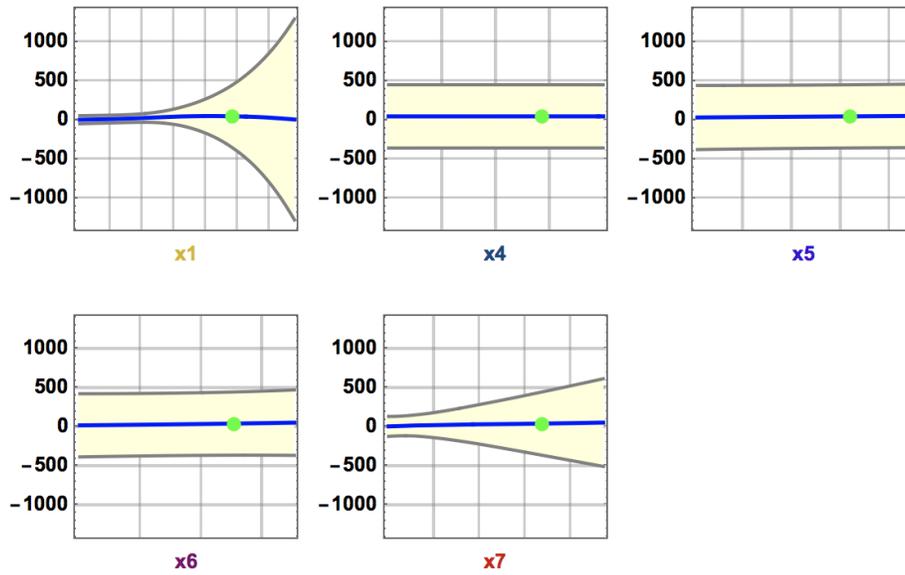


Figure 7. Ensemble response plot (BCH fees)

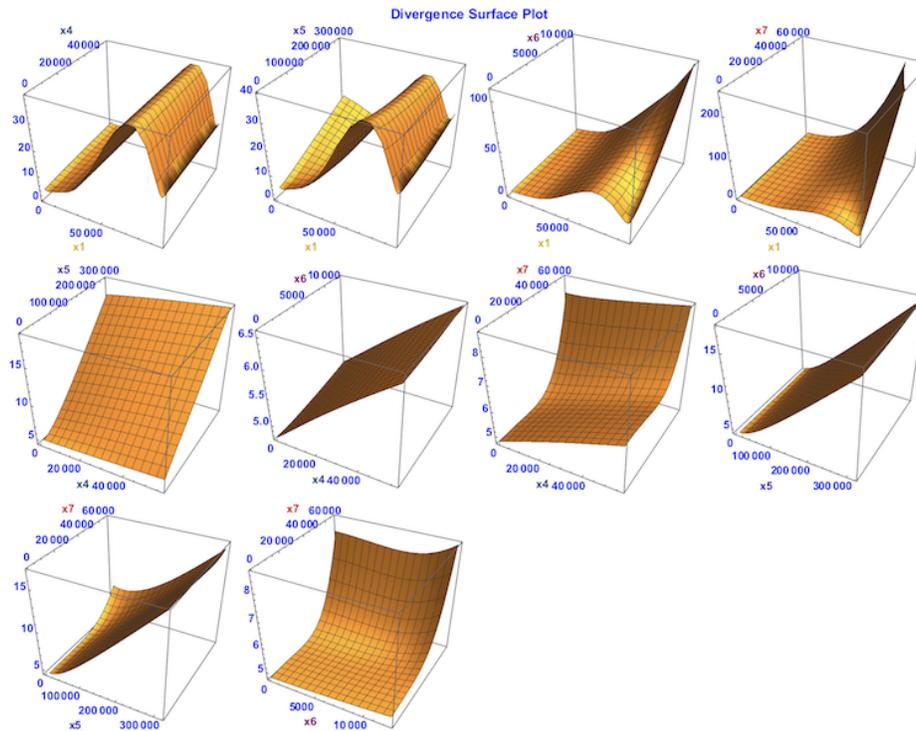


Figure 8. Divergence (BCH)

Behavioral finance

Mis-pricing due to non-rational decision making and market inefficiencies offer arbitrage opportunities that an intelligent agent would try to exploit. But an AI that is aware of the trust asymmetries across its operational space is also able to compare intrinsic fragilities, even if the distribution of problematic events are not directly observable. In Taleb and Douady formulation, the risk measure assumes certain extrapolation rules that have first-order consequences, and these consequences are even more amplified when the risk measure applies to a variable that is derived from the one used for estimation – when the relation between the two variables is strongly nonlinear. For (predictive) navigational purposes, the agent asks whether people (or other AIs) have found a path of least resistance (evidence of trust asymmetry) and what is its associated trustability. This aspect is modeled using Forrester dynamics, and it captures the response to changes satisfying both system modeling and risk modeling.

Information flow

The AI that seeks to optimize blockchain configurations, or simply navigate the environment, is aware of the off-chain “social fabric” because it fills the role of communication: you can improve by introspection if you communicate.

To manage complexity several approaches are possible, including using Lawyer’s expected force (a centrality measure)¹⁹ to greatly simplify the problem. When node power is low, influence is a function of neighbor degree. As power increases, a node’s own degree becomes more important. The strength of this relationship is modulated by network structure, so it is expected that it will be more pronounced in narrow and dense networks such as social networking (e.g. Twitter channels of bitcoin whales). The network effect, however, has two levels: one is the on-chain\off- chain interplay (symbolic regression model of active accounts/addresses driven by social network activity), and the other is the off- chain\off- chain interplay (for instance, of the dynamics between Twitter channels and Telegram groups).

Vector fields as temporal streams

An activity must be decoded sequentially over time. The intelligent agent may do this by using a combination of genetic programming techniques (after all, somewhat static DNA and its transcription pattern over time creates biologically essential temporal patterns) and signal processing (e.g. Kalman filter, for short-term streams), but a complementary approach for fast evolving systems that are always in flux is to use actual fields. In the case of economic systems such as blockchains, standard signal processing analysis techniques and information theoretical measurements help visualize the historic correlations, but a sound investment strategy should also consider the correlation migration –how the correlation changes (or not) over time. While it is possible to plot a correlation graph for each point in time, we find that using vector fields²⁰ allows for mappings with a higher information density, especially for portfolios of a large size –for instance, consider that when tokenized Dapps are also viewed as assets, we are facing prohibitory large portfolio sizes. To implement the method we begin by defining the convention for the vector components. From the possible traffic sources for a new project, we found that referrals and social networks are the more prevalent, especially in the early stages of a proposal listing when word of mouth in social networks such as Reddit and the ability of the founding team to generate buzz in media and news sites plays a role. The resulting vector field gives rise to a flow. A fluid flow provides an effective way to summarize the dynamics of a portfolio to include an arbitrarily large number of entities, rather than simply scaling up the number and size of correlation graphs (not to mention that for communication purposes, a vector field is also a more intuitive representation of cashflows equivalents). In one hand, the (total) vector magnitudes are a measure of strength, in the other, the interaction between the different assets (as revealed by singularities in the flow) present a portrait of the system (the portfolio attention correlations). Figure 9 shows a vector field for a 32-asset mapping in Ethereum during March, April, and May 2016, rendered using 4 techniques to highlight different aspects of the flow.

Investors (and the intelligent agent) ascribe an intrinsic value to stability. By using the mapping from Figure 9 and small multiples to draw each month separately, every field snapshot is a moment in time, and the apparent flow mobility shows progression in portfolio positions. Therefore, one can easily identify which flow structures tend to remain unchanged, and when a major event occurred; the streamlined plot (Figure 9.d) is ideal for such type of visual analysis. The vector plot (Figure 9.c) presents the “intensity” dimension lacking in the streams, which are focused on directionality. The LIC (line integral convolution) rendering (Figure 9.c) is a human friendly and aesthetically pleasant format that helps reinforce the flow structure without losing analytical capability, especially if one makes it overlap the vector map, or the streamlines, depending on the data dimension to analyze (by using LIC the entropy of the visualization increases, more information is conveyed). The mesh network representation of the flow (Figure 9.d) is a machine format that maintains some of the human friendly features of the other visualizations –one can easily see how computation by clusters might become a useful device to reveal equilibrium points in the vector field topology: unstable nodes (sources or saddles), stable focus (spiral sink), stable centers, etc. This

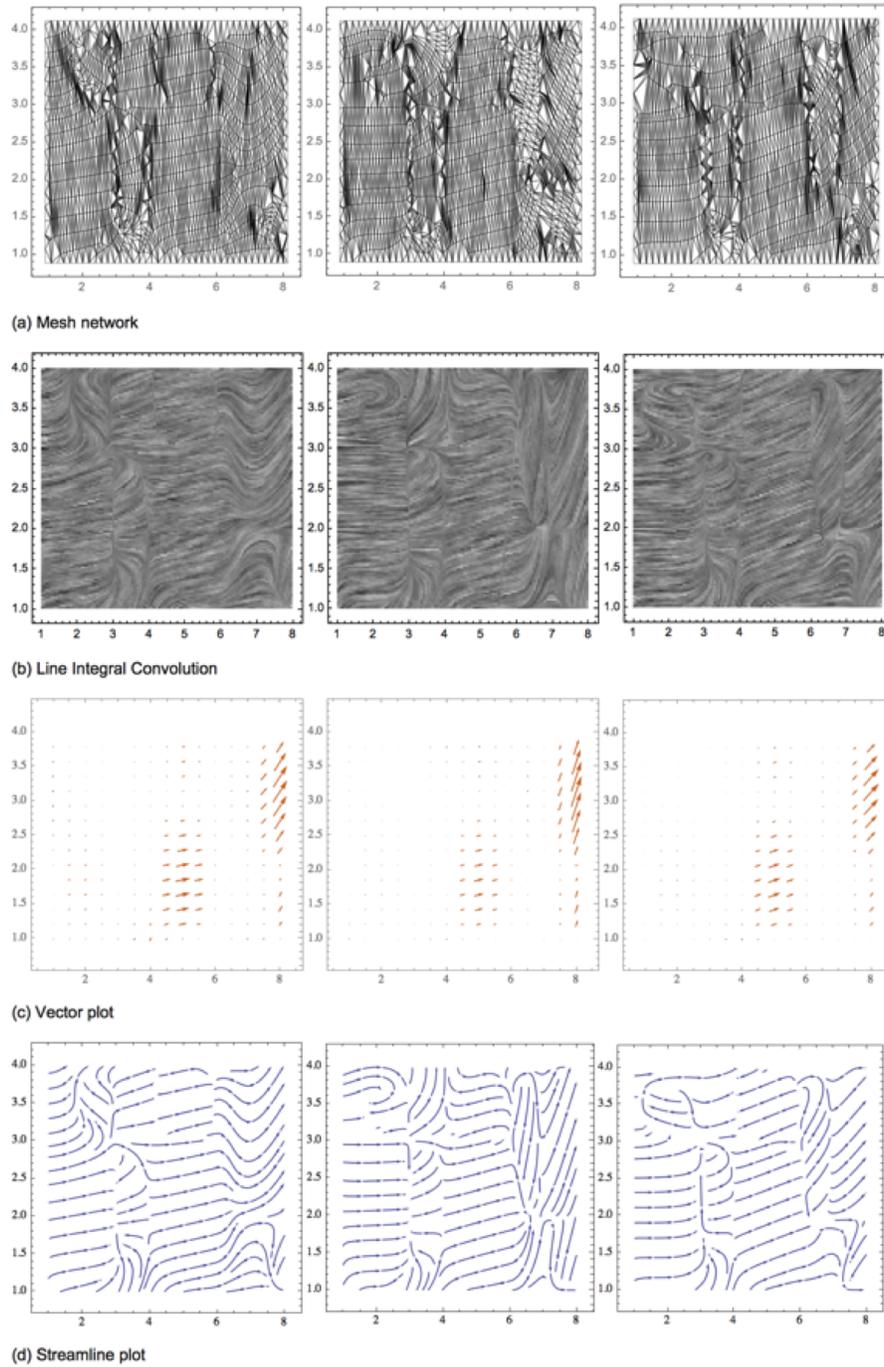


Figure 9. Time variant vector field sequence

representation is obtained by drawing mesh divisions between every line or polygon generated by a plotting function, in this case, the one obtained after the stream plot. Finally, given the duality between singularities in vector fields and network structure, the fields analysis is suitable to be implemented at scale.

Applications

Intelligence services

Although privacy coins offer desirable features in some settings, for national security purposes is often needed to understand the user's clusters at least at a macro level. Trust asymmetry (in the blockchain / off-chain boundaries) reveals information such as geography and audiences, which allows to re-construct digital personae (groups' identity profiles); it also provides insights into hidden states and phase transitions within those multiplex networks. The applications include mapping the character of Zcash and Monero communities and providing partial source/destination metadata related to the use of secret contracts and similar technologies that facilitate coin mixing (which obscure the original source of cryptocurrency used within the protocol). These applications are also relevant to market intelligence, a practice that becomes more challenging as international privacy standards strengthen.

Financial Risk prediction

Ensemble prediction with evolutionary computing augments both technical analysis and time series ARNN results by providing context and by providing explicit trustability ranges. The intelligent agent is thus capable of reasoning about interventions: what if I change X? This is the alternative to creating static models – rather, we create models dynamically and perform spatiotemporal encoding of information using a blockchain as a substrate for the intelligence. This also implies a sort of “value by memory” where a system that has *experienced* more about the world is more valuable than one that consists only of the algorithm.

Political risk prediction

The political economy is a contest for attention modulated by reputation, and thus a perfect fit for context-aware AI.

In multiples areas, from influencing public opinion to political campaign financing, demand is influenced by the available supply (of information).

An AI that minimizes trust asymmetries on its objective function can use well-known human biases (tendency to follow rules of thumb-credulity, cognitive dissonance-double down on beliefs, human inclination to spread pleasant-sounding lies) to assess provenance of the data and context, in applications related to detection and mitigation of fake news and deep fakes. The embedded Oracle can operate as a standalone feed, or as a complement to specialized technologies that take advantage of blockchain features for this purpose (no single arbiter of truth, public record). In this application, the genetic programming provides an audit trail on its genome (tree structures), and, an event-based notification function (when a breakdown of trust symmetry occurs).

Part of the tasks of the AI will deal with inferring intent: for instance, an analysis of the Bernie Sanders and Gary Johnson campaigns shows asymmetries at higher scales: the demand for information and actual voter commitment do not correlate for the top contributors (attention price). But It also pertains to crypto native applications: the bitcoin donation adoption was found to be more prevalent among libertarians, a group ideologically aligned to decentralization of monetary policy.

Conclusions

The characteristics of blockchain-based AIs such as being incentivized natively through the use of tokens of value, and not having a single point of failure, are attractive propositions, but also mean that decentralized intelligence will be hard to kill if something goes wrong. And, depending on the stage of its development, such a decision could meet ethic questioning. It is therefore imperative that those intelligent agents go beyond the basic expectation (do not do harm to humans, do the job, do not lose money) to actually solve the vulnerability issues of humans systems (security) while easing human anxieties by providing transparency (in the words of Manuela Veloso, verifiable answers and consistency of answer) and operating under a set of beliefs (“mental” models) that are compatible with the human experience. To do this, the AI needs to have an adequate degree of trustworthiness on its own assessment, and trustable symbolic regression provides a means to that – in the same way that humans augment their intelligence with AIs, AIs can augment their intelligence with a time-variant model of the environment created from off-chain signals. This implies both operating with a reasonable degree of intuition about cause and effect, and with the ability to deal with edge cases (even in the case of narrow, purpose-specific AI).

If we take a lesson from history, making a new weapon so terrifying that it will be inconceivable to use (e.g. Leonardo's battlefield tanks, von Neumann's mutual assured destruction nuclear doctrine), is itself a form of deterrence. If blockchain is truly irreversible social computing,²¹ and being trust hard to earn and rebuilt, memory itself could be a useful deterrent for

misbehavior and carelessness, for humans and machines alike. But it also means that where there is a trust imbalance (usually in the periphery of the blockchain, in the coupling with the off-chain systems that support it) there are opportunities for either trust disintermediation or arbitrage, and possibly, value creation. Moving forward, this combination of awareness of irreversibility, value by memory, and reasoning about introspection, perhaps implemented using non-ergodic variants of cultural genetic algorithms,²² could allow machines to navigate the world using the same fundamental device that evolution has provided to humans: trust. And ultimately, the question is not if we should trust AIs, but rather how AIs will trust us.

References

1. Kyburg, H. E. & Pearl, J. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. *The Journal of Philosophy* **88**, 434 (1991). URL <https://doi.org/10.2307%2F2026705>.
2. Wölfer, R., Cortina, K. S. & Baumert, J. Embeddedness and empathy: How the social network shapes adolescents' social understanding. *Journal of Adolescence* **35**, 1295–1305 (2012). URL <https://doi.org/10.1016%2Fj.adolescence.2012.04.015>.
3. Liu, Y.-Y., Nacher, J. C., Ochiai, T., Martino, M. & Altshuler, Y. Prospect Theory for Online Financial Trading. *PLoS ONE* **9**, e109458 (2014). URL <https://doi.org/10.1371%2Fjournal.pone.0109458>.
4. Engelbart, D. C. Toward augmenting the human intellect and boosting our collective IQ. *Communications of the ACM* **38**, 30–32 (1995). URL <https://doi.org/10.1145%2F208344.208352>.
5. Fareri, D., Chang, L. & Delgado, M. Computational substrates of social value in interpersonal collaboration. *J Neurosci* **35**, 8170–80 (2015).
6. Venegas, P. Trust Asymmetry. URL <https://doi.org/10.22541%2Fau.151979448.82088697>.
7. Taleb, N. N. & Douady, R. Mathematical definition mapping, and detection of (anti)fragility. *Quantitative Finance* **13**, 1677–1689 (2013). URL <https://doi.org/10.1080%2F14697688.2013.800219>.
8. Blankenship, J. *Forging Blockchains: Spatial Production and Political Economy of Decentralized Cryptocurrency Code Spaces*. Master's thesis, University of South Florida (2017).
9. Foreword: Coase and the Theory of the Firm. *Managerial and Decision Economics* **36**, 1–1 (2014). URL <https://doi.org/10.1002%2Fmde.2700>.
10. Prigogine, I., Stengers, I. & Pagels, H. R. Order out of Chaos. *Physics Today* **38**, 97–99 (1985). URL <https://doi.org/10.1063%2F1.2813716>.
11. Menezes, T. & Roth, C. Symbolic regression of generative network models. *Scientific Reports* **4** (2014). URL <https://doi.org/10.1038%2Fsrep06284>.
12. Venegas, P. On the sources of systemic risk in cryptocurrency markets. URL <https://doi.org/10.22541%2Fau.152074266.61910113>.
13. el Alaoui, A. O., Dewandaru, G., Rosly, S. A. & Masih, M. Linkages and co-movement between international stock market returns: Case of Dow Jones Islamic Dubai Financial Market index. *Journal of International Financial Markets Institutions and Money* **36**, 53–70 (2015). URL <https://doi.org/10.1016%2Fj.intfin.2014.12.004>.
14. Nagayev, R., Disli, M., Inghelbrecht, K. & Ng, A. On the dynamic links between commodities and Islamic equity. *Energy Economics* **58**, 125–140 (2016). URL <https://doi.org/10.1016%2Fj.eneco.2016.06.011>.
15. Auinger, F. VIX Index. In *The Causal Relationship between the S&P 500 and the VIX Index*, 37–52 (Springer Fachmedien Wiesbaden, 2015). URL https://doi.org/10.1007%2F978-3-658-08969-6_6.
16. Brodersen, K. H., Gallusser, F., Koehler, J., Remy, N. & Scott, S. L. Inferring causal impact using Bayesian structural time-series models. *The Annals of Applied Statistics* **9**, 247–274 (2015). URL <https://doi.org/10.1214%2F14-aos788>.
17. Vladislavleva, E., Smits, G. & Kotanchek, M. Computational Intelligence in Industrial Applications. In *Springer Handbook of Computational Intelligence*, 1143–1157 (Springer Berlin Heidelberg, 2015). URL https://doi.org/10.1007%2F978-3-662-43505-2_57.
18. Vladislavleva, E., Smits, G. & Kotanchek, M. Computational Intelligence in Industrial Applications. In *Springer Handbook of Computational Intelligence*, 1143–1157 (Springer Berlin Heidelberg, 2015). URL https://doi.org/10.1007%2F978-3-662-43505-2_57.
19. Lawyer, G. Understanding the influence of all nodes in a network. *Scientific Reports* **5** (2015). URL <https://doi.org/10.1038%2Fsrep08665>.
20. Čížinská, R., Krabec, T. & Venegas, P. FieldsRank: The Network Value of the Firm. *International Advances in Economic Research* **22**, 461–463 (2016). URL <https://doi.org/10.1007%2Fs11294-016-9604-x>.
21. Rao, V. Blockchains Never Forget. <https://www.ribbonfarm.com/2017/05/25/blockchains-never-forget/>. URL <https://www.ribbonfarm.com/2017/05/25/blockchains-never-forget/>. Accessed on Mon, May 28, 2018.
22. Reynolds, R. & Liu, D. Multi-objective cultural algorithms. In *2011 IEEE Congress of Evolutionary Computation (CEC)* (IEEE, 2011). URL <https://doi.org/10.1109%2Fcec.2011.5949757>.