Trustless crypto-markets: perceptions of Value, Risk and Cost

Dr. Tomas Krabec, PhD, MBA (Skoda Auto University, Prague)
krabec@is.savs.cz

Ing. Percy Venegas, ME, MBA (Economy Monitor, Costa Rica)
v.percy@economymonitor.com

Introduction

By 2025, 10% of global GDP to be stored on Blockchains [World Economic Forum]. Asset classes: crypto currencies (Bitcoin, Ethereum) and instruments built on public/private decentralized ledgers secured by cryptography (sidechains). *"Trust minimized cash flows" [Miller, Szabo]*: in a decentralized system that executes transactions and contracts, in theory, trust is not needed. *Smart contracts:* blockchain-based programs that can establish and enforce fiduciary relations between parties. Auditable by parties and regulators. *"The DAO", a Decentralised Autonomous Corporation:* first decentralised investment fund conceived to finance proposals on other decentralised applications, or Dapps. Listed by default. Largest crowd-funding event in history (and an attack target due to a flaw in code logic- a shareholder moved funds deceiving balance checks): $200M raised in 1st month, +$50M compromised 3 weeks after (for comparison, Bangladesh central bank had $81M stolen due to the SWIFT exploit). Unwound 2 months after launching, effectively creating 2 competing cryptocurrencies with different mining profitability, hashing capacity and price. *Crypto tokens as bearer shares:* exposure from intrinsic cost factors and governance structure. But what about trust on smart contract design, the code (law) itself? And, even if a "replicated, shared ledger" [Gendal] offers full code and transactional visibility, are there any risk signals/market preferences encoded in other value flows?

Irrational exuberance?
"The DAO" (top) and Ethereum (bottom) market capitalizations. Source: CoinMarketCap

Methods

Value. The fair value of the coin [Blundell] as the present discounted value of the variable mining cost with a probability p of a fatal risk event in any period. Using a n-year horizon,

$$PV = (1-p_1)(M+\varepsilon_1)d_1 + p_1(1-p_2)(M+\varepsilon_2)d_2 + \cdots + p_1p_2 \ldots p_{n-1}(1-p_n)(M+\varepsilon_n)d_n$$

Where: $d_i = 1/(1+r)^i$
r is the riskless bond rate and i=1...n
M reflects the (constant) electricity, hardware time and human capital cost of mining a Bitcoin, and ε is a random add-on to that cost depending on the degree of difficulty of the algorithm at the time, random 'luck' and other one-off factors.

Cost. Equilibrium fair cost of proof of work per block, for Bitcoin [Aste],

$$equilibrium\ fair\ cost\ of\ proof\ of\ work\ per\ block = \frac{duplicated\ fraction\ of\ the\ value\ of\ a\ block}{number\ of\ blocks\ required\ for\ settlement}$$

Risk. We use financial signal processing to study volatility (envelope analysis) and intensity (power spectra); network correlations expressed in graph form for asset correlations, and vector fields to map flows. We compare assets at a similar level of complexity using a simplified form of *FieldsRank* [Venegas, Krabec and Cizinska], an information theoretical value measure modeled after Lawyer's Expected Force Network Centrality; given a set of traffic value probabilities p_i, the absolute information entropy is taken to be,

$$FR_{IN} = -\sum p_i \log(p_i)$$

Results

Data: We sampled a portfolio of decentralised applications (Dapps) from the system that was set up by The DAO fund to deliberate on financing proposals [dao.consider.it]; we focused specifically in the category "Proposals working toward a smart contract". The proposals data included age (since publication, in days), number of opinions, and score, which are taken as quality signals. We augmented the dataset with records from the State of the Dapps project [dapps.ethercasts.com], which provides Dapp name, description, website URL address, GitHub URL page, Reddit URL address, responsible team/organization, category and project status. We used the presence of a Reddit, Github and Website addresses as an indication of project maturity (Reddit is a social network frequented by programmers and a preferred discussion forum to vet the viability of software project ideas, and is usually used together with Github, a code repository popular among the open software community). We then obtained timeseries data for incoming web traffic (total visits worldwide and average time on site, desktop and mobile, from February to July 2016) from a panel of 200 million internet users, internet service providers and click stream data providers [Similar Group Ltd, Searchmetrics GmbH].

Correlation graph. We applied the method of portfolio diversification with graph theory by Chen, using Wolfram Mathematica. The correlations during the one-month period just before The DAO attack and similarities in information content of incoming flows (FR_{IN}) provide the initial subjects for study: Security_A, an internet-of-things startup with strong interests in The DAO community (core code contributors), and, Security_B, presented in the investment proposal as a The DAO alternative, already operational. By the principle of portfolio diversification, the assets must be as uncorrelated as possible to reduce risks due to attention/attention price fluctuations.

Attention pricing. To factor attention pricing into the decision making process (essentially, a minimum cost flow problem) we use the inverse proportionality between engagement investment (using average time on site) and attention price; this follows Herbert Simon's Attention Economics. The expected returns of each proposal per year: project A USD $4,4M, project B USD ~$3M; note how despite larger expected gains, the market seems to favor the asset less correlated to the success of The DAO itself –specially during the uncertainty period between the attack, community deliberation, and the hard fork (effective bail out of The DAO).

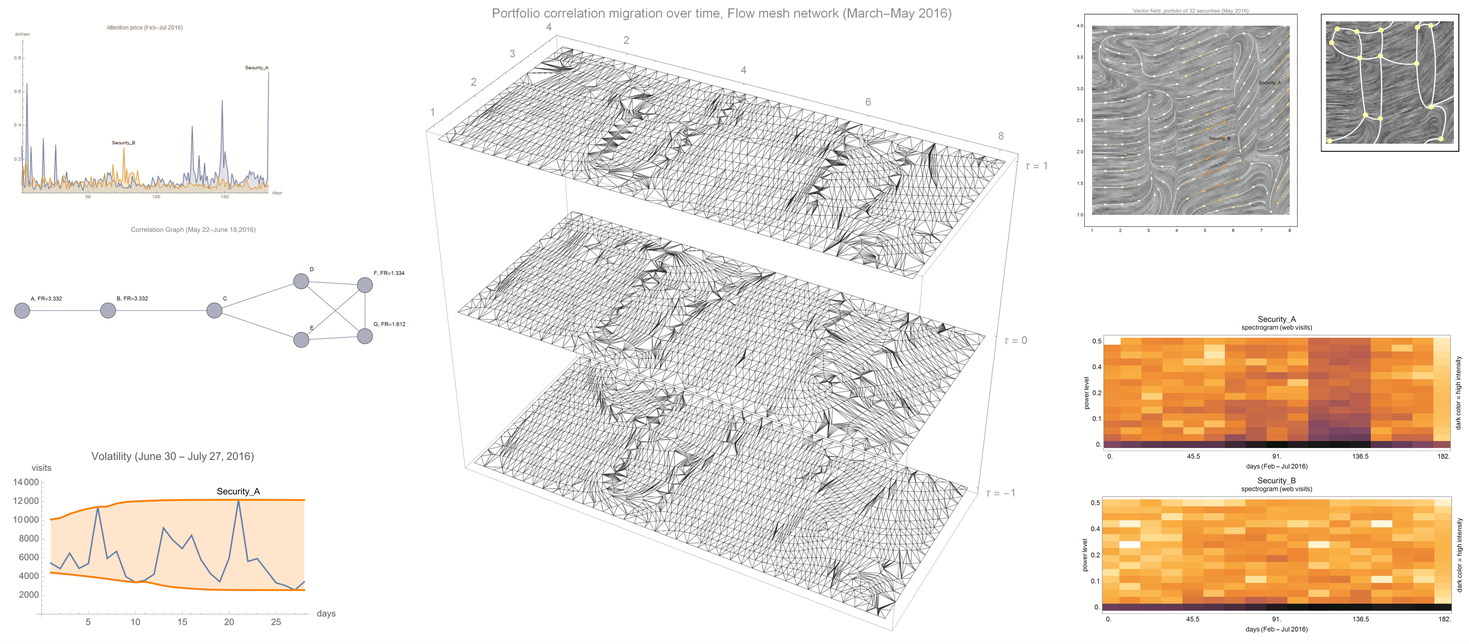
Spectrogram. Unlike (deterministic) blockchain data, the web traffic signals are always estimates with differences among providers; the spectra (plot of the magnitude of discrete Fourier transforms of partitions of the signal) helps identifying a (data acquisition agnostic) "fingerprint" that allows to recognize the asset despite those variations. This frequency domain analysis of site visits facilitates recognizing the patterns: Security_A presents high fluctuations during the attack crisis, Security_B is again more steady.

Volatility. To measure how well intrinsic value stays relatively stable, we use the SNIP (statistics-sensitive nonlinear iterative peak-clipping) envelope estimation method; we look into Security_A, the scaling factor σ=2 (above zero) validates the spectra observation.

Vector field. We expand our portfolio to 32 assets by creating a grid and sequentially seeding a vector to each point; other mappings may be used to represent any desired topological analogy. In the early stages of a listing, word of mouth in social networks and the ability to generate buzz in media sites are the highest traffic contributors, therefore the convention for the vector components is {referrals, social}. The resulting vector field gives rise to a flow. In the portrait of the system (flow dynamics) during the high growth period that preceded the attack, streamlines represent flow direction and color gradient represents intensity (number of visitors); Securities A and B are again found as strong performers. This helps identify singularities in the portfolio (i.e groups that tend to move in sync or not) such as nodes (sources or saddles), stable focus (spiral sink), stable centers; also, false positives: we found potentially misleading rankings, where proposals with high score and vote count showed no actual signs of demand.

Feature-based data analysis (network detail). The topology of the velocity field of a flow can be seen as a condensed representation of the streamlines and may therefore serve as a skeletal, simplified representation of the flow [Weinkauf]. By identifying sectors of different flow behavior it might be possible to embed robust control [Sargent, Hansen] to deal with uncertainty in portfolio selection.

Mesh network. The progression in portfolio positions is now depicted using a network form (May is the top layer, same as the previous vector field that was rendered using Line Integral Convolution; the other layers show the buildup period since March). Clusters in this "fabric" of *value flows* reveal a mixture of "hidden market trends". There is a visible breakout (points of information entropy gain/loss) towards a new equilibrium on April (τ=o), but still Security_B remains among the most stable assets in the portfolio.



Conclusions

A *Trustlessness premium*. In Blockchains "the cost is a security measure" [Aste]; high cost (for miners) and high probability of fatal risk have a material effect on value. Even in a programmatic setting, investors are forced to trust in the design (Code is Law), and human governance structures. Exposure increases in cryptoassets (smart contracts have larger attack surfaces than cryptocurrencies)– but when the attacker is a shareholder/stakeholder and not an external actor, the attack vector is "people not being able to create 100% perfect contracts" [Gertis]. The *full cost of being trustless* should be factored in.

***Attention economics* and the *Fields* approach.** Trading (Exchanges) data and voting (Fund) mechanisms can not reflect all changes on risk profile of decentralised applications; in the period of uncertainty while the Dapp is pursuing funding, it is useful to use "the market as a voting machine" [Graham]. The value web and the web of information are intertwined: Micropayments sidechains assign a transaction price to "calls" on URLs (a channel keeps fees low to users); in such marketplaces, *traffic flows are, literally, cashflows*.

Vector fields are scalable, fit to analyze arbitrarily high numbers of securities (critical since in the internet-of-things every device can run a smart contract, and "a wealth of information creates a poverty of attention" [Simon]). Flows, and their morphological network components' possible areas of research: Machine learning (pathfinding optimization), Watermarking [Kiyavash] and steganography (e.g LIC as substrate to encode data to be handled outside of the blockchain), non-planar topologies [Aste, Di Matteo, et al], and to adapt state of the art algorithms such SinkRank [Cook, Soramäki] for Dapp portfolio selection (e.g decentralised networks are robust by design, investor's control of exposure is not: similarly as people irrationally undervalue cryptoassets due to their rapid appreciation and underestimate the risk of investment [du Rose], in the presence of uncertainty they can fail to diversify their cryptoassets investments by treating smart contracts as simple apps). *"Navigational" financial cartography reveals the uncertainty portrait.*

Literature cited

Aste, Tomaso, The Fair Cost of Bitcoin Proof of Work (June 27, 2016). http://ssrn.com/abstract=2801048

Blundell-Wignall, A. 2014. "The Bitcoin Question: Currency versus Trust-less Transfer Technology", OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing.

Chen, Samuel. Portfolio Diversification with Graph Theory. 2012. A Wolfram Research resource.

Good, Gavin. 2014. Ethereum: a secure decentralised generalised transaction ledger (yellowpaper). http://gavwood.com/Paper.pdf

Venegas, Krabec and Cizinska. 2016. FieldsRank: The network value of the firm. *International Advances in Economic Research, International Atlantic Economic Society*.

World Economic Forum. 2015. *Deep Shift Technology Tipping Points and Societal Impact*.

Acknowledgments

Thanks to the discussants at the Cambridge Centre for Risk Studies Seminars.

"…although we usually assume there is a sharp line of distinction between what is money and what is not-and the law generally tries to make such a distinction- so far as the causal effects of monetary events are concerned, there is no such clear difference. 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" F.A Hayek