TEXT AUTHOR
Drago Indjić, SBI Advisory Board Member
PROFESSIONAL INVESTMENT MANAGEMENT - HEDGE FUNDS

Funds, forks and folk on my crypto journey

It is a privilege to be invited to contribute to the SBI blog. My 1,500 words are personal, carrying significant prejudice reflecting computer science as an on-going hobby and skillset over many years. Many technological (or algorithmic) developments feel as exciting today as in the distant past, but luckily I can now rely on a wealth of experience resulting from a non-stop adaptation to changes in the tech ecosystem.

Let me start with a short summary of my biased framework of mind. *There is no magic*. No technological disruption can jumpstart a single nation; nor heal the old scars of socialist and post-socialist transition in countries of "emerging" Europe. Furthermore, social-economic disruptions damaging markets and capital formation are path-dependent. The momentum is persistent and the effects are cross-generational[1]. In addition, the goal of long-term wealth preservation (for individual retirement or future generations) is almost surely outsourced - contracted and delegated - to investment management firms offering arguably an unlimited choice of investment products and services. Paradoxically, the investment industry simultaneously features global inputs and highly parochial outputs and product distribution. The industry remains strictly regulated yet highly lucrative, which isn't really such a contradiction in terms for the lucky few who gain critical mass.

As a first illustration of investment industry demand and supply, consider choosing one or more of only 13 retirement investment funds in Serbia and an average holding of about ¼ BTC per future retiree[2]. The statistics themselves create a lot of food for thought (and even more to be desired). For the second illustration - not to promote and solicit any investment - take a case of a small investment company born and bred in Prague several years ago. Perhaps due to unusual location, it was not easily exportable (in contrast to a 50% increase in the number of Škoda cars sold over the last decade in the EU). It took two years to restructure the fund as an alternative investment vehicle in accordance with the European regulation to make it acceptable and accessible across the EU.

Today it is a small three-month-old "baby" resident in Amsterdam and facing a bright future. The portfolio managers speak various Slavic languages, share common values and pursue a quantitative approach to investments. Naturally, exploring new investment opportunities

---

[1] https://en.wikipedia.org/wiki/Belgrade_Stock_Exchange. The national Assembly adopted the Stock Exchange Law on 3. November 1886, and the Law was proclaimed by the then King of Serbia Milan M. Obrenović.
[2] https://www.nbs.rs/internet/latinica/62/62_2/dpf_04_17.pdf, p. 12, cca 2000 EUR expressed in BTC as at end of April.

makes good business sense and one of them is to join forces with a team of crypto practitioners to attempt to launch an EU-domiciled crypto investment fund.

I happen to be the most grey haired executive team member - Chairman. This is a hands-on role and I ought to be fully prepared to act on all current and future business and regulatory challenges. In particular, I should adopt strong governance - also known as fiduciary perspective - protecting the end investors.

So from where should I take my deep dive into the latest crypto fashion? Londoners get accustomed (or rather spoiled) by a never-ending stream of events, often designed to appeal to non-Londoners. In anything related to money, central Mayfair area venues are usually emphasised. On the other hand, BlockSplit.io would have been far more fun as their 87-strong Telegram channel indicates exactly as I am typing this blog on a dull, rainy Saturday morning[3]. Regrettably, a "business" trip to any Mediterranean destination is somewhat difficult to justify from (any) investment fund expense account. (That ship sailed long ago.) I am more than happy to cover the topic of investment fund fees and charges in depth in another blog (ideally featuring Ms Gina Miller better known for another timely topic related to the United Kingdom).

Spoiler: there is no a single price chart or ICO. I am very sorry. If you are after these, feel free to stop reading right now and please share your experience from another event.

Luckily, there is always an IEEE or similar professional society event. I am happy with simple, less hyped red-brick academic surroundings such as University College London, ordinary filter coffee in paper cups and biscuits (shout out to Hyperledger and Linux Foundation) and ("u inat") cannot be intimidated by either ladies (Sarah Meiklejohn) or gentleman with PhDs in cryptology. Hence, last Monday's **IEEE Security and Privacy on the Blockchain Workshop** made so much business sense: virtually no travel expenses and a mere €100 registration fee (even cheaper for students). Only about 40 people turned out (and even less tweeted #IEEESB2018), making the networking experience and personal contacts great. All presentations have been made available on http://ieee-sb2018.cs.ucl.ac.uk/#schedule.

My favourite takeaways from the event are:

(i) private coins and the privacy-preserving protocols,
(ii) improving security and resilience to the adversaries (ASICs, selfish mining, Sybil attacks etc),
(iii) governance challenges, or simply Prof. Bryan Ford (EPFL) himself.

Monero has been referenced in several presentations. It is inspiring to see that Kevin Lee (UIUC) and other academics reporting rather than choosing to exploit vulnerabilities in present protocols such as Ring Confidential Transactions (RingCT; akin to CryptoNote). Lee has reviewed distinct types of attacks and defences and proposed an end-client algorithm improvement using an authenticated data structure with low complexity (O(logN), fast) that

[3] "Trust me" with my timestamps, or think about incorporating https://github.com/petertodd/timelock

will identify malicious (lying) server nodes whilst avoiding the necessity of yet another hardfork[4].

It was also instructive to learn about the size of snapshots of various chains (for Monero only 40 GB, but nevertheless these are always demanding file sizes at an operating system level).

In the same spirit, Alishah Chator (JHU) analysed RingCT in practice: the privacy can be high, but the required data size can make the implementation memory-heavy and ultimately impractical. Note that unlike Monero and ByteCoin, Zerocash and Zerocoin feature the constant size. Chator proposed that future Monero transactions *sample* the transaction index (Tx) space, thereby keeping the cover set description size at reasonable size (~100kB for covering 100k Txs, i.e. not growing linearly). From a classical electrical engineering perspective, it was intriguing to think about "sampling" in a crypto context and glance over derivation of a Recoverable Sampling Scheme (RSS) based on polynomials, making it independent of the size of Tx. The cover set descriptions will dominate size costs in Monero and similar private coins and RSS can keep the costs manageable while preserving anonymity.

The private coins were referenced in other presentations: "zk" (Zero- Knowledge) acronym kept popping out in relations not just to Zcash but also emerging problems: Oded Leiba (Ben-Gurion) addressed the problem of trusted decentralised distribution of software patches to IoT devices (note how many we will eventually need to deploy; currently pushed through cloud providers and hence representing a single point of failure). Here the incentives for the fair exchange of updates are resolved as smart contracts (Hashed Time-Locked; Zero-Knowledge Contingent Payments) and an ingenious deployment of zk-SNARKs on top of Ethereum and torrents.

Regarding the topic of security (ii), Ritz (TU Munich) decided to model "selfish" miners that deviate from the protocol, are not affected by network lags and that may operate a large fraction of mining power to build a secret blockchain fork, observes a honest network that nearly catches up and then publishes his fork, making honest miners lose a block. Ritz has shown that Ethereum running the latest of seven (no less) hard forks in March had 16% stale blocks (15 seconds block time) and in simulations observing various mining revenue and security performance metrics discovered that at 24% of stale blocks, a selfish miner needs 18% of hashpower to be profitable and just 34% to achieve control. The selfish mining can be further optimised to achieve even lower thresholds - and ETH is defenceless against it. On the other hand, Shayan Eskandari (Concordia) in his talk contrasted Bitcoin's PoW net hashrate of ~30 Eh/s to Monero's ~500 Mh and to various options for decentralised mining (including Coinhive and the overhyped cryptojacking that is shown not to be profitable at all - yet aspiring malicious miners keep trying to obfuscate IP addresses to bypass the blacklists).

The best content was related to governance (iii): Prof. Ford's (EPFL) keynote speech on fairness and decentralisation. On the technical side, his group's ByzCoin demonstrated 700+

[4] Yet by sheer coincidence, fork countdown, two more days: https://monerov.org/

tps performance (at PayPal level, 100x faster than BTC) with permanent commitment in seconds; recently developed OmniLedger achieved 6k tps (Visa network performance) by addressing the horizontal scaling problem (i.e. each miner or validator should replicate all state and verify all Tx: each stores all of ever-growing history and adding nodes does not increase capacity) through “sharding”.

There was much more to come in terms of fairness and governance and achieving a noble goal of democratic decentralisation in systems. For example, BTC membership is described as analogous and unnecessary as any fraternity hazing ritual (“now form a new block”) and BTC power is wasted as well as being highly unevenly distributed (e.g. 60% in China). The alternatives exist (permissioned ledgers, PoS and tools from RandHerd, Chainiac) and soon we reach the analysis of a very concept of democracy, “one person, one vote” principle exemplified in the “Proof-of-Personhood” proposal. These advanced concepts are attempting to mix privacy with accountability (explored in Zcash, zkLedger) and shown to eventually hit grand societal challenges with discussion of the Universal (Permissionless) Basic Income (!).

Two other presentations were amusing but lacked a fundamental research flavour: one by practitioners on distributed identities (verifiable claims, Sovrin) and the last one, on challenges in offering Blockchain-as-a-Service (Hyperledger, Coco).

It was enjoyable to participate in an event touching not only deep theory behind contemporary open problems but also ethical issues with serious implications, very rarely discussed in similar forums. I am looking forward to enjoying more IEEE events, obtaining my IEEE Life Member status (in only 7 years) and passing many white-hot technical torches to a youthful SBI community!

Drago Indjic

May 2018