INPUT | OUTPUT

IOHK | BLOG

A trip to Malta and a Grothendieck milestone

APRIL 18, 2017 4 MIN READ

Last Monday should have been particularly jarring given the recent excitement.

However, it was anything but. Sunlight was flooding the back garden and all the small birds of the neighborhood came together to perform an impromptu concert at maximum volume. I could hear them clearly through the double glazing. Spring had sprung in Dublin. And I'd just come back from Malta talking Ethereum, Cardano, blockchain, crypto, functional languages, goal management and a ton of other cool stuff. Life is good.

It was my first time attending the Financial Cryptography and Data Security conference. The conference is a week-long annual event for cryptography as applied to finance. This year, IOHK's chief scientist Aggelos Kiayias put a great programme of speakers together. Instantly recognizable figures from the crypto community attended – Adam Back, Emin Gün Sirer, Vitalik Buterin and many more. IOHK researchers attended and it was great to see people who may only know each other through twitter feeds and published papers get to speak to each other.

I hope and presume this conference has generated many fine and detailed articles on Coindesk and beyond. This won't be one of them. Particular highlights for me were listening to MIT professor and cryptography pioneer Silvio Micali speak about the Algorand protocol and the conscious decision to keep incentives out of the equation. That instantly generated a little controversy and is going to need a long second look.

Dmitry Meshkov, IOHK researcher, presented Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies which is of particular interest to Team Grothendieck as we have wrestled with our implementation of the "Modified Merkle Patricia Trie" as specified in the original yellow paper. In all its forms it's a clever idea – being able to move forward and back through the state by memorizing a root hash and being able to show tries are equivalent based on the equivalence of their root hashes. Dmitry et al have a scala implementation, and if I heard Vitalik Buterin correctly (he commented after the presentation) he suggested there might be room for improvement on the original implementation, so there are possibilities for enhancements there.

The conference was good, but it had some stiff competition from all the fun I had and everything I learned from mixing with other IOHK employees. IOHK employees usually work remotely but for more than a week almost 40 people gathered in Malta, who had traveled from far flung places like Osaka, St. Petersburg and California, including IOHK founders Jeremy Wood and Charles Hoskinson. While that week was mostly about the conference it was also an opportunity to get some work done. On the top floor of some very nice rented office space, the Serokell and Daedalus teams along with other key personnel on the Cardano project hammered out plans and approaches to give said project a major push forward. There was time for some introspection too and a lot of productive meetings around development methodology.

A real highlight of working for this company is tripping across experts in many technical fields – functional languages, formal verification, full-time life time cryptographers, language designers and creators, high energy physicists… High energy physicists. Who tell jokes.

And it gets better. The previous week, the week of the 27th of March, Team Grothendieck arrived in Athens to work on our next and arguably most important milestone – "Transaction Execution" or "tx execution" for short. This was the first time the whole team came together to work, physically together and in same time zone.

The team reached its first milestone on Friday 24th March. That milestone involved downloading all blocks to the local machine and providing those blocks to other clients, further dispersing the transactions across the peer-to-peer network. The client also supports "fast download", which is the process of downloading the state trie from a point in recent history in order to shorten the time required for a client to get fully up to date with the blockchain. The premise being that downloading the state trie is faster than executing every transaction since block 0. As our first milestone it was very exciting to reach, but also to see the blocks and transactions flying around the network and know that we can successfully synchronize our local database with the rest of the Ethereum Classic network.

We had a productive few days at the university of Athens, the area is quiet, cool in the shade and conducive to working. The sun shone, the wind blew and the coffee was good. Our hotel was close to the university so we got to walk the streets of Athens in the mornings and see a little of daily life in the city. The subject of our days in Athens (transaction execution) is the process of updating the ledger by applying valid transactions to it block by block. After each block of transactions has been applied to the ledger the ledger exhibits a new state. This state is stored in the form of a state trie and the root of this trie is a hash reflecting precisely the contents of the state trie. The questions we had to answer were – did we understand the goal; did we understand how we measure success; did we have the functionality covered by existing tasks; how long would it take and finally some knowledge swapping as working apart inevitably means small knowledge silos had begun to develop despite our efforts. By Thursday evening we had satisfactorily answered all these questions and we expect to reach the tx execution milestone by the end of April.

On the Friday the team attended the Smart Contracts conference and spoke with Charles Hoskinson, Prof Aggelos Kiayias, Darryl McAdams and others about the future of smart contracts and the law.

There was tentative agreement on the eventuality of smart contract template libraries, so if for example the author wanted to provide an upgrade path for the contract in the event of some issue being found (ahem!) or have some means of dissolving/locking the contract if the participants lose faith, a tried and trusted set of templates would exist for the contract author to mix and match. Templates of this type could claim regulatory compliance out of the box, which is a great (if not new) way to leverage the usefulness of software in the world of contract law – solve a problem once and reuse the solution ad nauseam. I suspect this is an area most smart contract developers currently enjoy ignoring!

A final word on Athens, the Acropolis museum is a wonderful building and worth a visit even if they housed nothing there, but coupled with the treasures of the ancient world and a good restaurant it's a must-see if you find yourself in the area.

Here's hoping the end of April sees us reach another exciting milestone, an even bigger one this time, and we are able to execute every transaction in the blockchain using the Grothendieck client. That would really give the birds something to sing about…