INPUT | OUTPUT

IOHK | BLOG

HOSKUS PARVUM OPUS: A BRIEF SOJOURN BACK TO ETHEREUM

AUGUST 02, 2016 CHARLES HOSKINSON 14 MIN READ

Heart of Darkness

We must never cease from exploration and at the end of all of our exploring will be to arrive at where we started and know the place for the first time. This quote from T.S. Elliot has become increasingly more meaningful to me over the last few years. I've had an opportunity to travel to 15 countries, more than 500,000 miles and meet thousands of amazing people, yet I feel as if I've returned to where I started with a new perspective.

First, I suppose it's prudent to start with the early days of my journey. Quite painfully, I recall June of 2014. I had pneumonia and had just left Switzerland after a brutal fight over the future of the Ethereum project. I was on the losing side and now was headed to England to spend a few days with Michael Parsons, who was generous enough to provide a room in his house while I collected my thoughts about my future. I was in shock from being stripped of an identity.

Just a few days prior, I was a founder of a remarkable project with a beautiful vision of a decentralized world computer that was immune to censorship alongside the machinations of inconvenienced power brokers. And then I had become a sickly man having trouble breathing, traveling through an overcast city to a small house without a title, purpose or any vesting in a movement. It was a dark time, bereft of humanity or kindness save a few rare friends and my Marlene for whom I'm eternally indebted.

The following months were left with a great degree of uncertainty. I pondered returning to mathematics and picking up where I left off studying the great unsolved problems of additive number theory (See Nathanson's excellent two part series on the topic.) I received several offers to lead a new ventures- some with VC backing and good teams. Yet honestly my heart wasn't in the game anymore.

Ethereum Rising

I really loved the amazing promise that Ethereum presented and to watch it unfold from the sidelines without stake or the ability to contribute was just too much. I invested so much time sleeping on floors, flying around the world and fighting almost constant exhaustion trying to keep everything together despite deep philosophical divisions in the team and vision. I had to detach and do other things.

While I had my grievances with the remaining founders, there was great solace in the project maintaining the original social contract. And despite my admittedly bitter criticisms about governance and the use of funds, this contract seemed to be immutable. Gavin invented new words to encapsulate the code is law mantra, and Vitalik would appear on a nearly weekly basis in some form of media extolling the need for a censorship resistance smart contract system.

The world was surprisingly receptive to the vision. Ethereum grew like a weed both in mindshare and market capitalization. It was incredibly satisfying to see every doubter reassess their prior comments, forgetting old stings and trying to eschew the hard line for a more neutral tone. It's amazing how prognostications of impending doom and gloom transform into praise when people start making money. Readers with an overabundance of time should refer to Jeff Garzik's tweets.

Bad Decisions

It's a pointless exercise to litigate the sins of Ethereum's governance in a blog post nor justify my latent bitterness in a sharply written argument. Nothing productive can be gained from this effort outside of reinforcing notions people already have. Rather it should be stated that the core of Ethereum has become badly compromised by an extremely poor decision.

The Ethereum protocol doesn't care about Charles Hoskinson. It doesn't care about Gatecoin or Bitfinex. It doesn't care about the IRS, the SEC or the government of China. This lack of concern is the value proposition's apex. Ethereum is a horribly inefficient computer that is perhaps the most expensive ever built relative to its peers. The reason we pay that price is because we want a guarantee of computational apathy.

The leadership of the ethereum project have made a decision to fork the protocol to eliminate the social contract of computational apathy. This fork is not about returning stolen money. It's not about protecting the interests of the Foundation from a legal or regulatory perspective. It's simply about changing the code is law paradigm to code is usually law until it's not.

There was another option. I recall when Bitcoin has to make sudden changes to avoid a bug that allowed for the creation of billions of new coins. Issues that are clear flaws in the protocol's design that break the intended social contract are non-controversial to fix. I don't believe there are many in the ETC community who would object to correcting a flaw in the EVM that suddenly creates billions of new ether. It's the changes to the social contract that are hazardous and always result in a community split.

For these changes, there needs to be a commitment made by the holders of the token to embrace the new system. Proof of burn is a perfect mechanism to accomplish this task. With ethereum, it could have been taken to the new level. An assurance proof of burn smart contract could have been written to pool ether holders wanting to embrace the new system if there was a certain threshold of participation (say 51 percent). If the threshold wasn't reached within a time limit, then the participants get refunded. Otherwise, the contract executes and all the funds are burnt leaving a clean cryptographic proof to redeem tokens on a new chain. DAO holders could have been given a special purpose token excluding the thief.

The purity of this approach creates universal consent amongst the participants in the new system with the new social contract. A vacuous vote with no stake at risk is not consensus- especially when there is around 10 percent participation. Instead it seems to be a failed attempt to manufacture a democratic mandate to do something the core developers already wanted to do. It appears they didn't want two chains to co-exist so

they forced the issue.

I did not sign up for the paradigm of code is sometimes law. It makes absolutely no sense to me. Why waste millions of dollars in energy and run such an inefficient computer if it's not going to provide hard guarantees of fidelity? Why shouldn't I just run code on a federation of servers with carefully chosen trust pairings? Why shouldn't I just play the jurisdiction game and trust my code to neutral and stable states like Switzerland? Such places usually have the moral high ground of a democratic mandate and known conflicts of interest unlike the current leadership of Ethereum.

Obviously the existence of Ethereum Classic seems to convey that I'm not alone in my protest and disgust for the fork. There are thousands of very angry miners, developers, and stakeholders who did not support the actions the foundation took and are directly expressing their rage via supporting the original codebase.

While this aggregation is powerful and clearly deserves a re-evaluation of the decisions of the last few weeks, it's not a cohesive, productive ecosystem with a vision, a roadmap and the ability to execute. It's effectively the cryptocurrency equivalent of a recall election. People made a choice to fire the prime minister, but they didn't select a new one.

Return to the Center

This brings me back to my return to Ethereum. 2014 was a very long time ago for me. I've grown a lot as a person. I lead new company with nearly 30 employees to worry about. We are engaged in thoroughly interesting work ranging from the formalization of proof of stake, complete with security proofs based on the GKL15 model (publishing soon!), to studying governance at its most elemental level.

I have no desire to abandon our current projects and my personal obligations to attempt to force a Vitalik versus Charles showdown. A vanity play would accomplish nothing, and the market itself is a far better distributor of karma than any man could ever hope. There isn't an ether white whale for me to slay.

My Participation in Ethereum Classic

Thus it is my burden to explicitly state how I would like to contribute to the ETC community alongside what I won't do. First, I will not seek a leadership position. It is needlessly divisive to inject myself into this movement with the aim of being the ETC CEO or some other kind of power broker. Nothing good can come from the distraction, and there are better people to lead. Second, I will not promote a roadmap that enforces a zero sum game between ETH and ETC. They are now projects governed by different philosophies and different communities. They shouldn't conflict in principle. Third, I will not support an effort to centralize the project around a new foundation. Centralization of power is the entire reason we are in this mess.

Now on to the things I will do. As I previously mentioned, ETC is currently unified in anger and resentment. There are many groups of people in the ETC community and they will eventually conflict with each other after the dust has settled. Also a fairly large amount of trading volume into ETC has come from the bitcoin space. It's unclear if this community is going to solidify behind a stable vision and roadmap outside of the code is law paradigm, which is admittedly an extension of bitcoin's honey badger approach to transactions.

Abstracting the point to something productive, I think it's reasonable to explicitly state the social contract of ETC and make a commitment that it will not change. Bit Novosti drafted a manifesto that seems to be the current ideological driver of ETC.

Therefore my first goal is to unify a fairly strong majority behind the basic tenets of immutability, irreversibility and openness. My hope is to transmute the anger into a productive movement unified behind some basic goals like Bitcoin enjoys. I fully admit this might not be possible and some hard choices may have to be made; however, I'm optimistic we can pull together into a cohesive movement.

Second, from a roadmap perspective, ETC needs to decide whether it will stay connected to ETH or diverge. I strongly argue that divergence is necessary as it's logically inconsistent to reject the Foundation's judgement, yet still accept their vision for the project. While obvious improvements, bug fixes and optimizations of things like the EVM should be capitalized on, ETC should chart its own path.

The most immediate concern is the proof of stake transition. I believe that the transition to Casper will not be straightforward. Rather, difficulty will likely be experienced due to the ad hoc methodology of Casper's design and the inexperience of its architects.

Designing new consensus algorithms is among the most challenging tasks in computer science, as illustrated by Lamport's turing prize for Paxos. Trying to address problems of scalability, human incentives, modeling with process calculi and other such things in a single transition with a billion dollars at stake is a tall order.

It seems far more reasonable to embrace a smaller change and focus on the other major deficiencies of the system such as the developer experience of smart contracts or sub-protocols such as the recent ZCash contract and HAWK. Therefore, I will advocate to remove the difficulty bomb and to transition to something like VCU's recently developed PoW/PoS hybrid algorithm, which enjoys an incredibly sound theoretical foundation and the careful hand of peer review. Furthermore, when ETH takes the leap to Casper, the miners have somewhere to go.

As a final point in the short term roadmap, the failure of the DAO is not solely due to the arrogance and greed of the Slock.it team. The language they used to develop the DAO (solidity) was never designed for high assurance software. There exist well designed formal methods such as coq proofs that can provide mathematical guarantees of behavior.

It has always puzzled me why the ethereum team didn't initially emphasize these techniques. Smart contracts are generally small pieces of code that need high assurance of correctness. That's literally what these tools were developed to provide. There has been some great initial work done by Pattersson and Edstrom at Chalmers on using Idris to draft smart contracts. Furthermore, the Foundation seems to be taking formal verification more seriously. I will support work along these lines and attempt to bring such things to ETC.

Third, there is the matter of governance and funding. As I previously stated, I believe firmly it is counterproductive to establish a new foundation for ETC. We are blessed with an opportunity to try new ideas. Ralph Merkle has recently published a well written whitepaper (cite) on a system called DAOs, Democracy and Governance based upon ideas from Robin Hanson and others (also enjoy his recent Epicenter Bitcoin Interview). Arthur Breitman is preparing to release the first version of Tezos at Strange Loop in September that will create a formal mechanism to update a cryptocurrency protocol. And the Dash community seems to be focusing heavily on decentralizing governance and appears to have achieved some degree of success for their project. Given all of these advancements and great ideas, why should we resign ourselves to a foundation chained to local laws in a particular jurisdiction with a director?

It seems more prudent to gain community consensus on where ETC and ETH will diverge in the immediate future and then focus attention on developing a better governance model inspired by these ideas. As for funding, IOHK will commit to hiring three full time developers to exclusively work on implementing a roadmap for ETC for at least one year. Furthermore, IOHK's research division will develop a governance proposal within that year for ETC. In terms of an initial start, we are exploring if our Scorex codebase and EthereumJ can be hybridized.

Finally and somewhat ironically, I'd like to try to be a peacemaker during my time in this community. We gain nothing from fighting each other or name calling. We gain nothing from staging 51% attacks or a lawsuit against entity X for grievances. The reality is that ethereum classic should be treated as sharedrop targeted towards ETH holders. Everyone got the drop. Some sold, some lost their ETC and yes the DAO hacker gets a large share. But it is important to point out no one paid for their initial ETC.

If we continue to treat ETC or ETH as the one true chain, then we will spend the next few years sorting out the differences if it's even possible. Let's instead treat this like a philosophical split of an existing open source

project and someone gets to be libreoffice and someone gets to be open office. I understand it's not clean and that wasn't the decision of the people in ETC, but it's where we are at and we have to accept it.

As a fig leaf, it seems reasonable for the first joint effort of the ETH and ETC development teams should be an effort to completely resolve the replay attack concerns (here's a nice writeup). Someone has to blink.

Successful divergence gives ETH and ETC a wonderful what if opportunity to AB test different ideas. Why should it be wasted because of pettiness? To the ETC community, Bitcoin stayed by its principles and has achieved a ten billion dollar market cap and changed the world. We don't need to win by destroying ETH.

I Know This Place

I hope you enjoyed reading this long blog as much as I enjoyed writing it. One of my fondest memories was traveling to Miami in January of 2014 and meeting the Ethereum team for the first time in person. It was an innocent time filled with unbounded potential and passion. ETC feels like those times again, and we have an incredible opportunity to do something special with a great community that is willing to go the extra mile for their principles. That's a rare gift and I'm glad to be part of it in any capacity that's helpful to its growth.

It seems I've come to know this place for the first time. It's been a remarkable journey.