The Cryptocore Forms Communities

I got my hands on my first personal computer in 1980 - it was a Sinclair ZX80 that was loaned to me by my science teacher who didn't know what to do with it. It only ran BASIC programs, but it was part of the personal computer revolution because it was designed for use by an individual rather than being designed to support multiple users in an organisation that controlled how it was to be used. There were various other personal computers used on the way including MicroBees and C64s in school labs, but my first, owned by me, personal computer was bought second hand from a family friend when I was at university. My car that was stolen from a street near the university was unexpectedly found and returned to me - but I was so broke that I couldn't afford to register and insure it. I had got used to trains and buses and so I sold the car and bought the computer with the money - an original IBM PC/XT. Now I've had a personal computer of one kind or another ever since - but alas, not for much longer because you see, the Personal Computer is dead. Every device you buy now is again a multi user computer where the first and most important user is the one that an organisation such as Microsoft or Apple or Google installs on the device to make sure it serves them and their goals. The transition from a personal computer with a personality created by you to a device controlled by organisations is all but complete as it joins your phone, tablet and motor car as being a device owned by the organisation and leased to you under their terms. The personal bit in “personal computer” has been killed off as it is not as profitable as giving you a computer that removes your personal control of your own computer and the data you create with it. It is now an impersonal “device” back under organisational control.

Meanwhile, in liberal democratic societies the law still tries to find the balance within the triumvirate of government, individuals and corporations to try to ensure that each can perform their function but not get such a great advantage that they can control the whole rather than serve within the whole. However the law is slow while technology is fast, and so it is easy to see that governments and corporations able to deploy capital can rapidly get the advantage over the individual in that triumvirate leaving the unrepresented personal technology space to die on the vine without a lot of organised

collective support. And so the same dynamic that applied to the personal computer has been applied to the internet. The internet was supposed to be a network of peers where no one was able to exert control of the whole, but today we have the “splinternet” where the network designed to be a whole has been splintered into domains controlled by large corporate and government interests. And I don't say those words as breathless socialist hyperbole - I say them as a pragmatist who sees corporations like Facebook and Google who can colonise whole aspects of online life, Apple and Microsoft controlling devices, and countries like China who (in an ironic inversion of the issues of the natural environment) can simultaneously control the the doctrinal “purity” of their own online colony while they push political pollution into those of the “other”. Again, this is just a simple observation that large entities in my world are attempting to find their optimal version of the gilded technological cages we will inhabit in the centre of the panopticon defined by their various collective or personal visions.

Of course this didn’t occur without pushback and the cypherpunk movement arose with the raison d'etre to not just to think about the problems and solutions of a connected world panopticon, but as Eric Hughes said in his line that is now famous in the small concentric circles of crypto developers - “cypherpunks write code” to actively develop their solutions. And so while Satoshi Nakamoto is in the pantheon of cypherpunks for bringing forth to the world the concept of the blockchain as a solution to create decentralised money, he should also be remembered that he got there because he also wrote the code to make it real in order to prove it. There are plenty of deep discussions of intelligent concepts that do not get done; but the blockchain concept and Bitcoin did get done because Satoshi did it, proving along the way that writing code is indeed the ultimate direct political action that you can take when it comes to experimenting with tools to escape whatever digital panopticon raises your personal ire.

But the Satoshi blockchain solution only goes so far. An oft overlooked irony of our times is that while the cryptocurrency community spawned by Bitcoin talks about how cryptocurrencies enabled by networks and cryptographic techniques can increase personal freedom and control, it was networks and cryptography that allowed our freedom

to own and control our devices to be locked away from our reach so the personal could be removed from our personal computers. It is the very same networks, cryptographic tools, and hardware keystores implemented into corporate owned hierarchies that control our devices that crypto advocates say can undo them by being organised into a flat peer to peer model of individual agency. They are both correct, which means that cryptographic tools and techniques do no more than support the way humans want to organise themselves and their technology to achieve theirs and their collective goals. Some groups want to use technology to seek control, while others want to use it to be free from control.

The problem with cryptocurrencies though, is that they don't deliver the full promise. The blockchain does deliver the ability for a peer to peer network to be the trusted third party that achieves consensus over time about messages sent among adversaries; but it doesn't deliver much else. There is no encryption in cryptocurrencies, which means all data is public, and the way that people interact with cryptocurrencies today is the antithesis of the way it is presented. Instead of being a peer to peer network where each individual is a node on the network and empowered with freedom from control and censorship; what crypto is today is a concentrated client-server model where users use browsers to talk to intermediary servers that talk to cryptocurrency nodes controlled by protocol owners and fiat service providers. The crypto nodes managed by these providers are now so large and cumbersome that the monolith needs to be split into functional parts such as mining/validating, smart contract execution, and trust beacons. And the only way you can interact with the whole edifice is across the networks and servers run by companies that are within the control of governments and regulators, and on devices with the same control structures of app stores, plugin gatekeepers, and device censorship that killed the Personal Computer. We need to stop the collective delusion - crypto cannot pretend to work in a whole new way when it lives within the same system using the same design principals which we know allows for the removal of the personal and facilitates the imposition of corporate and government network control models.

This essay is not leading to a grand manifesto railing against the machine, or worse, a whitepaper informally describing a definitive

solution to it all. I am glad that I live in a liberal democratic society where the government, individuals and corporations are in a rough and tumble to find the balance between the individual and the collective. Rants against one or the other are tiresome and counterproductive; as is the shouting of a crypto denouement. But what is productive to me is to ensure that technology keeps getting created that helps the discussion and the reality of what can be done for individual freedom within collective pursuits. My dream is to develop a fully personal and individually managed computer that can be created and kept under the control of an individual like me in the same way that they are in control of their own body and mind. I call this the “Intercomputer” and I'd like to see that done for no other reason than it would be cool to see it done. If that computer can be “global” so that a user controls their space and also shares with others across a global address space in a personal and unmediated way, then I'd like to see that done for no other reason than I think it would be useful for others. But what people do with the intercomputer is of no interest to me any more than what they do with the tools of their own body and mind. What interests me is progressing the technology to get it done for no other reason that I believe it can be done and it will be useful. I also think it can strike a blow against those wanting to take away our freedoms. That is neither a thought crime, a revolutionary manifesto, nor making gold from lead - it's just following an idea and signing up to do some work. And I also do it for fun, so if it just ends up being an art project, so be it.

The augurs suggest we all need to help do the work to ensure our ideas are not made into thought crimes by those in government who are dogmatic, lazy, or banal and want the computer systems to do their job for them. We also have to keep a dual watch and work to ensure that our choices are not taken away by those too greedy to care about the consequences of their removal of our freedoms for their own narcissism and profit. It is by no means a futile pursuit as I do believe that the other wonderful innovation that has arisen from the cryptocurrency movement but which I don’t think is acknowledged enough as the most valuable, is that the fusion of crypto technology with a new generation has also created the ability for communities to come together using the blockchain as an organizing tool and data sharing platform, and these onchain communities are adopting the core values

of the younger with a mind to openness, sharing, and inclusion. I believe this happy coincidence will allow the movement to scale beyond having to rely on those that can “write code” as it lets multi-skilled groups form and work together on ideas in a way that is far more powerful than those of the curmudgeons of the cypherpunk era. Yes, cypherpunks write code, but in this new era, the cryptocore forms communities.