FREE-MAN'S PERSPECTIVE
• PARALLEL SOCIETY •
We have it in our power to begin the world over again.

ISSUE #42 November 2024

IN THIS ISSUE:

Cypherpunk Is Back

Cypherpunk showed up on the Internet in 1992, in the form of a Usenet group, having previously emerged in a few Silicon Valley living rooms. Quickly it developed a very specific way of looking at the world. Adam Back, an early cypherpunk and the creator of *proof of work*, described it this way:

> Cypherpunk is a state of mind – a proactive approach to societal change by doing: building and deploying tech – rather than by lobbying politicians or asking permission. It's also a mission statement of a life goal of what's interesting: societal change for individual empowerment.

It was cypherpunks who spread strong encryption to the world, against heavy threats. And as the 1990s proceeded, a significant number of intelligent and motivated people began to see what our new Internet

Cypherpunk Is Back, continued...

really meant to the world... that it was a new and empty territory, and one we could build as we saw fit.

The 1990s were an exciting time for cypherpunks, as we spread strong encryption across the world, produced excellent manifestos and began stringing technologies together into working systems. We built cryptographic mixes, ran anonymous proxies, and much more. As the decade wore on the original Cypherpunks list began to degrade (my old friend Sandy Sandfort had to moderate it for a while to settle it down), and less came from it.

By 2000 the list was barely productive, though we did have a very large project called Laissez-Faire City. But by 2003 that was over as well and cypherpunks went quiet. There were other lists, but the old culture of the Internet was changing, as "normies" flooded in and parasitic services rose to take advantage of them. Perhaps more importantly than that, the cypherpunks crew needed paying jobs, and writing encryption simply wasn't in demand. Most of them had to focus on paying the bills rather than rebuilding the world.

E-Gold was operating at this time, and while it was a grand and related adventure, it wasn't a particularly cypherpunks thing. Through the rest of the 00s, cypherpunks was mainly forgotten. For quite a few years Jonathan Logan and I (Jonathan being my partner in Cryptohippie) felt like the last of the cypherpunks. We weren't really, but it felt that way.

And then came Bitcoin. Bear in mind that Bitcoin was not an instant hit and didn't revive cypherpunks for some time. It started on just a couple of small lists that few people were using. Still, within a few years it became clear that this wasn't just some random new idea, but a very serious new idea. Little by little, that recognition spread.

Bitcoin became terribly exciting, of course, but it did so slowly, and checkered with difficulties. Still, between 2011 and 2014 its exchange rate with dollars had gained a lot of attention and bright, young, aggressive people were giving it their attention. That's when what we might call "the Bitcoin effect" came into play.

The Bitcoin Effect was two-fold:

- It led thousands and eventually millions of people to study money: What is it really? What makes good money? Where do dollars come from? And so on. This is a radicalizing field of study.
- It radicalized people who were initially interested in no more than price increases. They came to Bitcoin hoping to get rich, but once they grasped what this thing was, they became cypherpunks. As a great T-shirt used to proclaim: *Came For The Lambo, Stayed For The Revolution*.

And so cypherpunks rose again. But even so, this time the money aspect overpowered the cryptography and privacy aspects, and so it didn't feel quite like the original cypherpunks.

Recently, however, that has begun to change and I'm feeling excited about cypherpunks in a way I haven't in a long time.

The Miracle Of It All

It is faith that impels the world forward, and cypherpunks has always been an act of faith. The faith I'm referring to here isn't necessarily religious faith, but a deep belief in something that doesn't

Cypherpunk Is Back, continued...

presently exist: a commitment of will toward something that you can't yet touch.

And that faith has, in fact, worked miracles. (Depending on how you define the term, of course.)

I was unexpectedly confronted with the reality of that faith when I did an interview on cypherpunks some years ago. The interviewer asked me, "Didn't you sometimes worry that maybe you were wrong about all these things?"

It was a reasonable question, the fact being that we were essentially individuals, standing opposite to all the high and mighty of the world. But what popped out of my mouth was, "Oh no, we knew we were right." And we did. Without ever thinking of it in that way, we simply had faith.

I began to grasp the power of that faith at my favorite cypherpunk conference: looking around at hundreds of young people who really grasped this thing, I stood amazed at what had happened over the years. *Where did they all come from?* was my question to myself. It was a miracle.

And to understand the scope of this unfolding miracle, this passage from Alan Charles Kors (in *The Birth of The Modern Mind*) is essential. Here, he's describing the crucial period of change for Europe, as the medieval world became the modern world:

> If we stopped the clock at any moment between 1685 and 1715, and looked at the universities, looked at the educated and looked at the learned journals, it certainly would not have been obvious what was emerging that would so dominate and shape the 18th century. For this period between the 17th and 18th centuries is still very much a mixed intellectual world. But the new philosophers are emerging. They are increasingly setting the terms of debate. And they are increasingly winning the affections of the growing reading public of Europe.

The crucial point here is setting the terms of the debate. New ideas are routinely opposed, simply because they are new. But if you persist in those new ideas – if your faith in them is sufficient – they will find their way into the public discourse, and will, if they are potent ideas, soon enough begin settling the terms of the debate.

And so it has occurred with cypherpunk ideas. Consider these facts, please:

- The next President of the United States campaigned on defending Bitcoin. Mr. Trump has promised to beat back Senator Warren and other haters, he has suggested a strategic Bitcoin reserve, and so on. He has further promised to free Ross Ulbricht, presently the leading cypherpunk martyr.
- The next President's sons are building a DeFi system, and one targeted to the unbanked: the billions of people worldwide who have no bank account, and are so cut-off from modern finance.
- Wall Street is getting in on the act. Already there are multiple ETFs. Custody operations (the bank securing your bitcoin for you) are also available. And perhaps most importantly, banks are either accepting or preparing to accept Bitcoin as collateral for dollar loans.
- The US Treasury is courting a stablecoin. Stablecoins have become huge internationally, and stablecoins are most commonly

Cypherpunk Is Back, continued...

backed by Treasury bonds. That made stablecoin operations, like Tether, massive buyers of US government bonds. And the ownership of Tether is strongly cypherpunk. This group was catapulted into heavy-duty finance, and now has the US Treasury petitioning them to buy more bonds, and to buy longer-term bonds. The old joke was that if you owed the bank a thousand dollars you had a problem, but if you owed the bank a million dollars, *they* had a problem. Well, the US Treasury now faces the problem of keeping Tether happy... of keeping cypherpunks happy.

- Julian Assange has been freed. The number one cypherpunk martyr for a long time has been freed. And part of the story is the Assange DAO, which raised $53 million to free Julian. I'm not aware of the details or processes, but Assange was freed with the help of a cypherpunk vehicle (a DAO... *adigital autonymous organization*) and anonymous donors.
- The former Prime Minister of the UK wants bitcoin. This was missed by almost everyone, but when Tucker Carlson asked Boris Johnson for an interview, he has told he could have one, but he'd have to pay a million dollars, in the form of dollars, gold or bitcoin.
- The President of Argentina is an anarcho-capitalist. The overlap between cypherpunk and anarcho-capitalist approaches 100 percent. And so, the President of a major nation is now one of us, and is stridently pursuing such ideas. In addition, the President of El Salvador isn't too far from being an anarcho-capitalist.
- VPNs, Bittorrent and cryptocurrencies are everywhere. This is tech that we invented, and it has spread around the world, to the point where it's part of daily life for an enormous number of people.

Cypherpunks, astonishingly, have set the terms of the public debate, on a large scale. And again considering overlaps, cypherpunk overlays very significantly with homeschooling and what we might call the "return to family" movement.

I'm ready to continue on the role of faith in all of this, but I'll let that go and get to new tech that is presently coming out of cypherpunk groups.

Shielded CSV

This is one of the more exciting uses of technology for Bitcoin. It uses *client-side verification* (CSV) rather than on-chain verification. This trick, also used in Lightning, pulls verification off of the blockchain, allowing for more transactions per block; or, as is often said, it allows for scaling.

CSV, and particularly *shielded*CSV, not only helps scaling, but it massively improves privacy. That makes this especially practical, because privacy, by itself, doesn't sell terribly well. The reasons for that are some combination of silly and sad, but things have been that way all the same. Shielded CSV blows through that by selling the scaling and providing the privacy merely as part of the package.

Shielded CSV is still in its early stages, but it holds immense promise. Please develop and promote it any way you can. You'll find the whitepaper here.

FediMint

FediMint is a pure digital currency in

Cypherpunk Is Back, continued...

the original, Chaumian tradition. It can handle incredible numbers of transactions, clearing them within a few seconds each. And what has made it especially compelling is that it can be used to send wrapped bitcoin.

Wrapped bitcoin, as the name implies, is analogous to wrapping your bitcoin in an envelope and sending it through the system that way. The bitcoin is fully yours and fully spendable on the receiving side.

FediMint gets its name from the architecture of the system, which is that of federations: groups of trusted parties. A family could run a FediMint server, or a club, or anything of the type. And I like the larger implications of that: If you're trustworthy person, and able to cooperate with other good people, you gain a significant advantage over untrustworthy people.

So, super-cheap, super-fast, nearly limitless and perfectly reliable transactions are available to the man and woman who can show themselves as a solid, reliable person.

Zero Knowledge (ZK) Proofs

Zero knowledge proofs do this:

Prove that something (like a transaction or a message) is authentic or accurate, *without knowing any of its details*.

Think about that for a moment: With ZK proofs, you can verify that you're above or below a certain age, a resident of such a place, are holding so much bitcoin in escrow, or whatever, *without ever revealing the underlying information*.

- ZK proofs are just a clever use of cryptography, and there's a vocabulary unique to it, but it is extremely powerful and is developing well. It also has (or can have) excellent qualities for quantum resistance.

DAOs

Digital Autonomous Organizations, or DAOs, have been with us for some time, but seem to be coming into their own recently. They function almost like an ideal offshore corporation, but have further characteristics as well.

The most notable of the new DAOs was the Assange DAO, which raised $53. million to get Julian released. And released he has been. I can't tell how instrumental the DAO was in the release, but I'll bet it wasn't just coincidental.

And for what it's worth, DAOs can now be registered in the US state of Wyoming, should the operation require some traditional legal standing.

Lightning And Stablecoins

Lightning, as we note regularly, continues nicely, providing fast, cheap, secure Bitcoin transactions. Lots of people are running Lightning nodes (as we do at FMP), which is a the-more-the-merrier sort of arrangement.

Lightning, or rather Lightning Labs, is further training developers rapidly, a crucial part of the larger puzzle.

As noted earlier, stablecoins have become huge, and with Bitcoin's Taproot Assets upgrade, stablecoins can be sent through Lightning very cheaply and almost instantly. With better privacy too.

Nym: The Crypto Privacy Project

Anonymity has been, and remains, an essential threat to the legacy system of states and domination. But at the same time, the lack of anonymity (including privacy) is a deadly impediment to human expansion and thriving. "Everything visible to the

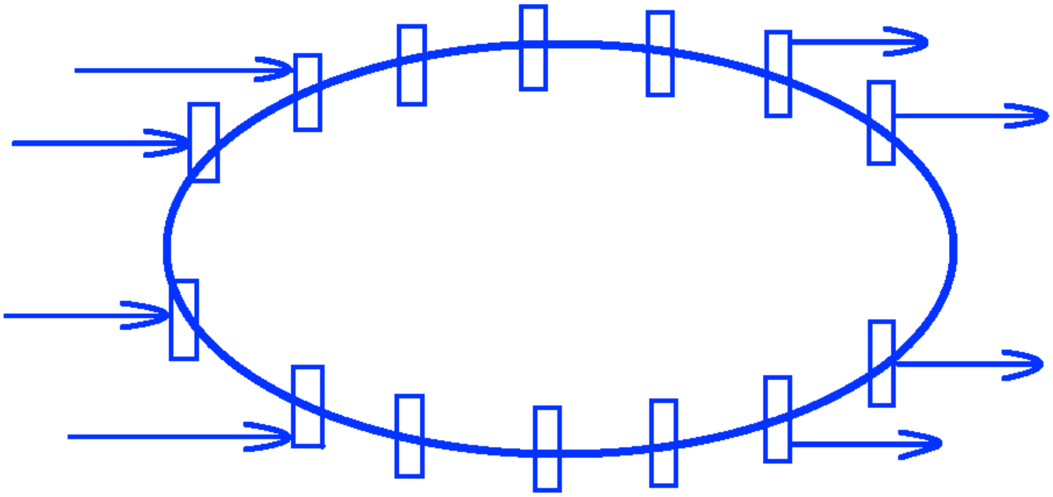
Cypherpunk Is Back, continued...

the overlord" is simply a version of slavery, and slavery kills the soul more than it does the body.

In the early cypherpunk times we created effective Internet anonymity with simple tools like anonymous proxies, but as time went on… as nation-states began to catch up… it became a lot harder. VPNs created effective privacy for some time, but bad and cheap VPNs drove quality out of the business, at least more or less. An effective, general solution has been lacking, although certain aspects of the overall problem (as with IPFS for non-censorship) have come forward.

Enter Nym: The Crypto Privacy Project. This group has been around for a while, but didn't produce much. Now, it seems, they are ready to deliver. And in particular, they are delivering systems that allow people to control their own identity, rather opposite to the social media model.

Briefly, the project is using the anonymity network model to create privacy. This is an expanded version of the original crypto mix model, and it's the model the Cryptohippie used. It looks rather like this:



Messages travel every which way in the network, entering and emerging at random places. Add-in time delays and a few other tricks, and tracing messages becomes quite difficult.

And so this again is a technology to support and develop. Once used widely, we'll have our privacy back, or at least a large portion of it.

Venice AI

While I'm not particularly a fanboy for AI, it is a powerful new technology and may have a very large impact in the years ahead. And, as we've learned over the past year or so, it can be used quite badly, as when it is trained to be politically biased, among other things.

Venice AI is a new version of AI, made by an early Bitcoiner named Erik Voorhees. Erik has put his bitcoin to use, building a variety of necessary systems, and Venice AI may prove to be one of the more important of them.

Venice AI (read about it here) is private and uncensored AI. There is no built-in bias, political or otherwise. It is designed (in the cypherpunk tradition) to be open source, permissionless, and decentralized.

If you're at all interested in Artificial Intelligence, I encourage you to look into, and support, Venice AI.

Cypherpunk Is Back, continued...

Blue Skies

The past four years have been difficult ones for cypherpunk projects, as censorship was massively promoted, free-speech advocates collapsed and vanished, and social media overwhelmed the world. Now that is changing, and the skies for us are clearing.

The skies are also clearing as Bitcoin is rising. That's especially significant since Bitcoin wealth has been the primary driver of new cypherpunk projects. This is one area in which the exchange rate of Bitcoin matters a great deal.

The regulatory pressures on Bitcoin, Monero (which I haven't mentioned nearly enough) and the entire suite of cypherpunk tech will not vanish, but they will pull back. Wall Street and the banking systems will still attempt to capture cryptocurrency, but they're not likely to succeed, especially as their systems feel the press of insane debts, inflation that probably can't be stopped, and the competing monetary systems of the East and South. In other words, they're facing multiple fronts in their money wars.

And so we must use this opportunity well. Find things you can be passionate about; support them, promote them, believe in them.

Ultimately it's faith that will win the battles for sound money and honest living. We must honestly believe in what we're doing: That is what will change things. And so I'll leave you with two quotes: the first from music producer Rick Rubin, and the second from my friend Harry Schultz.

Note that Harry's quote was from the pre-Bitcoin era and so focused on gold (also a decentralized currency). But I am taking the liberty of replacing "gold" with "Bitcoin." I am completely confident that Harry would not object. In fact we discussed this over the last few years before his passing.

> Faith is rewarded, perhaps more than talent or ability.

> Money sets a standard that spreads into every area of human activity… Layer by layer we are corrupted when money loses certainty… Fight for Bitcoin. Not for profits, though they are helpful… but for a future that returns to sanity. If we have a Bitcoin standard we get a better human standard! The two are intertwined. They are the ultimate cause and effect. Bitcoin blesses.

* * * * *

What's Going On

January, 2025

Overview: A corner has been turned. An over-extended, unsustainable and delusional set of beliefs is finally unraveling. It will not be saved, though its convulsions may continue for some time. And we now see that we have been setting the terms of the debate.

The legacy society:

Author Jeff Thomas likes to say that "Communism ends with a whimper, not a bang." That (thank God) is what we're witnessing in real time. And yes, the intellectual model of the past generation – the ideas that those in power and those educated in universities worshiped and enforced – were a version of communism.

This is not merely an American change. As the Financial Times noted recently,every governing party facing election in a developed country in 2024 lost vote share. We are witnessing an extremely arrogant model collapsing of it's own weight. As we move forward it will be replaced, bit by bit.

But we must not fight within the conversations *du jour*. Rather, we must work ahead of the curve: setting the terms of future debates rather than being mired in the present ones. And that means that we must keep working on new and better ways of communicating and cooperating. We must sail toward a distant star, especially now that we see it has been working.

What we're also seeing on this side of the corner is people finally speaking openly, rather than self-censoring for fear of loss. And one rather large example of this came recently, when a huge venture capitalist named Marc Andreessen spoke his mind on the Joe Rogan podcast, saying this:

> We had meetings [with Biden officials] this spring that were the most alarming meetings I've ever been in. Where they were taking us through their plans, and it was - basically just full government - full government control [of AI] - like this sort of thing, there will be a small number of large companies that will be completely regulated and controlled by the government, they told us. They said don't even start startups - there's just no way that they can succeed - there's no way that we're going to permit that to happen.

Right now a lot of people don't want to hear such things, but they will continue to be said, as the icons of Institutionalist Socialism (my term) begin checking out. Barring some very bizarre level of turnaround (which would all but certainly result in targeted violence), the old philosophy will loose one support after another and the old generation that gave their souls to it all will fall away. Those of the young generations who imbibed it will hopefully find ways to move on.

A very large change that may be coming is the US government moving in th e direction of tariffs. The US government paid for itself with tariffs before the creation of the Federal Reserve, and as impossible as it may seem, a move back toward that policy is quite possible. It would, however, collapse a good deal of "globalist" trade... though it would simultaneously spur the rebuilding of American manufacturing, and good jobs with it.

What's Going On, continued...

A tariff regime could work very nicely, though the forces opposing it would be large. That said, Mr. Trump's choice for the US Treasury Secretary, Scott Bessent, is pro-tariff, and so this does seem a serious possibility. If this does happen... and if regulations are simultaneously pealed back... it would be a great time to open a factory in America. There's real money to be made in manufacturing.

Mr. Trump is strongly fighting the idea that the BRICS countries will move away from the dollar, threatening 100% tariffs. That, of course, would cause a great deal of difficulty for some of those countries, but the fact remains that the degree of difficulty has been declining and will almost certainly continue to decline. As we've noted before, Russia is doing just fine, despite enormous levels of US restrictions and nearly every Western corporation pulling out in a moment.

Another interesting development is a move to restrain or break-up Google. A lot remains to be seen, but the movement is real, and almost certainly has high-level support. (The first legal action began in the previous Trump administration.) But whatever my misgivings about the players and processes, I would welcome the breakup of Google.

The New Society

We are winning. I know that feels like a foreign thought, but please try to move past the situations we all habituated to, because things have changed and we *are* winning (or, more properly said, succeeding). Try to accept this.

Among many other things, Elon Musk will be able to move his space plans forward now. Instead of having to fight against bureaucratic opposition, he'll be able to move at whatever speed his technology permits. Musk's plan is for 5 uncrewed test missions to Mars in 2026, followed byhuman missions in 2028. That's *big* stuff, and with Mr. Trump as President, and Mr. Musk as a major player in his administration, it faces very little opposition.

Despite Wall Street and other old-model groups, our "next economy" will continue invading the old. Among other things, the states of Texas and Pennsylvania have begun the process of setting up strategic Bitcoin reserves. So have the nation of Brazil and the city of Vancouver. We'll see what happens with these, but others are sure to follow. And in addition to "store of value" applications, our daily commerce applications, though generating less publicity, will also grow.

And, the adoption of Bitcoin by businesses over the past year is up 30 percent. A few more years of that will also change things.

And so the world has changed: not fully and not fully in line with my best wishes, but I'll nonetheless accept the changes with thanksgiving. The best use of our talents is to use *the things which are* to maximum benefit, not to gripe about what should have been.

Politics:

The outgoing Biden/Obama/DeepState regime is straining to prevent the loss of its surrogates, sycophants and fellow travelers (even as they slash at each other). These deeply overlapped groups will not go away in a moment, but they've already lost a great deal, especially a popular thirst for war. Most of the mayhem over the next four years is likely emanate from them, in one way or another.

Mr. Trump's inauguration in just a few weeks will formally mark the changeover, which, if I'm not mistaken,

What's Going On, continued...

will be more significant than it appears. The people he’s appointing are serious about changing the culture of US governance: intelligent and highly motivated outsiders (to some large extent), will now have their hands on the levers of power.

This change will be ugly and incomplete, to be sure, but it is breaking the back of the old order’s Institutionalist Socialism. Again, that’s big.

* * * * *

Upcoming Events

Ongoing:

- Bitcoin Meetups
- Ethereum Meetups
- Bioengineering Classes
- Crypto For Business Course

Coming Soon:

Bitcoin 2025
Las Vegas, May 27-29

New World Links

January 2025

1. On Watchman Privacy
2. Shop In Bit
3. Doing Good Works
4. Robosats
5. BitPunk
6. Reticulum
7. Gold For Daily Use
8. HodlHodl P2P Exchange
9. Start9 Hardware
10. The Unplugged Phone
11. Primal
12. Expanding The Lightning Network
13. Use Bitcoin Without Selling It
14. Bisq Decentralized Exchange
15. Plebian Market
16. Vexl's Financial Tyranny Index(PDF)
17. Liberty Travel Coach
18. Velas Crypto Resources
19. Dark-fi
20. Dr. Joel's New Course
21. Toward A Private Digital Economy
22. Internet Native Dispute Resolution
23. Private Telephone and Text
24. Another Climate Scientist
25. From Crossbows To Cryptography
26. Apollo Photos
27. The Crypto Anarchist Manifesto
28. Jones Plantation Film
29. Decentralizing Science

Memes of The Month

bitcoin
93K
COMING SOON
GERMANY TRYING TO GET BACK THE BITCOIN THEY SOLD AT 50K:
I WANT TO TALK WITH THE MANAGER
@MAXISCLUB BY REDY
951/2100

What you thought joining the resistance would look like
What it actually looks like

HOW MANY TIMES DID THIS HAPPEN BEFORE THEY HAD TO PUT A SIGN UP

Whenever I'm feeling down I just remind myself that trillions of dollars of propaganda didn't work on me

A Final Thought

It's funny how many things pop up once change really begins. And one of those is a set of terms to describe things we've talked about for some time: that everything held to by the "right thinking" crowd is pushed to the ultimate extreme before it finally breaks. Now we have a term for this, the *preference cascade*.

The term was first used some years ago, but very few people heard it, myself included. Now that has changed.

A preference cascade is a seemingly sudden shift in public opinion that occurs as individuals begin expressing what they had been suppressing over fear of repercussions. A related term, called the *preference threshold* marks the point were people begin to open up and speak. And until that point is reached, many people will engage in *preference falsification*, not allowing themselves or others to utter the unutterable.

This, of course, is what happened at the end of the USSR. Everyone grasped (more or less) that Soviet culture was a gigantic set of lies, but most people played the party line all the same... until they reached the preference threshold and started admitting it.

And so the mighty USSR ended. Likewise the bizarre Woke dogmas on race, gender and so on are breaking. The many enforcers of Woke-speak are falling silent in the face of their neighbors and in-laws speaking freely. Most will release their grips and not fight to retain their informal positions as moral enforcers.

A number of things have notably combined to pop the preference falsification bubble: Certainly the liberation of Twitter under Elon Musk ranks very high, akin to fax machines in the USSR. Another was Donald Trump's election. Both popped the compliance bubble, letting people realize that they were the actual majority.

Underlying that was the Covid vaccine fiasco. Many people have yet to face it, but the vaxx was the greatest medical failure of our times... maybe the greatest in human history. And all the former vaxx advocates know it, because, as I like to point out, *everyone got it anyway*. Even as they refuse to acknowledge the fact, they are not utterly blind to it.

And there are other aspects to this, such as the supposedly enlightened elite universities turning hard against Jews.

And so the change begins. Things will not be entirely the same from here on.

See you next time.

Come across something awesome?

Send a note about it to fmp@veraverba.com. (And forgive us if we don't respond.)

WE are the real world. Politics, TV, and Facebook are the illusion.