BITCOIN MAGAZINE®

DISPLAY UNTIL JULY 1ST, 2023

$21.00US

32

6 02648 40388 7

THE **WITHDRAWAL** ISSUE

BITCOIN AND THE PLOT TO DESTROY FINANCIAL PRIVACY

BY WHITNEY WEBB

Late last month, a bipartisan group of U.S. Senators introduced the Financial Technology Protection Act, which would "create a working group tasked with studying how terrorists or other criminals might use cryptocurrencies and other new financial technologies, and create proposals for Congress and regulatory agencies aimed at countering these uses". This working group "would be composed of representatives from the U.S. Treasury Department, Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Services (IRS), the Office of Foreign Asset Control (OFAC), the FBI, the Drug Enforcement Agency, the Department of Homeland Security, the Department of Justice, the Department of State and the CIA".

Bitcoiners should play close attention to these developments as the DOJ in particular has attempted to paint bitcoin as the payment of choice for well-known terror groups like ISIS and al-Qaida, signaling that the working group proposed by this bill will likely seek to specifically target bitcoin. Adding to this concern is the fact that a slew of recent mainstream media reports — which cite Treasury and FinCEN officials, DOJ officials and CIA analysts — have claimed specifically that "terrorists are turning to bitcoin, and they're learning fast", that bitcoin is the "new frontier in terror financing", and that "bitcoin is helping terrorists secretly fund their deadly attacks". Even the prominent military think tank RAND Corporation has argued that "bitcoin and the dark web" are the newest terrorist threat.

Many of these same entities, particularly the U.S. Department of Justice, are also currently helping to draft the UN's new cybercrime treaty, showing that there is currently a very global effort to stomp out "cybercrime" and alleged funding sources for "cybercriminals". However, much like the words "terror" and "terrorist" after 9/11, the terms "cybercrime" and "cybercriminals" are often vaguely defined by these same authorities.

Perhaps unsurprisingly, many of the groups looking to allegedly combat cybercrime in the U.S. and beyond, including the Department of Justice and the FBI, are part of an international public-private partnership housed within the World Economic Forum that is seeking to define these terms in unsettling ways. Not only that, but this group and its partner organizations are also seeking policy objectives that — if widely implemented — would treat anonymous cryptocurrency transactions, and specifically Bitcoin transactions involving mixers and related privacy tools, as criminal. They also assert, without evidence, that there is a direct link between an increase in the value of cryptocurrencies, especially of bitcoin, and cybercriminal activity.

This public-private partnership — the WEF Partnership Against Cybercrime or WEF-PAC — is run by a former intelligence agent named Tal Goldstein, whose military intelligence career was marked by his efforts to have intelligence agencies essentially fuse with private technology companies in his native Israel. Today, WEF-PAC's members not only include the FBI, the Department of Justice, and intelligence agencies of Israel and Britain, they also include massive too-big-to-fail banks like Bank of America and Santander as well as massive tech companies like Amazon and Microsoft. Even the non-profit that manages the SWIFT payment system is a member.

In recent reports, WEF-PAC has alleged that there is a connection between the use of cryptocurrencies as well as privacy enhancing tools such as mixers and the incidence of cybercrime. They go on to argue that, "Cybercriminals abuse encryption, cryptocurrencies, anonymity services and other technologies", even though their use is hardly exclusive to criminals. Though they refrain from naming any currency specifically, the WEF has stated elsewhere on its website that, "Governments don't like the fact that bitcoin users are anonymous, and they have concerns over its use for criminal activity and money laundering". adding that "their worries aren't unfounded".

It's important to point out that WEF-PAC doesn't see cybercriminals just as those who engage in hacks or financially motivated acts like ransomware attacks. To WEF-PAC "cybercriminals" also include those who use those technologies to "uphold terrorism" and "spread disinformation to destabilize governments and democracies". From that, it seems that WEF-PAC's inclusion of "disinformation" as a type of cybercrime betrays an intention to develop policies that, under the guise of "combatting cybercrime", will also promote increased online censorship.

In discussing "solutions", WEF-PAC calls for the global targeting of "infrastructures and assets" deemed to facilitate cybercrime, including those that enable "cybercriminal... revenue streams", which — as we will see shortly — refers to the infrastructure that allows for more private cryptocurrency transactions, and enables "the promotion of illegal sites and the hosting of criminal content". In another section, the group discusses seizing the websites of "cybercriminals" as an attractive possibility. Given that WEF-PAC and its members, like the FBI, view online "disinformation" as a form of cybercrime, this could potentially see independent media websites and the infrastructure that allows them to operate and finance their work (i.e., video sharing platforms that do not censor, etc.) emerge as targets. Earlier this month, the FBI, in coordination with the National Police of Ukraine, did just this, seizing nine crypto exchanges, the majority of which had bitcoin or btc in the domain name. Their crime? Offering "anonymous cryptocurrency exchange services to website visitors".

WEF-PAC further argues that "in order to reduce the global impact of cybercrime and to systematically restrain cybercriminals, cybercrime must be confronted at its source by raising the cost of conducting cybercrimes, cutting the activities' profitability and deterring criminals by increasing the direct risk they face". It then argues, unsurprisingly, that because the cybercrime threat is global in scope, its "solution must also be a globally coordinated effort". They say that the main way to achieve this involves "harnessing the private sector to work side by side with law enforcement officials". Shockingly, WEF-PAC calls for this "cooperation" to take place even if it is "not always aligned with existing legislative and operational frameworks". In other words, they are saying this cooperation should be allowed to take place even if it is illegal.

So how exactly do the members of WEF-PAC plan on confronting cybercrime "at its source by raising the cost of conducting cybercrimes, cutting the activities' profitability and deterring criminals by increasing the direct risk they face"?

While they are tight-lipped on the exact measures, another group closely aligned with the WEF that has considerable overlap with WEF-PAC specifically has some ideas.

The Financial Services Information Sharing and Analysis Center, or FS-ISAC, officially exists to "help ensure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy". In other words, FS-ISAC allows the private financial services industry to decide on and coordinate sector-wide responses regarding how financial services are provided during and after a given crisis, including a cyber attack or sector-wide concern over cybercrime, like past WEF warnings of a coming cyber "pandemic". Tellingly, FS-ISAC was created in 1999, the same year that the Glass-Steagall Act was repealed.

FS-ISAC's members include the biggest firms on Wall Street — Citigroup, Bank of America, Wells Fargo, and Morgan Stanley are among its members — and much of FS-ISAC's leadership contributes to, works for, or chairs committees and initiatives of the World Economic Forum, including those focused on cybercrime and ransomware. In 2021, FS-ISAC's Global Intelligence Office released several "predictions for 2021 and beyond". Most of these predictions express concern about a coming cyber calamity, though one prediction in particular stands out: The "economic drivers towards cybercrime will increase". FS-ISAC claims that the current economic situation created by COVID-related lockdowns will "make cybercrime an ever more attractive alternative", stating immediately afterwards that "dramatic increases in cryptocurrency valuation may drive threat actors to conduct campaigns capitalising on this market, including extortion campaigns against financial institutions and their customers".

In other words, FS-ISAC views the increase in the value of cryptocurrency as a direct driver of cybercrime, particularly for ransomware incidents, implying that the value of cryptocurrency must be dealt with if there is to be a reduction in cybercrime and if cybercrime is too be confronted at its source by attacking its "profitability", as WEF-PAC suggests. However, the data does not fit these assertions as the use of cryptocurrency by cybercriminals is low and getting lower. For instance, one recent study — ironically produced by WEF-PAC member Chainalysis — found that only 0.34% of cryptocurrency transactions in 2020 were tied to criminal activity, down from 2% the year prior. Though the decrease may be due to a jump in cryptocurrency adoption, the overall percentage of crime-linked crypto transactions is incredibly low, a fact obviously known to FS-ISAC and its members.

What's disturbing here is that mainstream media has widely circulated the claim that Bitcoin specifically is, to quote Forbes, "driving the $1.4 billion ransomware industry". Or NPR, "bitcoin has fueled ransomware attacks". Or an executive at WEF-PAC member Chainalysis, bitcoin is the "favorite by far" for ransomware attackers. I could give many more examples as there is truly an abundance of reports just like these that blame a jump in well-publicized cybercrime events — specifically ransomware attacks — on bitcoin's increased popularity and bitcoin's intrinsic value.

Yet, here, if the banks, intelligence agencies, and tech companies that partnered with these initiatives see, not just financial privacy, but the value of bitcoin itself as a threat, it goes without saying that their efforts to stop cybercrime at "its source" would not just involve eradicating financial privacy when it comes to crypto, but devaluing crypto.

With such groups openly discussing working outside of "legal frameworks" to accomplish their goals, Bitcoiners must start paying closer attention to these shadowy groups.

There is no proof that cryptocurrency, or more specifically bitcoin, is the key driver of cybercrime, as cybercrime significantly predates the existence of both bitcoin and crypto. However, cryptocurrency does present a threat to the plans of FS-ISAC members and their partners to begin producing digital currencies controlled either by approved commercial banks or central banks themselves, digital currencies that are designed to be easily surveilled. Central bank digital currencies in particular are being designed and implemented to erode financial privacy and autonomy. The success of CBDCs and related projects depends on neutering the competition, which is likely why FS-ISAC has called for the economic drivers of cybercrime to be combatted by "a global fin-cyber utility", which is of course the very same globalist entity that WEF-PAC seeks to create.

Not long before FS-ISAC and WEF-PAC made these claims, many members of both groups participated in a 2020 initiative hosted by the Carnegie Endowment, itself a member of WEF-PAC. The president of the Endowment at the time was William Burns, who subsequently became Joe Biden's pick for CIA director less than a year later. The Carnegie Endowment's initiative brought together many members of WEF-PAC and FS-ISAC with an important addition — representatives of central banks, namely the U.S. Federal Reserve and the European Central Bank. Also notably present in this initiative was the U.S. Federal Deposit Insurance Corporation (FDIC).

The report developed by these parties is astounding as it states that the main cause of global financial instability is not irresponsible central bank policies or commercial banks engaging in criminal behavior, but instead "the current fragmentation among stakeholders and initiatives". They argue that the main solution needed to "stabilize" the global financial system lies in reducing that "fragmentation". The only way to accomplish that, they say, requires the massive reorganization of all "stakeholders" via increased global coordination and specifically notes that the "disconnect between the finance, the national security and the diplomatic communities is particularly pronounced" and calls for much closer interaction between the three. It goes on to state:

"This requires countries not only to better organize themselves domestically but also to strengthen international cooperation to defend against, investigate, prosecute and ideally prevent future attacks. This implies that the financial sector and financial authorities must regularly interact with law enforcement and other national security agencies in unprecedented ways, both domestically and internationally."

Essentially, this initiative has called to begin fusing commercial banks and financial authorities (i.e., regulators) with national security and law enforcement agencies. This policy could not be more dystopian. Making things even worse is the fact that WEF-PAC, of which the Carnegie Endowment and many of the other organizations behind this policy are members, not only call for this same fusion to take place but also to do so in ways that may be illegal.

A merging of commercial banks, their regulators and the intelligence agencies is a complete nightmare scenario, but this is exactly what the World Economic Forum has come to promote as a model for "public-private partnership". But, perhaps more critically for American citizens, this is a policy developed with the direct participation of the Federal Reserve, the FDIC, the U.S. Secret Service, the FBI, the Department of Justice, and the country's most "systemically important" commercial banks. The "establishment" in this country supports these policies and, from what I can see, they have every intention of trying to make them a reality.

These American federal agencies, institutions, and commercial banks are playing a major role in developing regulations that will inevitably target bitcoin. They have made it very clear in these policy documents, incubated by groups like the WEF, that they see financial privacy, the popularity of bitcoin and the value of bitcoin as direct threats responsible for what they define as "cybercrime".

Yet, time and time again, the American people have been fleeced and looted by many of these same agencies and many of these same commercial banks. The big banks like HSBC can launder millions of dollars for drug cartels and nothing happens to them; no one goes to jail. The CIA has laundered untold millions through criminal banks like BCCI, a bank which also ran its own sex trafficking operation involving prepubescent kids, and again nothing was done and no one went to jail. FTX can launder aid money supposedly destined for Ukraine and then funnel it back as campaign contributions to the same political party developing crypto regulations, while painting bitcoin as a "national security threat". Sam Bankman-Fried was the only person arrested and right now, he's not in prison; he's sitting in a multimillion dollar mansion in California about to get 10 of the 13 charges against him dismissed. The current president's son can launder as much money as he wants after leaving the evidence on a laptop he abandoned and the intelligence community comes to his defense, falsely claiming the data on this laptop — now admitted to be his — was a "Russian hoax". These guys are the real criminals and if you think they care about stopping money laundering and cybercrime in any meaningful way, you have been had.

But, soon, if nothing is done to stop these policies that are being drafted behind closed doors, use a Bitcoin mixer and take steps to keep your Bitcoin transactions anonymous, you'll be accused of acting suspiciously like a "cybercriminal". Complain about the obvious double standard and you'll be accused of spreading "disinformation" and become a cybercriminal yourself.

What should particularly concern us now is how these agencies, entities and "public-private partnerships" plan to manufacture consent for their policies. As things stand right now, a lot of the policies dreamt up by these groups that I've just described would, I hope, be rejected by the vast majority of Americans. That is, of course, unless the right crisis were to come along and suddenly make most Americans extremely concerned about "cybercrime".

While warnings of a so-called "cyber pandemic" floated around in 2021 as a series of high-profile and highly publicized ransomware attacks took place, we haven't heard as much since. Yet, with the last global crisis, COVID-19, officially over according to the U.S. government and the WHO, some are raising the alarm that a new global crisis is soon to make a dramatic appearance.

Well, given what I've been saying, let's check in with the World Economic Forum and see what they think this next global crisis will be. Well, in January of this year, Jeremy Jurgens, No. 2 at the WEF after Klaus Schwab, asserted that a "catastrophic mutating event will strike the world in 2 years". What a confident prediction! So what is this "catastrophic mutating event" that will strike the world before 2025, according to Jurgens? If you guessed "a global catastrophic cyber event", you win.

At a presentation at this year's Davos, Jurgens claimed that "93 percent of cyber leaders, and 86 percent of cyber business leaders, believe that the geopolitical instability makes a catastrophic cyber event" essentially inevitable before 2025. Joining Jurgens in fearmongering over a cyber doomsday was Jurgen Stock, the head of INTERPOL, one of the most influential members of WEF-PAC. I should also add that the UN, which, as I mentioned earlier, is currently making its new cybercrime treaty, has named Interpol as "uniquely positioned to be the implementing partner of a number of the 2030 Sustainable Development Goals", specifically when it comes to "disrupting financial streams" of alleged terrorists, "securing cyberspace", and "curbing illicit markets".

Jurgens' and Stock's comments about a "catastrophic cyber attack" before 2025 spawned hysterical mainstream headlines warning of "cyber apocalypse 2023". That same month, Newsweek's print edition featured an ominous hacker on the cover with the words "Hack Attack: How Cybercriminals Outwit All Efforts to Stop Them". Many of the experts quoted in the Hack Attack article work for companies that are WEF-PAC members, like the intelligence-linked cybersecurity firm Checkpoint.

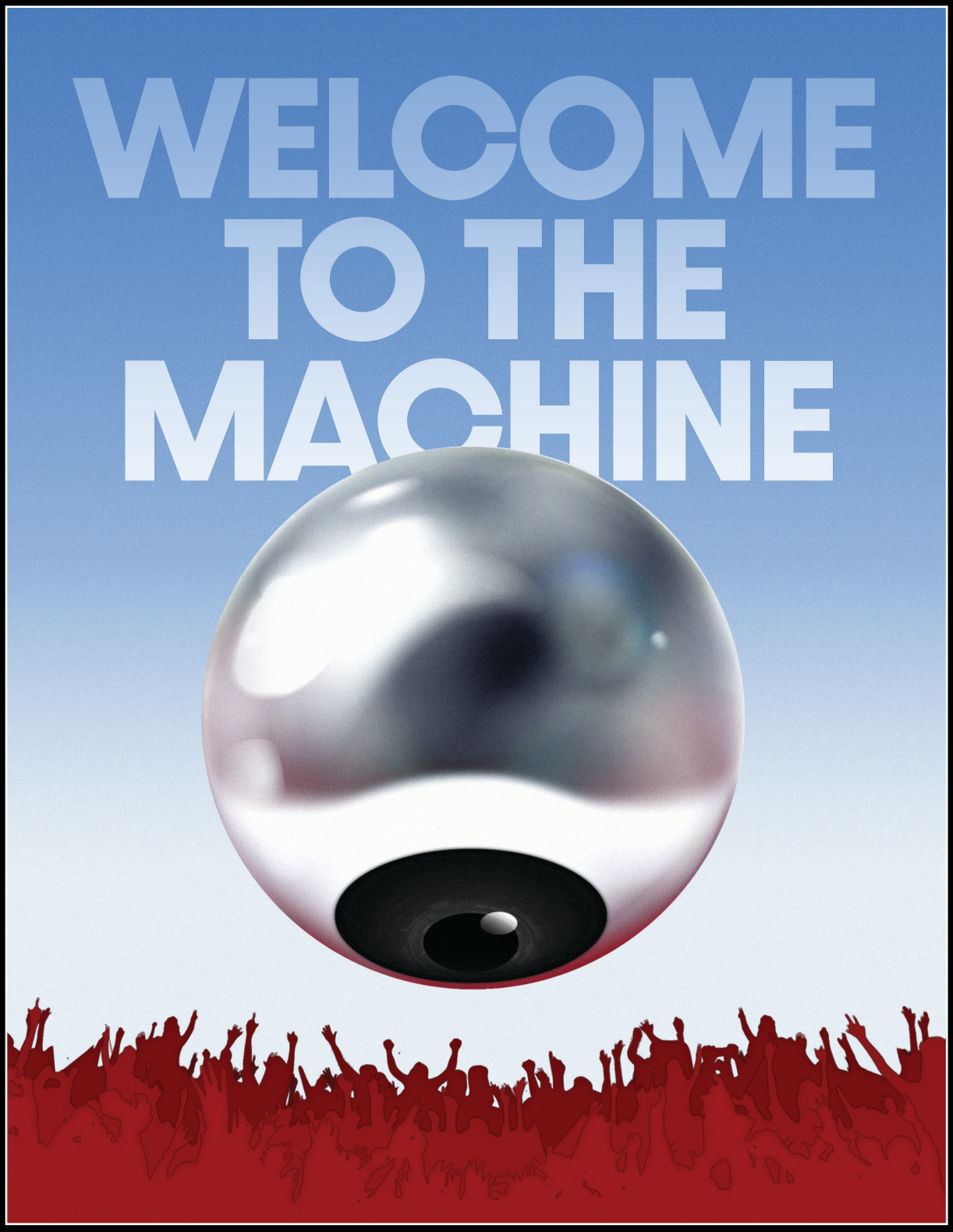
In recent years, there has been much talk about a big doomsday cyber attack and now it seems top people at the WEF and WEF-PAC feel confident enough to put a relatively short timeline on it. How bad will this attack be if and when it materializes? Considering that the head of the Department of Homeland Security has claimed that the "next cyberattack" will kill people, it seems like a cyber 9/11 may be waiting in the wings — to be followed shortly thereafter, of course, by a cyber Patriot Act or something very similar. If bitcoin is blamed for motivating or funding the cybercriminals deemed responsible for such a catastrophe, what will happen to public opinion about bitcoin and what type of legislation might we see rammed through Congress?

Given what I've described here, the WEF and its allies, including several U.S. government agencies, need a couple things to come to the forefront of the public mind before they can offer the dystopian "solutions" that they have already on the books. In order to fuse banks, regulators and the national security state to end "fragmentation" in the global financial system, "global financial instability" must first become a major global concern. With everything that has been taking place since the collapse of Silicon Valley bank, it seems we are not that far away from "global financial instability" becoming a top concern for the average person.

The other thing they need to happen is for the average person to become incredibly fearful of financial privacy and online privacy, to the point that they will willingly trade their privacy for greater security, or rather what will be sold as greater security. Bitcoin, privacy-minded crypto, and privacy-preserving technologies like encryption must become public enemy No. 1 in order for the offered solution — a completely surveilled internet and completely surveilled financial system — to be accepted by the masses.

The fight over the control of the cryptocurrency space is part of the larger war being fought over the future of our society, our country and the world. Will we sleepwalk into a world of CBDCs where intelligence agencies, central banks, and commercial banks have fused into the same Orwellian entity, where holding "terror-linked" bitcoin or using encryption or mixers makes you a "cybercriminal"? Or will we fight the groups and institutions that have looted American wealth for well over a century and demand a return to the Constitution and the right to privacy, not just financially but in all senses? Those that wish to force us into the former scenario clearly and unequivocally see Bitcoin and privacy-enhancing technology as a direct threat to their power.

There has never been a more important time to choose a side.



This fan-art is inspired by a Pink Floyd animated video originally projected as a performance backdrop when they promoted their album *Animals* during the "In the Flesh" tour in 1977. The image is based on George Orwell's political fable *Animal Farm*. It became the original music video of the song "Welcome to the Machine" directed by Gerald Scarfe.

CALL FOR SUBMISSIONS

"Satoshi, grant me the serenity to accept the things I should not change, like monetary policy, the courage to self-custody the things I can, and the wisdom to know the difference between fiat and hard money."

We here at Bitcoin Magazine are free speech maximalists who also take pride in carefully spotlighting the humans and projects in written contributions from the voices of the moment in Bitcoin. Any editorial has an unwritten responsibility to platform the many schools of thought from the people that support it. Well, consider this a written acknowledgement.

The greatest strength Bitcoin has is its community and we want to know what has captured your interest. Got something to share? Do you think Bitcoin Magazine is the right place to tell your story? What exactly would you like to read about? We could not possibly continue to serve the Bitcoin-only needs of our community without directly hearing from Bitcoiners themselves. This will only continue to grow difficult as what it means to be a Bitcoiner continues to broaden.

We will continue to post pieces that contain opinions far off the beaten path, from writers with minds and ideas entirely of their own free will. We might even disagree amongst ourselves if we should publish a piece or not. Ultimately, free speech posturing is toothless without an open call for submissions.

Bitcoin is for everyone. Remind us. Help us show the world that Bitcoiners come from all walks of life from every which place. Send us an email and tell us why you and your story deserve a handful of pages in a print issue or online.

Even Bitcoin started with an email.

C786-529C-ODD3-64E2-F5A8-8554-OECD-433F-4C11-FFFE

THE EDITORS

BITCOIN MAGAZINE PRINT TEAM
print@btcmedia.org