A CASH APP ZINE

BREAD

01
THE BITCOIN ISSUE

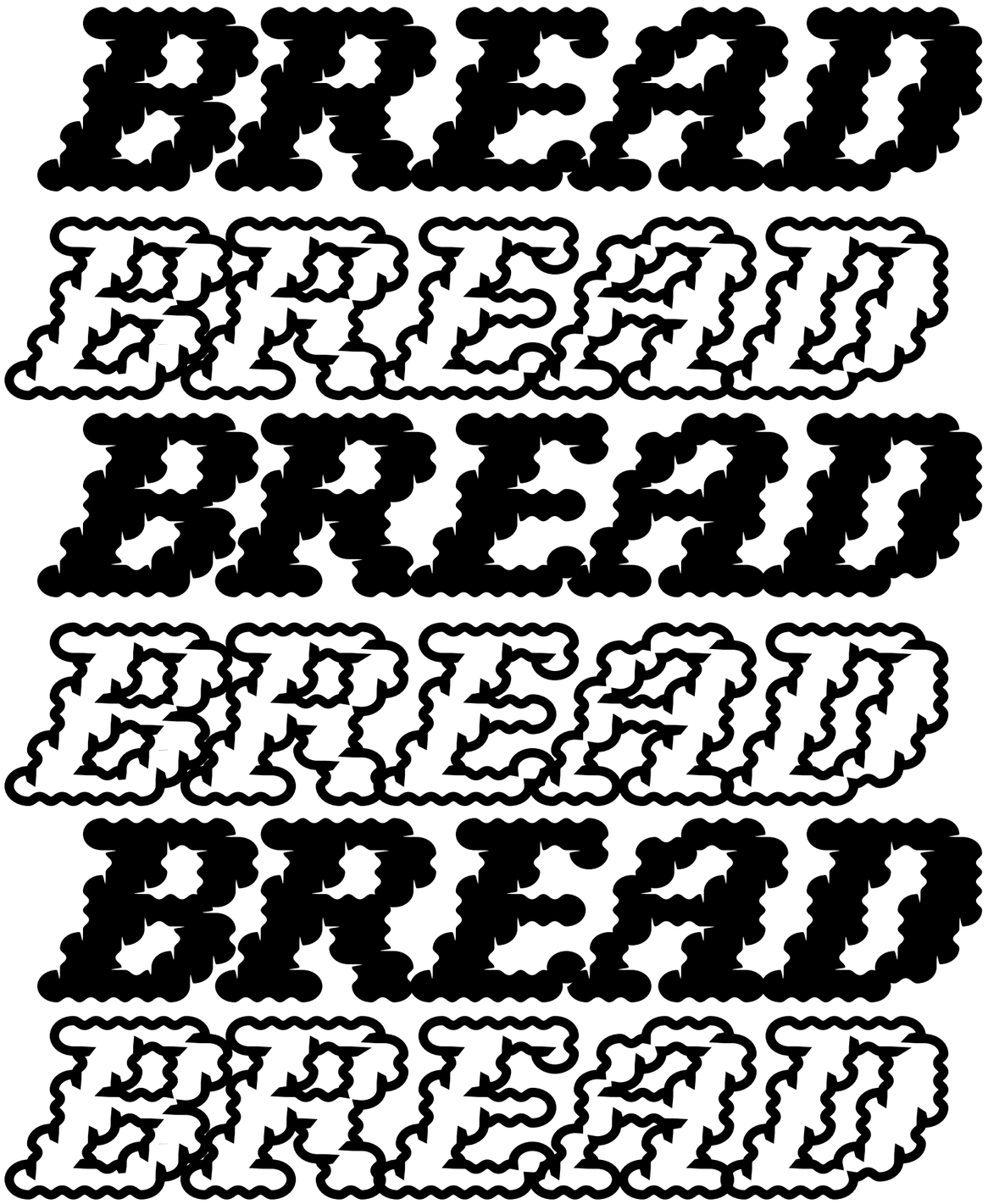

BREAD
BY
Cash App
STFNY.U
SEP 04 '23 13:52
1 BREAD 0.00011 BTC
1 MILK 0.000075 BTC
1 EGGS 0.00013 BTC
1 ONIONS 0.000056 BTC
1 BANANAS 0.000030 BTC
SUBTOTAL 0.000401 BTC
TAX 0.000075 BTC
AMNT DUE 0.000475 BTC
CHANGE DUE 0.00 BTC
0.000033 BTC
THANK-YOU FOR SHOPPING WITH BREAD!
CALL AGAIN SOON
HTTPS://CASH.APP/
BTC
BREAD
FARM FRESH
BREAD
Vitamins

BREAD

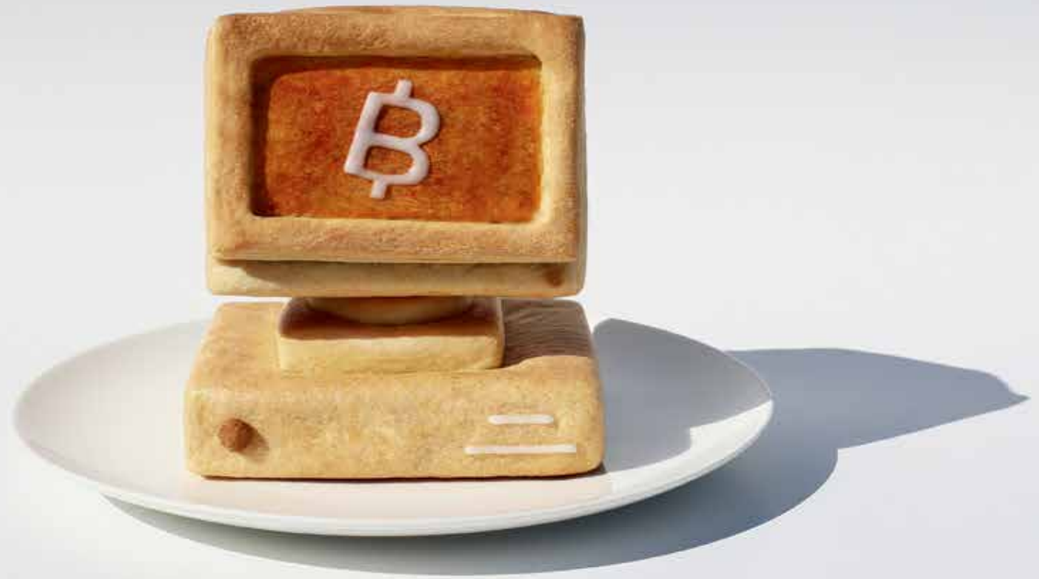
noun

1. money; i.e. *let's get that bread*, means let's make money.

A NEW ZINE
FROM CASH APP
THAT'S
REINTRODUCING
BITCOIN.



BY DAISUKE @DIMDA



THE BITCOIN ISSUE

CONTRIBUTORS

Allison Davis
Aurore Chauve
Bob Jeusette
Cevallos Brothers
Christopher Walker
Collier Meyerson
Daisuke
Elise Craig
Elle Clay
Emilia Petrarca
Emma Hazen
FOOD
FRKO
Intranetgirl
Juliet Thompson
Margaret Rhodes
Masterpiece Printers
New Distribution House
Nick Tabor
Olympic Studio
Porto Rocha
Raul Lopez
Richard Turley
Satoshi Nakamoto
Shuhua Xiong
Stephanie Specht
Steven Montinar
Unfun

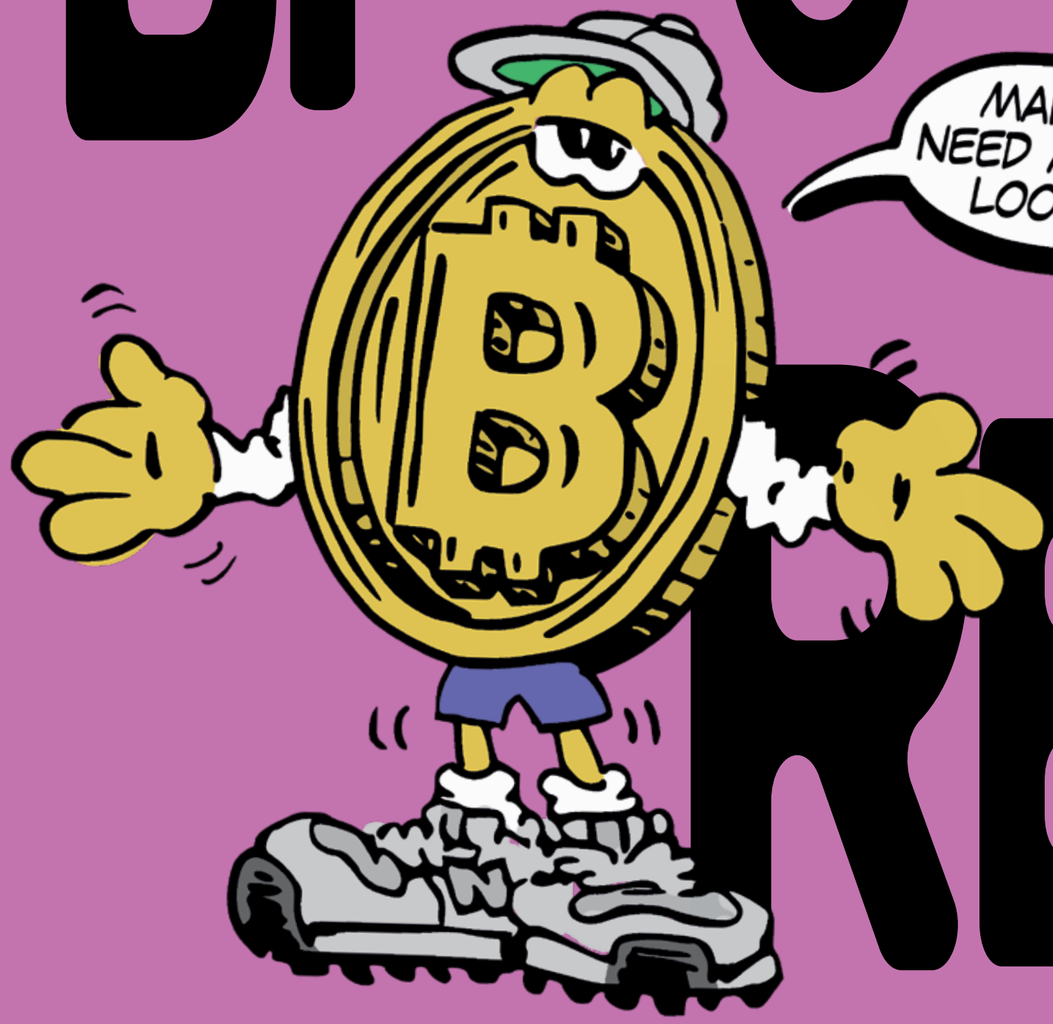
TYPEFACES

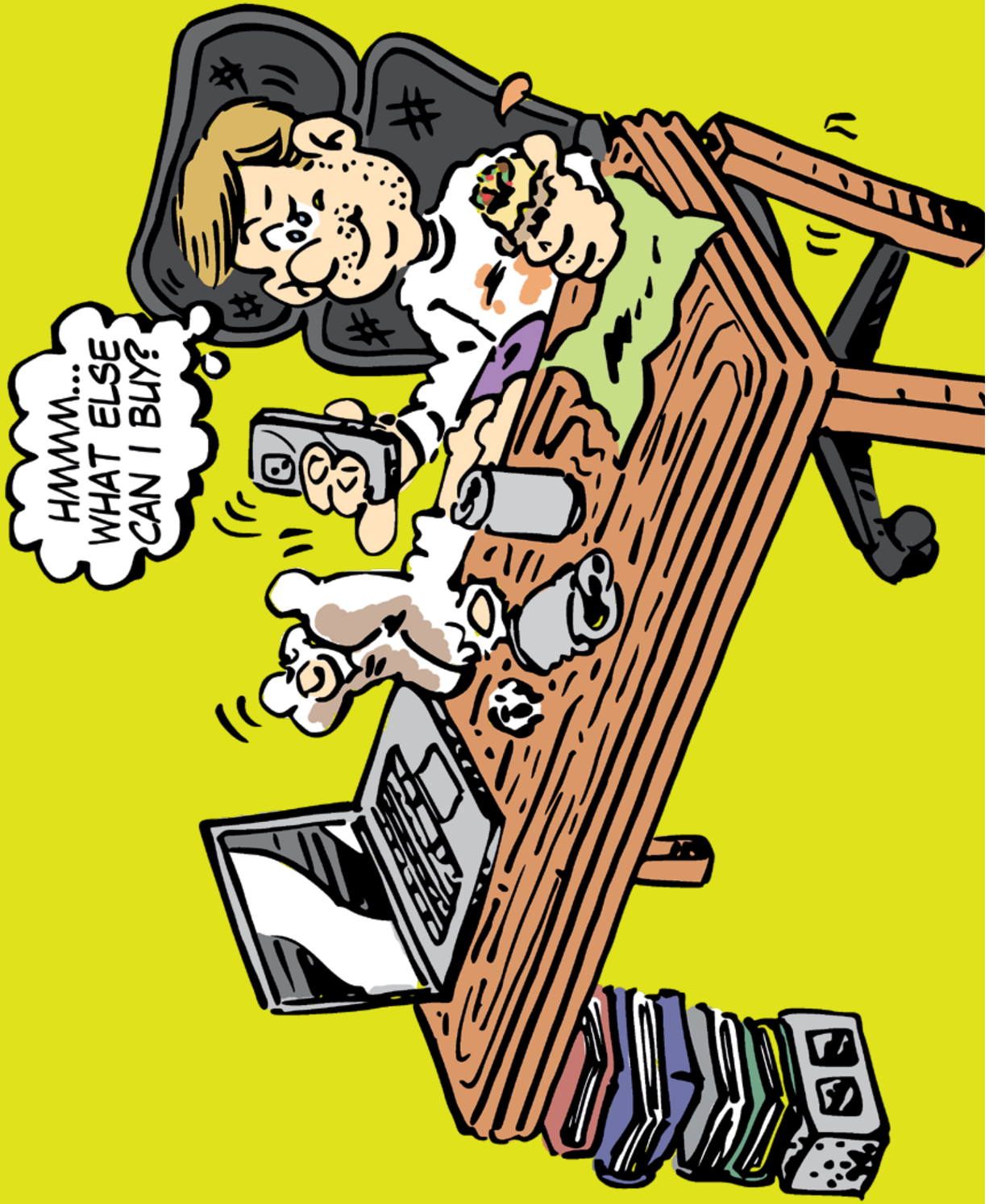
Söhne (Klimt Type)
HAL Timezone (HAL Typefaces)
EK Roumald (Erkin Karamemet)
Brondi (LinoType)
Narly OT
Kuenstler Script
EB Garamond

IMAGES BY FRKO

WORDS BY COLLIER MEYERSON

BITCOIN NEEDS A REBRAND





THE CULTURE OF BITCOIN IS OURS TO DEFINE

You know "The Bitcoin Guy." He's a 27-year-old white Harvard dropout from Brookline, Massachusetts perpetually reclining in a $700 ergonomic desk chair with his feet—adorned by holey white athletic socks—atop the dining room table. It's always late where he is, 2 am, 3 am, the dark hours. In 2019 the Bitcoin Guy was eating soylent, but body positivity impacts him too, and now he's back on San Francisco burritos. He buys the burrito during the day when he has to move his car, but waits to eat it until he's back at his computer during the dark hours. He's the only one who can understand the market, and oh, he'll mansplain bitcoin valuation, and mining and the Bitcoin Network to you in such a condescending way you'll never want to ask again. Like the boogeyman he haunts our dreams, but what if he wasn't real?

A Pew study from April, 2023 finds that while Bitcoin Guy is most likely young and a guy: 41% of men 18–29 years-old say they have engaged with the digital currency, as opposed to just 16% of women.

But he doesn't totally fit the image of some white guy in some old socks watching the stocks. The same Pew study says that overall, 21% of users are actually Black, 21% are Latino, 24% are Asian, while only 18% are white. Perhaps even crazier, Black users are more likely than their white counterparts to say they've been active in the past year.

Sure, he's a guy, but he's not a *white* guy. Already we're busting up some stereotypes: you don't have to be white, to be in the bitcoin club. Let's keep going, because if we can poke holes in this behemoth bitcoin bro, chomping late night Al Pastor from his perch in San Francisco's toniest neighborhood, then the stereotypes begin to lose power. And with the revelation that Bitcoin Guy isn't real, one thing comes into stark relief: the culture of bitcoin is ours to define. The Bitcoin Guy? He's ours to create.

In order to do that, we have to understand why we think of this "Bitcoin Guy," in the first place. Why is it this stereotype that's got a foothold in our collective consciousness? Why is *this* guy our bitcoin fantasy?

It starts with the people who seem incredibly hyped about it. Elon Musk's Tesla bought up $1.5 Billion worth of bitcoin a couple of years ago. Mark Zuckerberg tried, and failed, to make his own cryptocurrency. Those guys don't wear a google glass and walk around in frayed cargo shorts (in public) but they sure do invoke the legions of tech bros who do.

A 2019 Medium article discusses the phenomenon of bro culture inside of tech and argues that the culture is derived from "brogrammers." Fewer than 1 in 5 graduates of computer science are women, according to Girls Who Code. A 2018 book called Brotopia excoriated Silicon Valley's predominantly white, male sexist culture drawing from reports history and wretched diversity reports. That blockbuster book, along with the

IT'S NOT UP TO BITCOIN TO SHAPE ITS IMAGE BUT RATHER, US. IT'S UP TO THE PEOPLE WHO HAVE ALREADY FOUND IT.

emergence of #MeToo, spurred an industry-wide identity reckoning. But it didn't last long.

Some incremental changes were made. Money was donated by men, organizations for seed funding for women were created. But, according to the New York Times, "...women still get just 2 percent of venture capital funding and Black founders get 1 percent, where the largest tech companies have made negligible progress on diversifying their staff, and where harassment and discrimination remain common."

All of these ingredients make up a recipe for the grossest, most toxic culture you can imagine. One that doesn't give priority to the many other perspectives that exist, outside of the Soylent swigging dude who leaves his holey socks on during sex. And not only does it erase a legion of bitcoin users, the image actively turns people off. The Bitcoin Guy isn't just some annoying specter, he's become a gatekeeper, a deterrent, an obstacle to people who want to engage. In order to create a bitcoin community that's inclusive, widespread and welcoming to anybody who might want to invest, it's time to think of another mascot.

So, the rebrand. We know that the power brokers inside of bitcoin's larger universe might be predominantly white and men, but the users, or, "miners," tell a different story. And if these users are already bucking a system with tech bros at the top, then perhaps an even more diverse group might find the currency, if a tiny bit of effort was made.
It's tricky. *Bitcoin is decentralized, there is no comms department. Actually, there's no department for anything, because there's no company.* There are no employees. It's not up to bitcoin to shape its image, but rather, us. It's up to the people who have already found it, and industries outside of tech, who have interests in bitcoin's future, to evolve past the *Bitcoin Guy*. For all of us. For the whole of the world. We need to think about a new mascot, one that's compelling enough to rewrite the narrative of who bitcoin is actually for. (Everyone)

My humble suggestions:

Let's tap the fashion industry first, since they know about a rebrand, they do it every season. Jay Z x Gucci x Bitcoin. For one night and one night only, SSense lets you purchase clothes through bitcoin at computers set up at the Soho House pool. Move on to some men of the people. Think Bernie x Bitcoin t-shirt mashups. Have the squad's chicest, Ilhan Omar and AOC, go stump for bitcoin's makeover to their constituencies. The look of bitcoin, after all, is "the people."

Let's encourage the TikTok girlies to take it on:
Bitcoin Girl Summer, Bitcoin Fly Girls. Bitcoin against rats.

Tell bitcoin fans Julia Fox and Emrata to have an honest, raw conversation about the contents of their digital wallets. What else is a podcast for?

The truth is that we don't need one replacement for Bitcoin Guy, we need many. We want to hear from all the bitcoin users (well except one, you've had your turn, sit down). If you're reading this and you don't have old New Balances and a Google sweatshirt on, I'm talking to you. Join bitcoin, or come out of the closet as a bitcoiner. Save the world, be a spokesperson.

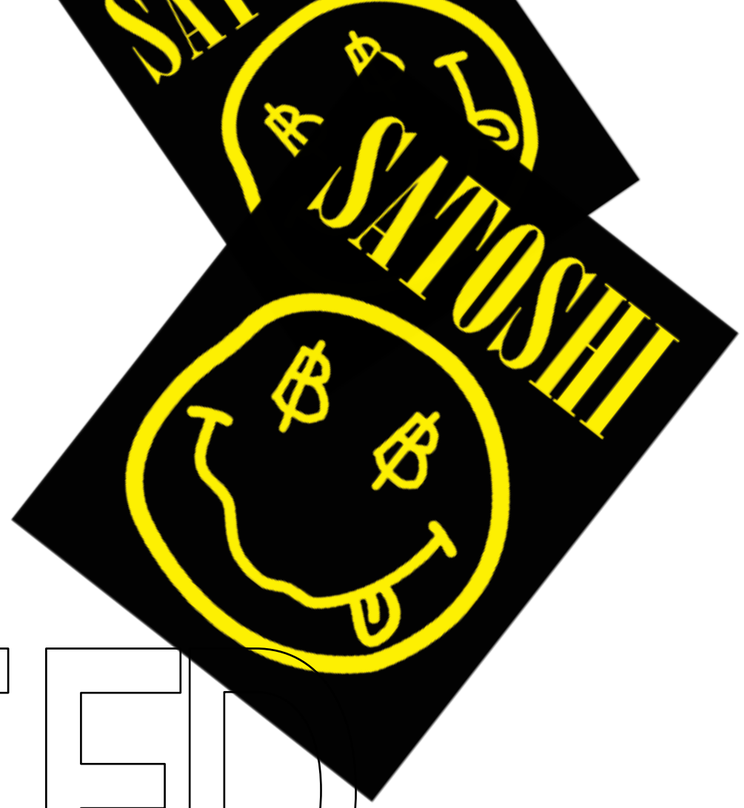
Collier Meyerson is a writer living in New York City.

BITCOIN GIRL SUMMER

strobo

WORDS BY EMILIA PETRARCA

WHO CREATED BITCOIN?



IT'S BETTER NOT TO KNOW

“HOW CAN MY FACE BE MORE IMPORTANT THAN THE SOUND?”

Underground Resistance member Mike Banks (a.k.a. Mad Mike)

Have you ever watched an episode of *The Masked Singer?* It’s this musical competition show on Fox that moms love. The premise: a handful of mostly hasbeen celebrities don fuzzy, elaborate, surreal-looking costumes that conceal their identities—a wide-eyed frog, a rose-cheeked piglet, the Sun—and perform in front of a panel of judges. While the contestant’s goal is to win the singing competition portion (their identity is only revealed when they are eliminated) the judges and at-home-audience have their own, unofficial mission too: use the performance and a handful of clues to figure out whose belting pop hits from underneath a giant pig head.

Each week as it’s revealed that gasp it’s former child rapper Bow Wow under that frog head or *holy shit* former boy band idol Nick Lachey donning the pig snout, or *oh my freakin’ god* LeAnn Rimes *was the sun!?* millions of people care anew about celebrities they haven’t thought about in decades. They might even throw one of their songs on a Spotify playlist, catapulting them back into relevance. So powerful is the allure of mystery.

In 2014, a *Newsweek* writer claimed to have discovered who created bitcoin, seemingly ending a years long head scratcher that had captivated (and then consumed) people since someone named Satoshi Nakamoto published a white paper, Bitcoin: A Peer-to-Peer Electronic Cash System in 2008. Alas bitcoin gained a foothold in the world, people wanted to know who they were. Were they a scientist, an analyst, a coder, someone who worked in the financial world or an economist? Were they AI? Who is this person who launched bitcoin onto the world (and who, by owning so much bitcoin, at one time, was one of the richest people in the world.) suggesting who the person (or people) behind the name was. The *Newsweek* reporter identified him as a physicist living in California; after the article was published, journalists camped outside of the guy’s house until, finally, the alleged father of bitcoin wrote a statement denying it, full stop. (In the interview he called it “bitcom,” as proof he was so unfamiliar with what it was.) There are still theories and YouTube videos and Reddit threads offering up other candidates, (including Elon Musk), we still really have no idea who is behind that whitepaper and despite that, or partially due to that, bitcoin still remains a cultural and economic force. Nakamoto’s refusal to reveal has given currency, one of the oldest and most familiar things in the world, a new life, cultivating a sense of mystery, subversiveness, and collectivity that traditional economic institutions could never.

There’s power in anonymity. Frank Ocean put it best, when he said, “the internet made fame wack and anonymity cool,” and disappeared. It seems unintuitive to wave off getting credit for creating something revolutionary or world-changing or even just cool, but the desire to conceal one’s identity is almost as intuitive as the desire to create it. Nakamoto, whoever they are or whatever they are, is following in a long line of artists, writers, performers, and designers, who created something and chose to cloak themselves in a shroud of mystery. By looking at those other examples, across disciplines, outside of just bitcoin, there’s insight into what’s gained by refusing to be known.

Not all instincts to obscure one’s identity are noble. (There’s such a thing as “good” anonymity and “bad” anonymity (to get away with a crime), explains John Griffiths, co-author of an essay called “The Renaissance of Anonymity,” “but there are other people who, in the past, may have had opposing political views, and so they had to protect their identity,” he continues. “Perhaps they were the ‘wrong’ sex, race, or social status to speak about such things. Regardless, “anonymity gave them the freedom to say what they thought needed to happen to protect society, while protecting themselves from being burnt on a pyre.”

When Voltaire published *Candide* in 1759, he did so anonymously, so he would be free to ridicule religious structures, governments, armies, and other powerful entities in its pages. Some might consider talking shit about celebrities the modern day version of this, to bullying and the spread of misinformation if deployed carelessly—but it certainly earns fans. The anonymous celebrity gossip account @deuxmoi has gained a huge following on Instagram by soliciting blind items from its now 2 million followers. We still don’t really know who is breaking all this news (though last year, one journalist made a compelling case that he’d identified the women behind the account) and fans follow along breathlessly.

As a creator, anonymity can take the burden off the individual by creating a sense of a collective voice. Folk music, for example, “implies some kind of collective authorship; it’s composed by the folk,” explains Griffiths. If no one author can be identified, a work becomes easier to share and participate in—and can be attributed to multiple different people at once, even if they don’t actually exist. The English virtual band the Gorillaz, for example, were originally two people posing as four. The Blue Man Group has cycled through a number of different players over the years. And who knows how many members comprised the Guerrilla Girls, an anonymous group of feminist female artists devoted to fighting sexism and racism within the art world.

“The Guerrilla Girls’ anonymity allowed them to say things that they could not have said without sabotaging their individual careers,” says RJ Rushmore, a writer who focuses on street art, graffiti, and public art. It also gave them supposed power in numbers. “Any woman in the New York art scene in the eighties could have been a Guerrilla Girl—or, maybe not, but you couldn’t prove it, right?”

Fashion designer Martin Margiela, has remained anonymous throughout his career, prefers the collective creative process to the cult of the individual. “While working as a team, you push yourself forward and move outside the boundaries; it’s a great thing,” his team once said. Anonymity was the entire brand ethos. Everyone in the Maison Martin Margiela atelier, Margiela himself included, dressed in uniform white lab coats. Models’ identities were also often concealed with face masks and tape, and clothing tags were left blank. “As much as all this rendered him invisible it made his house stand out as anti-fashion,” writes fashion critic Jeremy Lewis. The brand offered an “antidote” to the “conspicuous glamor” of the 1980s in the form of staunch minimalism.

Collective ownership can challenge any corporate enterprise, not just fashion. The members of Underground Resistance, an anonymous musical collective born out of Detroit, Michigan in the 1990s militantly rejected the commercialization of techno by wearing balaclavas in public, refusing to be photographed, and never licensing their work to labels. “They approached it in a very specific, very strategic way, with an awareness of how the music industry treats blackness as a commodity,” says Alexander Iadarola, a music writer and UX designer based in Brooklyn. “They tried to go against the grain of music industry exploitation, which is about cult of personality, and instead prioritized this idea of black collectivity and self-determination in the face of racial capitalism.”

In a documentary on the group, Underground Resistance member Mike Banks (a.k.a. Mad Mike) asks the question: “How can my face be more important than the sound?”

In our society, the face is a commodity, and so when a public figure decides to withhold it, it can be seen as a radical, almost anticapitalist act. Rather than promote their work, some artists would prefer to let it speak for itself, whatever that means. “I’m still very interested in testifying against the self-promotion obsessively imposed by the media,” says Elena Ferrante, the pseudonymous Italian author. “This demand for self-promotion diminishes the actual work of art, whatever that art may be, and it has become universal. The media simply can’t discuss a work of literature without pointing to some writer-hero. And yet there is no work of literature that is not the fruit of tradition, of many skills, of a sort of collective intelligence.”

The irony, of course, is that Ferrante said all this while promoting her work. Anonymity makes great fodder for conversation. Anonymity often goes a long way to help bolster one’s public image, even if that’s not the reason they choose to be anonymous (and it rarely is.) “By providing less of a scaffoldingfor people, or less of a story, people can make their own,” adds Rushmore. In this way, anonymity can be a successful form of myth-making, or spectacle. Some might simply call it a PR stunt. For celebrities like Kim Kardashian, who proved with her “anonymous” 2021 Met Gala look that she will always be impossible to miss, it can be an assertion of cultural power. She transcends anonymity. But for others, anonymity becomes the core of what they create. People spend their entire lives and careers trying to figure out who figures like Banksy or Satoshi Nakamoto really are, and are happy to. “The mystery is so much better than whatever the truth is, and I don’t want that ruined because, at this point, anonymity is a part of the art,” says Rushmore.

Daft Punk

Would Daft Punk, Deadmau5, or Marshmello have been as famous if they didn't wear such recognizable masks? Could they have cultivated such an image of "edginess" without them? Stefanie Kiwi Menrath, author of *Anonymity Performance in Electronic Pop Music*, concludes that, "altogether this self-stylisation as 'radically anonymous' served as an effective marketing tool for the whole scene—producing an 'enigma' of anonymity."

Anonymity doesn't just service the person who creates, there's a benefit for the person who is listening to the song, or reading the novel, or wearing the Tabi shoes, or yes, buying bitcoin. Take the most famous hidden figures in electronic music, a genre that prioritizes the crowd experience (versus pop which often prioritizes the idolization of the individual artist). By donning costumes that make them appear less human, artists like Daft Punk, Deadmau5, Marshmello, Zomby, become mere conduits for their work. "Looking at robots is not like looking at an idol," Guy-Manuel de Homem-Christo, a member of Daft Punk, has said. "It's not a human being, so it's more like a mirror—the energy people send to the stage bounces back and everybody has a good time together rather than focusing on us."

Satoshi Nakamoto has taken a similar approach with bitcoin, which is not owned and operated by a single authority figure, like a bank, but exists rather via a decentralized, collective digital ledger called the blockchain. (An approach that could be considered libertarian or anarchist.) Iadarola compares Nakamoto's role within it to the meme of Homer Simpson dissolving into the bushes. "It's less about the person and more about the network, or this sprawling technical infrastructure," he says. "Bitcoin is self-sufficient, and beyond a single person's control. It's almost animistic—like this energetic horse, or an animated, energetic force that is not human, but resembles aliveness."

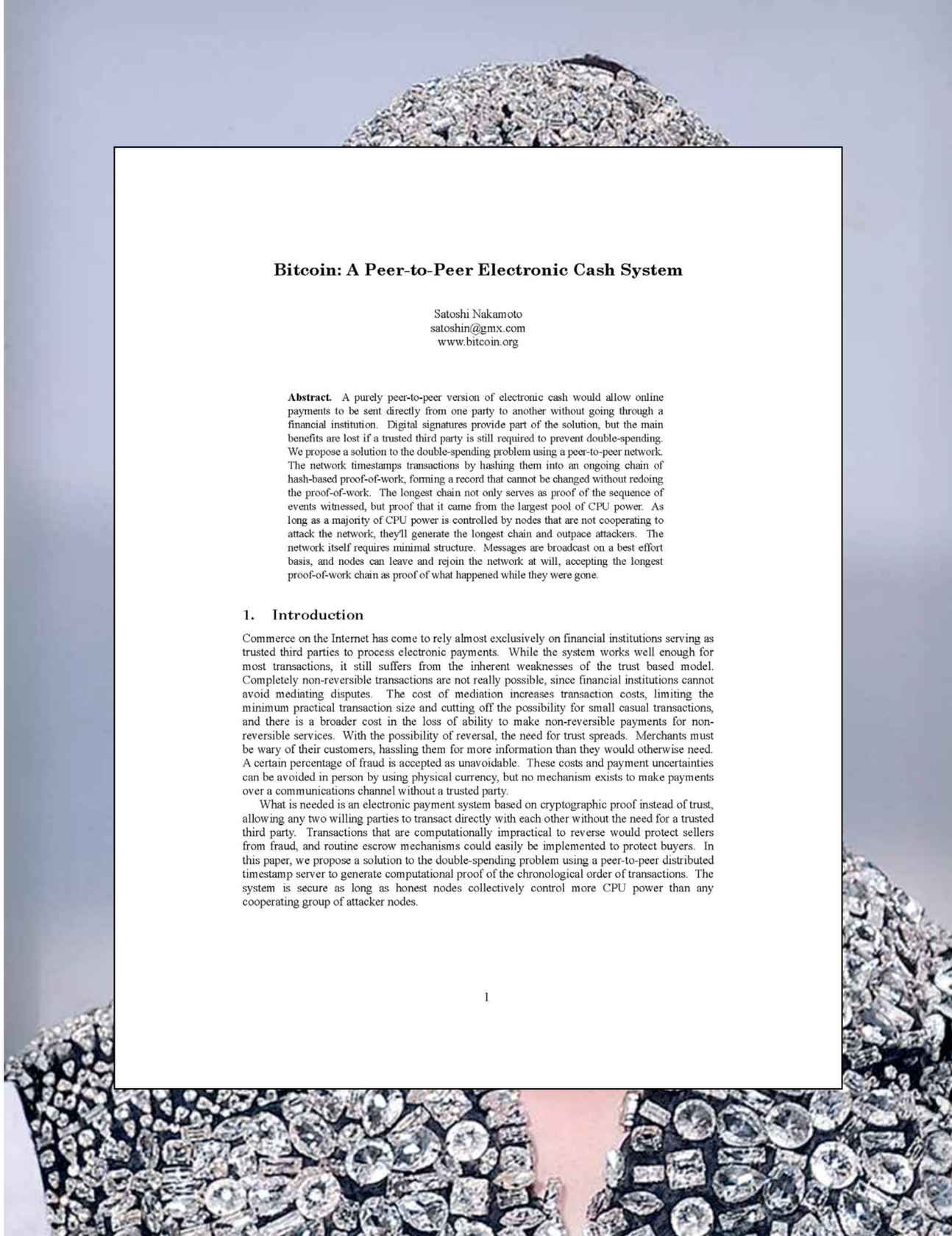
Bitcoin miners keep the blockchain going, but anyone can create a new bitcoin address, or the bitcoin equivalent of a bank account, and no personal information or credit check is required in order to do so. Your bitcoin transactions can be completely anonymous if you want them to be. No one has to know what you're buying, when you bought it, and how much you paid for it, or your financial history. (Though it is a public ledger, you're still leaving breadcrumbs, though just harder to follow ones.) Bitcoin is not backed by a bank or a government or a country or one single entity. In a world where privacy is increasingly rare—our faces are recognized, our data mined, and our identities frequently stolen—untraceable purchases have immense appeal for the average person, not just criminals. If someone told you that your recent pharmacy run for hemorrhoid cream didn't have to haunt you for the rest of your life in the form of targeted ads, wouldn't you be interested, too?

Emilia Petrarca is a Brooklyn-based freelance writer covering fashion and culture. She previously worked for *New York Magazine's The Cut,* and her work has since been featured in *The New York Times, T: The New York Times Style Magazine*, *The Wall Street Journal,* and more.

"IN OUR SOCIETY, THE FACE IS A COMMODITY"

THE BITCOIN WHITEPAPER PUBLISHED OCTOBER 31 2008 UNDER THE PSEUDONYM SATOSHI NAKAMOTO

TO THIS DAY THEIR IDENTITY REMAINS UNKNOWN



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

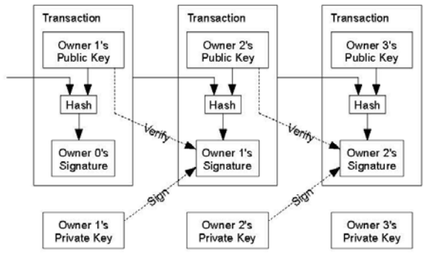
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

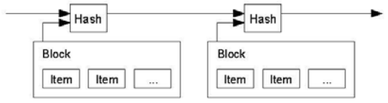


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

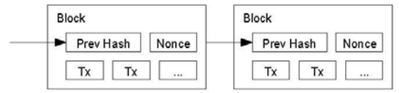
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

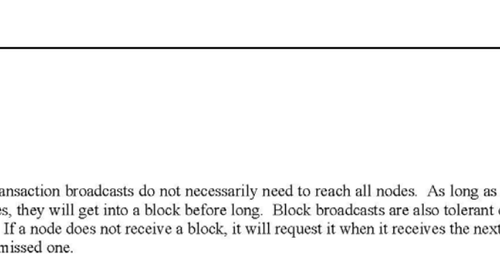
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

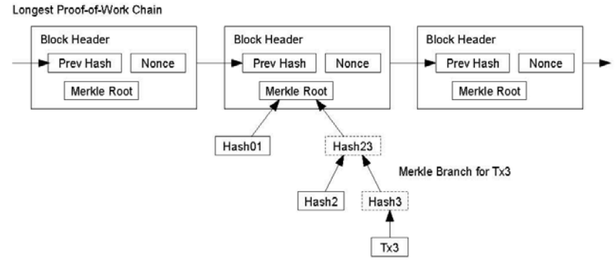
Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

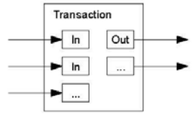
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

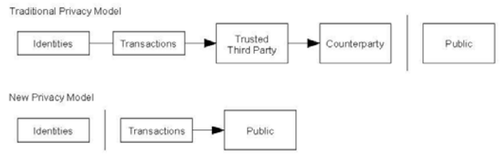
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

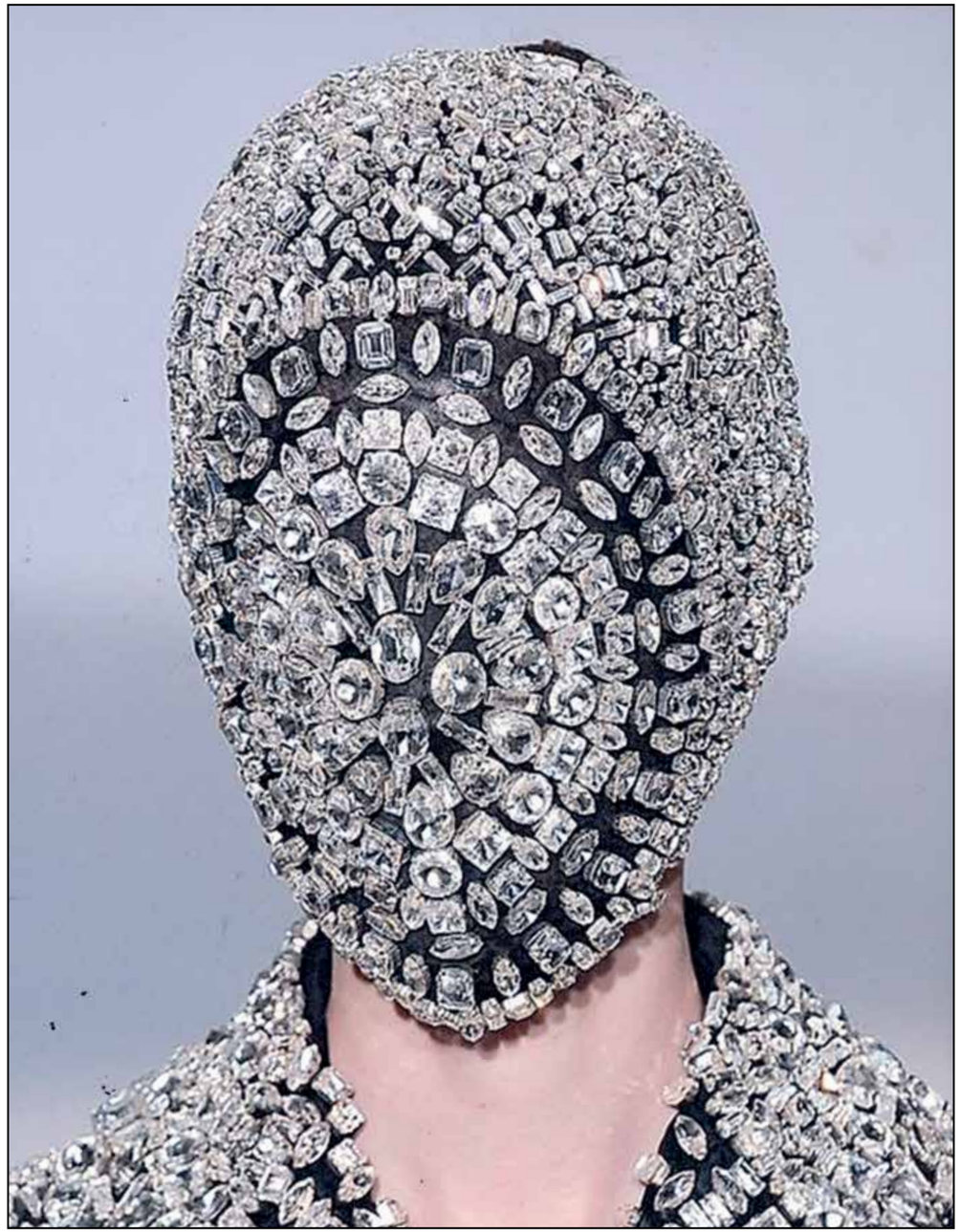
Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

8



Martin Margiela: Runway - Paris Fashion Week Haute Couture F/W 2012/2013

THE
BIG
BANG

JANUARY 2, 2009.
THE DAY BEFORE THE FIRST
BITCOIN WAS MINED


JANUARY 3, 2009.
THE DAY THE FIRST
BITCOIN WAS MINED
BY F0OD.XYZ

BAD FINANCIAL ADVICE

IMAGES BY SHUHUA XIONG

FIVE

WEIRDEST CURRENCIES EVER

The way we use money might have stayed the same, but actual money —or what's considered money—has had more reinventions and eras than Taylor Swift. From ancient clay tablets to credit cards, it's shapeshifted based on the technological advances of the time, and the needs of the people using it. But it wasn't always just rocks, paper or plastic, money has taken on some wild forms as it's evolved.

WORDS BY CHRISTOPHER WALKER

01 TULIPS

'Tulip Mania' engulfed 17th-century Holland during the Dutch Golden Age. Though not an official currency, tulips were highly prized, with some even traded for goods and services. At the height of the craze, a tulip bulb could allegedly cost as much as a house. Often cited as an allegory for speculative bubbles, some historians believe the tales of economic fallout may have been exaggerated, drawing from satirical poetry of the era.

02 FISH

Salted or canned - fish has a long history as currency. The Domesday Book documents eels as a way of paying rent in Medieval England. Barrels of salted cod were used for *settling accounts* in 17th Century Newfoundland, Canada. And in more recent times, cans of mackerel are widely reported as being used as currency in some modern day prisons.

03 SHELLS

Shell money has been documented all around the world. Since they were *easy to carry around* and *durable,* they functioned well as currency. They became symbols of power and wealth and some even wore their shell money as necklaces.

04

WHALE TEETH

Considered *precious stores of wealth* in Fiji, whale teeth were also used for important social *transactions*. Usually the bigger and older the tooth, the higher the value.

05

PORCELAIN TOKENS

Porcelain gaming counters were used for *small transactions* in some parts of 19th century Siam (modern day Thailand). Money anthropologists (such as Graeber) have noted local casinos who issued the counters sometimes went out of business and even sent a town crier to tell the locals to redeem them. The widely-accepted commodities of gold or silver were used for *major transactions* instead. The parallels to certain crypto tokens and bitcoin today are quite remarkable.

BY BOB JEUSETTE AND EMMA HAZEN

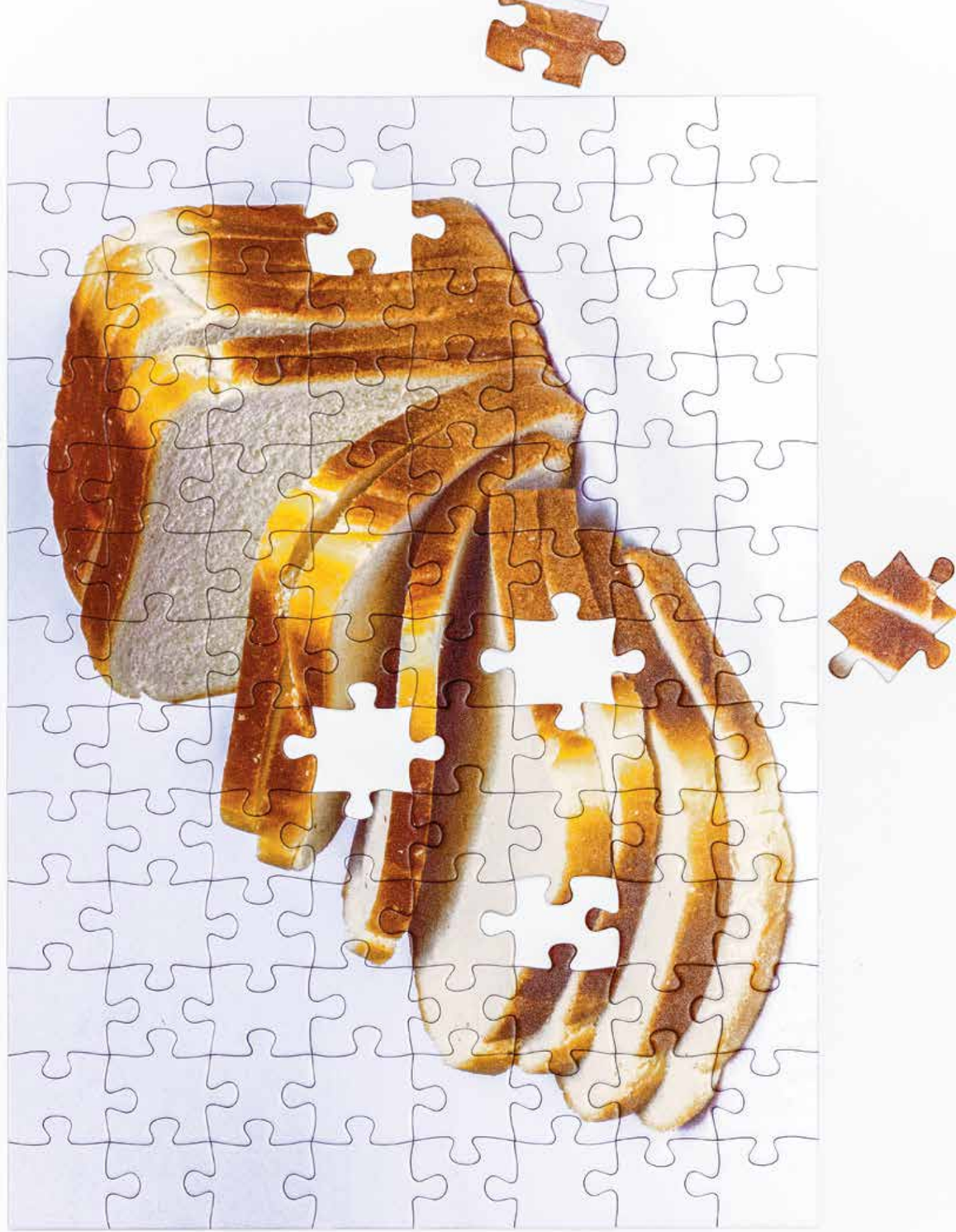
BITCOIN: RUN BY MANY

BITCOIN
IS
DECENTRALIZED

EVERYONE
ON THE
BITCOIN
NETWORK
IS TREATED
AS AN
EQUAL

NO ENTITY
OR
GOVERNMENT
CAN INFLUENCE
CHANGE
OR STOP IT

NO
MATTER
HOW MANY
BITCOIN
THEY OWN




BITCOIN · DIGITAL CURRENCY · PEER TO PEER · MONETARY SYSTEM

IMAGES BY STEVEN MONTINAR

INTERVIEW BY MALCOLM SMITH

BANKSY AND BITCOIN

Artist Steven Montinar explains how bitcoin gets its value.

The problem and the promise of bitcoin stems from the same place: the currency is volatile and inherently unpredictable; its value is dictated by how much people want it. The ups and downs of the bitcoin market can be a deterrent for the casually curious, and an obstacle for those who want to level up to novice investors. How is it possible to feel safe buying bitcoin when market trend watchers point to the up and down of the markets as proof of the dwindling allure of the currency? Sludging through the technical terms — a total headache. But, if we think of bitcoin like we think of a sneaker accruing value on the resale market (like the Apple Inc. Omega sports Apple Computer sneaker, designed as a free giveaway gift at a National Sales conference in the 1990s, now worth $50K) or the resale value of tickets to Beyonce's Renaissance tour, or, any piece of art, its unpredictability, begins to make sense.

Steven Montinar, a 24-year-old, New York based mixed media artist, has been working as a client liaison for Sotheby's since 2022 where part of his expertise is used to assess the how art is deemed valuable, and how it finds relevance in society, but he was personally familiar with the process, from the art side of things, long before he started this job. In 2020, Montinar's work, "Koupe Tet, Boule Kay," was acquired by The Whitney Museum of American Art. While, at the time, there was controversy around the acquisition process (more on that later,) Montinar is enough of an expert to understand why, and why it was bigger than the price tag. BREAD asked Montinar to walk us through the acquisition of his own work, as a way to understand bitcoin, by understanding the eternally in-flux currencies of the art world.

Let's begin in the most obvious place: how do you define value?

Coming into art, I had two revelations. The first one was informed by concept and the second was in the form of model. In that primary perspective of an art life, the concept changes the art's relevance. The way we manipulate, hold, and share our practice changes how the art interacts with the world. So with art, it's seen as a monetary unit alongside it being an external representation of yourself. As well as a hobby. As well as an emotional release or a coping mechanism. Art can exist as a trend, as a monument, as money, but it's all these things wrapped into one.

For me, value comes down to motive. And my motive with my artwork has always been visibility. Or maybe the better word is accessibility. My value in my practice comes through accessibility. Who does it reach? How did they reach it? How much access did they have to it? In a larger sense, accessibility is also how art retains value. It all depends on what aspect of the audience you are using to create value.

But what about the opposite of that, which is scarcity. You live in New York City where fashion is life. Everything from vintage designer clothing to sneakers sway in worth depending on availability. How much of a factor is scarcity in determining the value of a given artwork or product?

At the end of the day, art is an experience. It is an individual experience no matter how massive an audience it gets. If you can only experience a body of work by purchasing it, holding on to it, or showing up to an exhibition, those fleeting moments of exchange become imperative to its value. At The Met and MoMA, for example, I have a collection of writings that are specifically in the special collections library. The purpose of the library is to collect these written works and preserve them. And it's not just books, but pamphlets, newspapers, flyers and articles. They are things that are paraphernalia in the present but artifacts over time. So there's a scarcity not because it's not in demand, but a scarcity of who wants to archive, who wants to preserve it.

That same line of thinking applies to collectors. If someone walks into an auction house and they like the work, and are willing to spend, then they are also saying I'm buying this to archive. Archiving is the thing that works against scarcity but also works with scarcity. Who is archiving it correctly to extend time to create legacy? Scarcity becomes really important to value. The work never depreciates, it just doesn't exist anymore. An artwork that is ruined doesn't necessarily lose its value. Bansky, at Sotheby's London in 2018, shredded one of his pieces in auction. It sold for $1.4 million. And that raised a ton in value because it's the only one that exists that way. [Titled "Love Is in the Bin," the painting was resold by the anonymous collector in 2021 for $25 million, a new record for the artist.] Scarcity drives demand as well. It drives a demand in the audience, an interest in a specific audience, or it can change the audience that becomes interested in it. Now it's a collector's item or a special edition.

All art is born into the world at a specific point in time. How does its social value factor into its overall commercial value?

So what we're talking about is the time period. How important was that work in that specific time, and how does that importance or value translate outside that era? The Bauhaus movement and Dadaism are the first things that come to mind, especially when it comes to artistic design practices. Dadaism was specifically anti-art but over time it became high value artwork. It is the exact opposite of what was supposed to happen in its present time. Social value parallels this current. During specific cultural movements or world events certain work becomes more prominent, and more valuable, because of the larger audience. This happens at galleries a lot.

How so?

At the height of a movement, they start collecting certain artists. During the Black Lives Matter movement, there was a resurgence in wanting black artists. After that, there was the Stop Asian Hate movement, and the art world shifted to more Asian artists. Right now, the social value of artwork exists in this overlap of current trauma and future legacy. It's all about, how important will we deem that aspect in time?

The secondary market truly tells you what the world wants because the secondary market is run by the public. The primary market is based on a gallerist's interests — *I like this, it resonates with me.* It all starts with their interests. The secondary market is based on who is buying what and why they are buying it.

Have you experienced that with your work?

My first major acquisition was by The Whitney for "Koupe Tet, Boule Kay," which I made during the Covid-19 pandemic in March 2020. The reason that artwork became more visible was, one, the pandemic helped the art world develop into a virtual space. People who would not normally be looking at other people are now looking at these people through social media and online interventions. On top of that, trends in the art market are very real. I'm a black artist making work about the black experience, specifically my own black experience. The environment [art exists in] can recontextualize a work. So in the space of me existing as a black body online making art that represents my feelings about situations happening, like the Black Lives Matter movement, people start spreading your message.

I made "Koupe Tet, Boule Kay" before I knew where it was going to go. I needed a project where I could take time, concentrate, and block out some of the world. I gave it to Printed Matter, [an independent publishing nonprofit dedicated to artists.] They were doing a free downloadable archive for Black Lives Matter protesters. I originally put that into the world as a free tool to go out and protest. The Whitney got a hold of it. At first I thought it was spam. But them having my work created a very interesting reaction to my practice. Now I had backing, which brings us into the world of money, with bitcoin,

"BANSKY, AT SOTHEBY'S LONDON IN 2018, SHREDDED ONE OF HIS PIECES IN AUCTION. IT SOLD FOR $1.4 MILLION. AND THAT RAISED A TON IN VALUE BECAUSE IT'S THE ONLY ONE THAT EXISTS THAT WAY."

where things have to get backed. In the art world, you're always backed by an audience. Being backed by an institution holds a lot of weight, and you can use that weight to raise the prices of your work, or to raise your exposure in the art market or to find new opportunities to further grow. And that's what was happening.

But then things stopped short. With that show at the Whitney, of all the works they acquired, I was the only one they told, to my knowledge. The rest of the work they just took from this virtual space. Initially the piece was acquired for free since the Whitney was collecting freely circulating materials. After the backlash, the museum gave each artist $1,500. It became an issue. How do you navigate the virtual art market? What is a picture? Is a picture the original — if the picture's original — if you obtained that image? Do you own the original?

Technology has certainly changed how art is created, but also how we allocate value. Digital art can now be sold as NFTs. In 2021, an artwork by Beeple, which exists only as a digital file, sold for $69 million at an auction through Christie's. How will the relationship digital art has to the marketplace evolve in the years ahead?

Anything that becomes popular or relevant all comes down to how you package it. It's the same with social media. Every couple of years there is a new platform but it's the same thing as before. The issue with NFTs, and digital currencies similar in nature is that I personally believe they are packaged wrong. It's packaged wrong because it's hard to understand. For someone who doesn't mind learning all about bitcoin, about the different forms of it, its value and how its value shifts, there's no problem. But most people are not like that. It's all packaged wrong. The evolution of our visual art is further understanding its digital packaging.

As an artist, your work is all about recontextualization and infusing an object with new meaning. In the future, will the way value is assigned change? Will its packaging look different?

With currency, with value, with art, and the future value of products, the idea of simplifying the packaging of value becomes more important. With bitcoin, the value becomes harder for people to understand. The idea of a decimal point of value throws people off. It becomes confusing. The unsimplified visual of it makes you not want to understand it. There is all this context people miss because it is not packaged for them. It takes a certain audience to want to sit and ingest all this information.

It doesn't take a special person to understand this, but the better you package it, the larger the audience. In comedy, the same jokes are reused all the time but there is a difference in delivery and a difference in packaging that makes people more understanding or susceptible to receiving the message.

This interview has been condensed and edited for clarity.
Malcolm Smith is a writer living in New York.

Cash App

THE EASY WAY TO BITCOIN

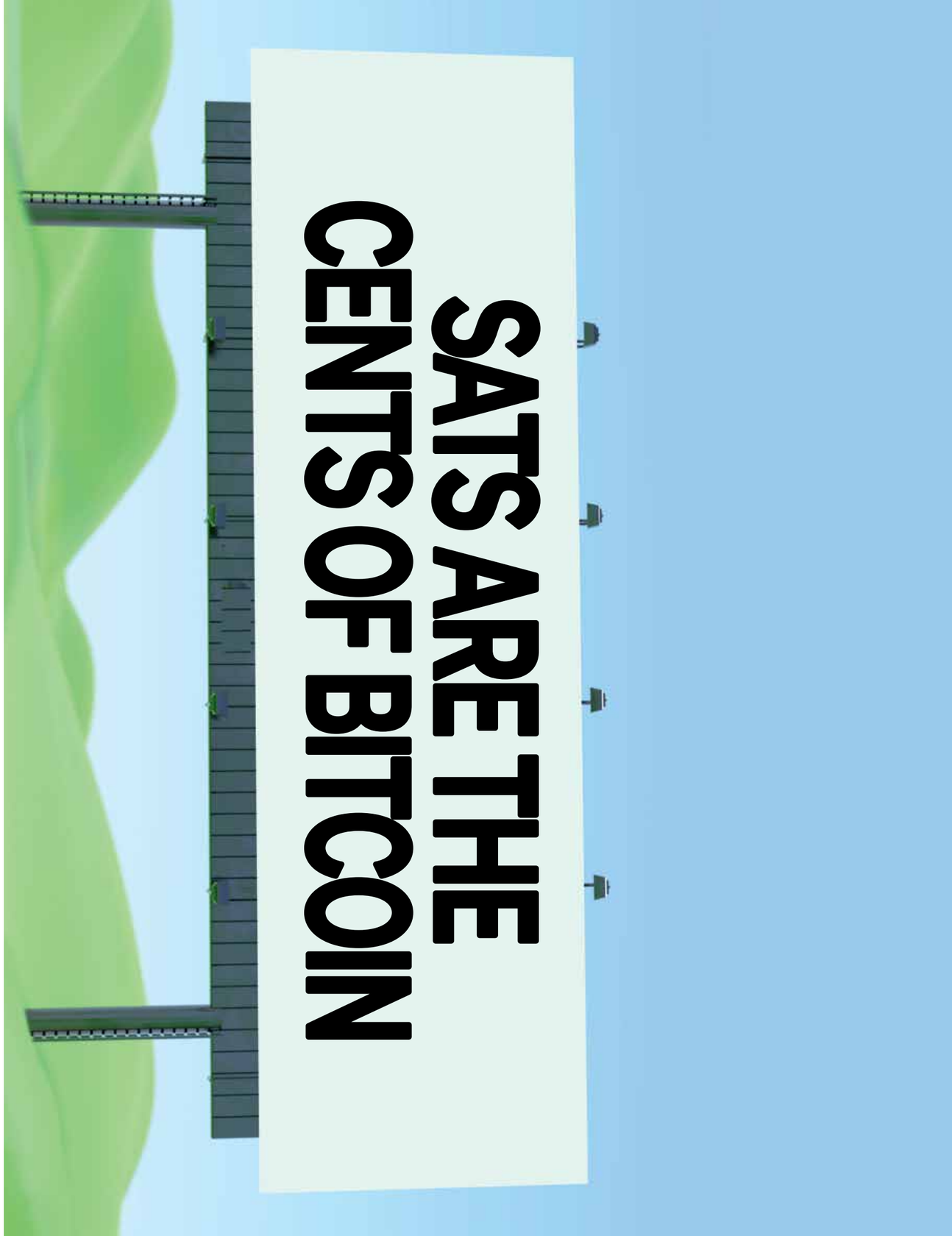
Buy, sell, send, receive,
and spend bitcoin anytime.

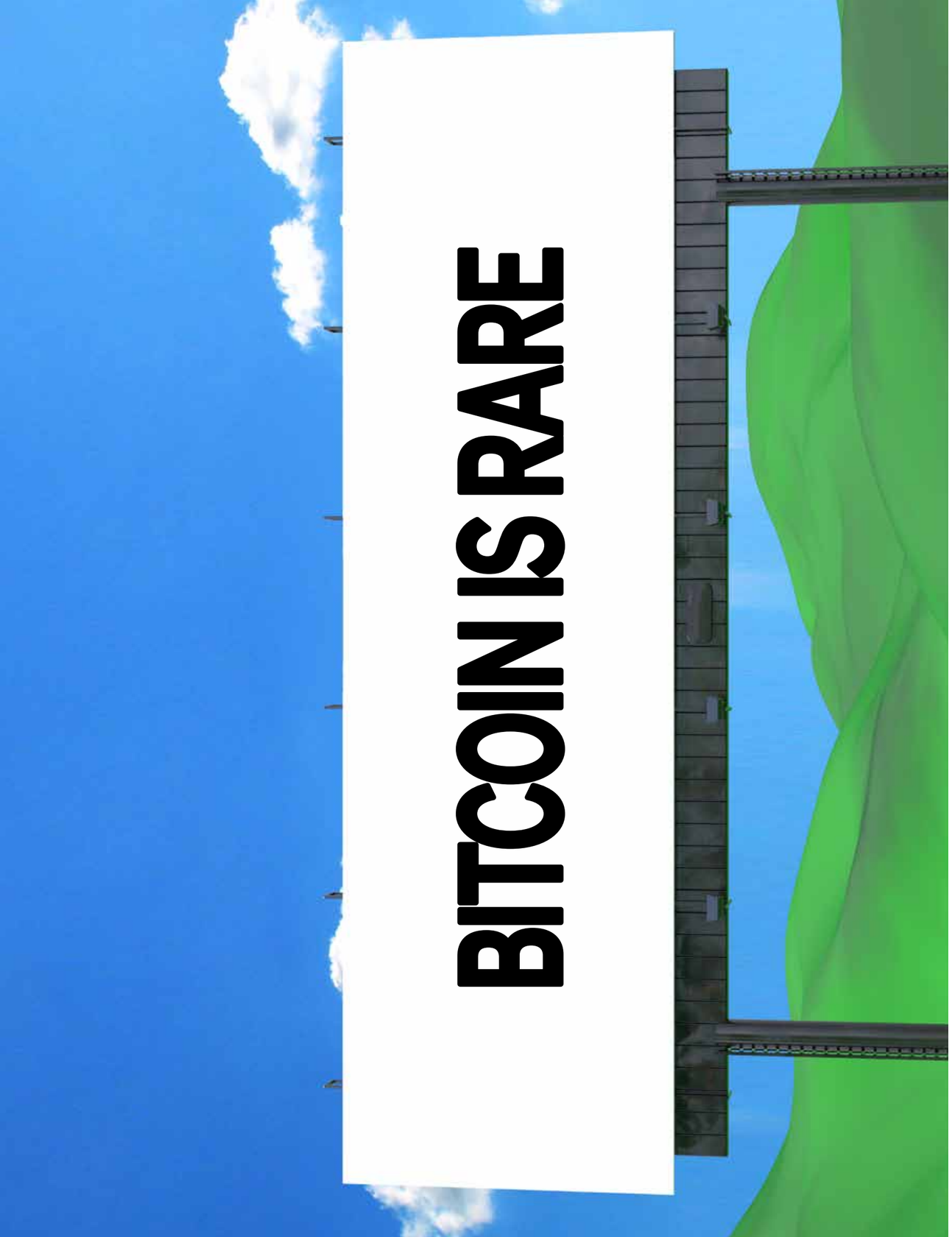
Download Cash App

BITCOIN FACTS

A CASH APP ZINE

ONE BITCOIN = 100 000 000 SATS

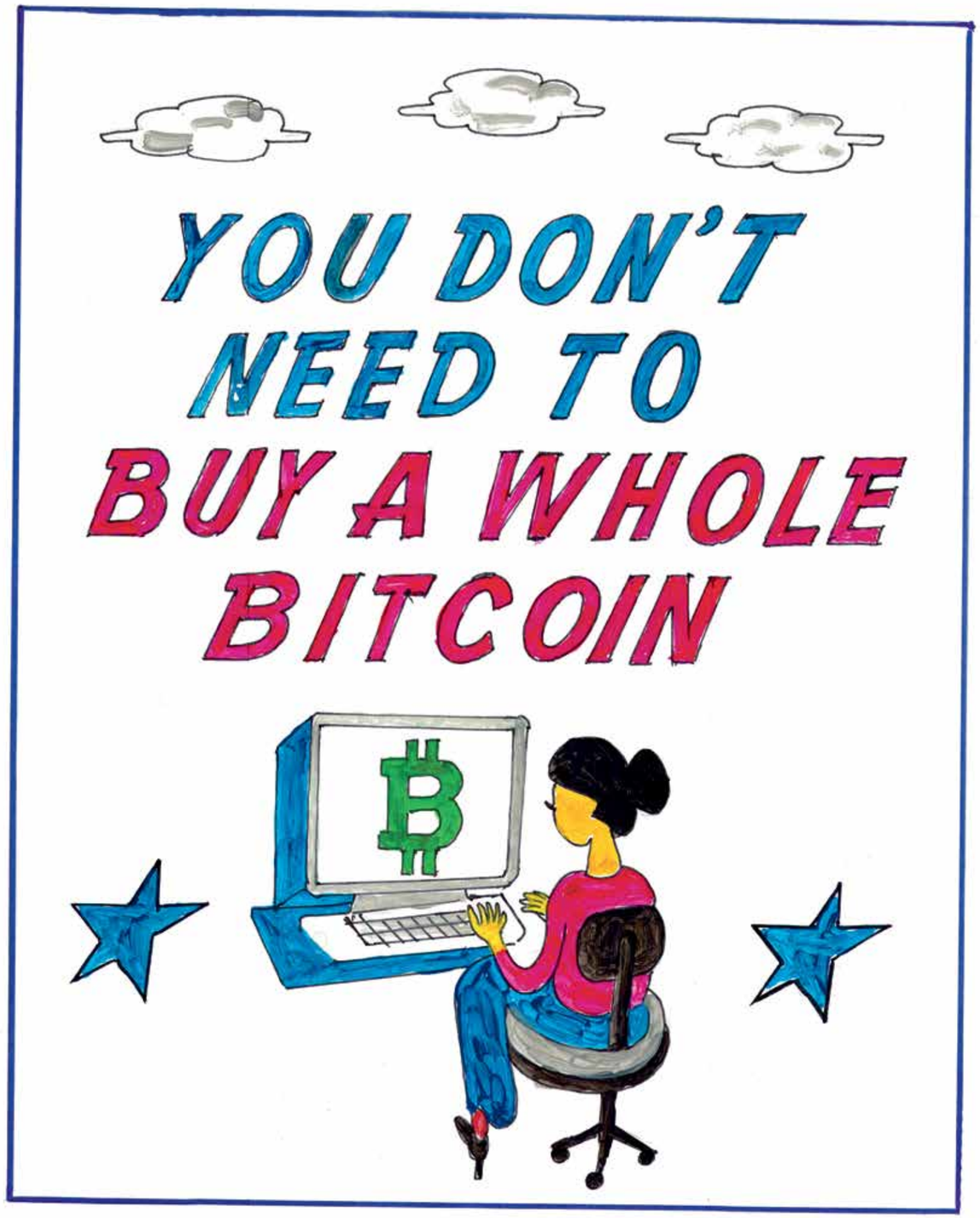


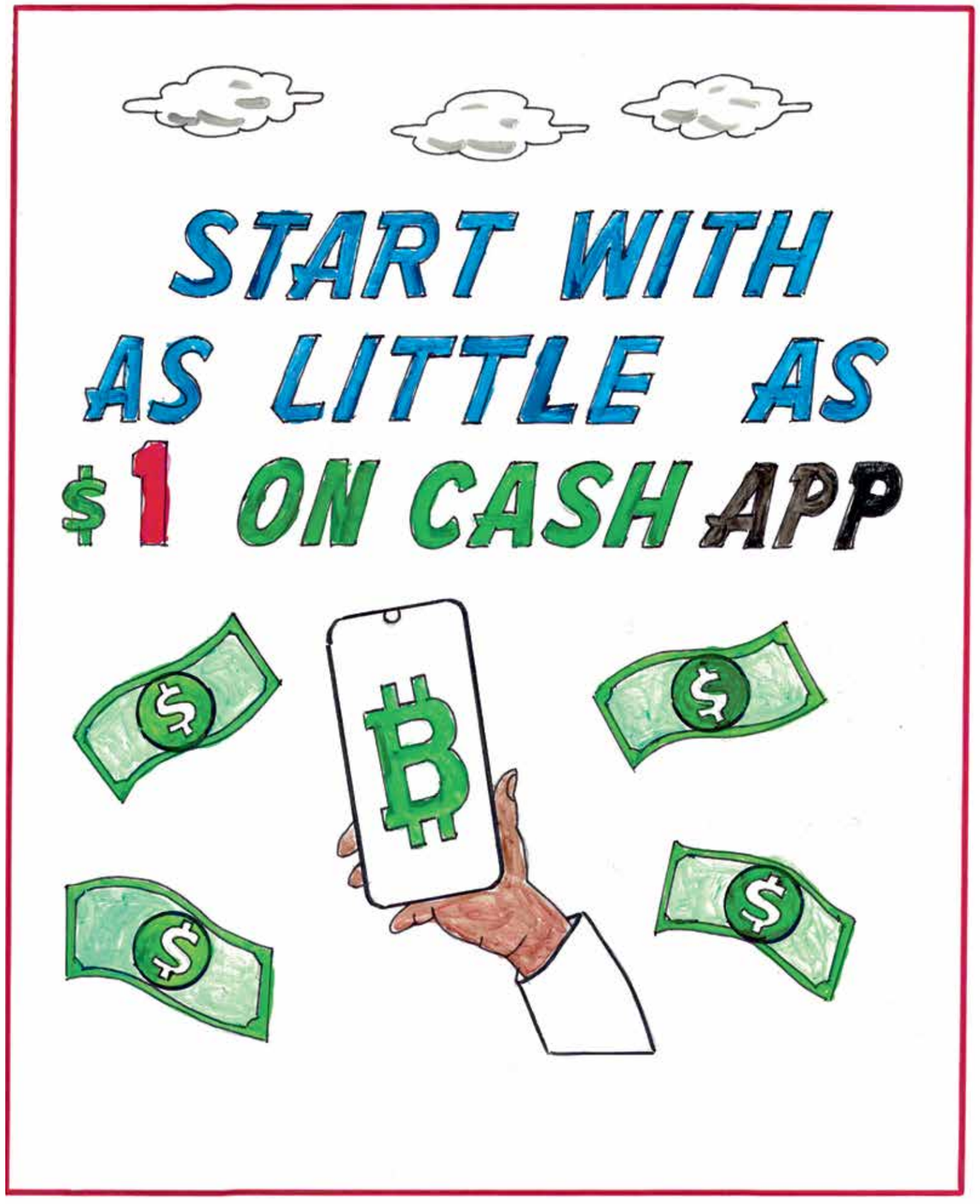


THERE WILL ONLY EVER BE 21 MILLION BITCOIN

IN EL SALVADOR BITCOIN IS THE OFFICIAL MONEY

BY CEVALLO BROTHERS





WORDS BY MARGARET RHODES

YOU CAN MINE BITCOIN WHERE?

ON A CORNER OF PRIME WILLIAMSBURG IN BROOKLYN, THERE'S A NEW AGE-Y BATHHOUSE WHERE PEOPLE SOAK IN HOT TUBS PLUNGE IN COLD ONES, AND DRAPE THEIR LANGUID BODIES ACROSS SAUNA AND HAMMAM BENCHES. UPSTAIRS, GUESTS WEARING ROBES SIT ON A HEATED PATIO AND ORDER WAGYU SKEWERS AND HOUSE-MADE VODKA INFUSIONS. IT'S LUXURY OF THE OLD-WORLD VARIETY, WHICH MAKES IT SURPRISING TO LEARN THAT IN THE BOWELS OF THIS TRENDY DAY SPA, CO-OWNER JASON GOODMAN IS RUNNING A BITCOIN MINE.

If you're familiar with bitcoin mining — or even if you've just seen a photo of a mine, typically a warehouse sprawled across tens of thousands of square feet and filled with shelves of ASIC computers and fans stacked to the heavens — you might wonder how this is even possible. Turns out, bitcoin mining isn't the sole province of large-scale blockchain companies. Some enterprises are small — like hidden-in-a-closet small. "Any building that requires energy — which is every building — can be used for this," says Goodman, who belongs to a widely distributed network of "home miners," or not-industrial-scale miners that have set up shop in unexpected places (including a ... volcano.) Since he launched the operation in 2022, the pools in his spa are heated by 12 computers that run around the clock, verifying bitcoin transactions and earning a little bitcoin in return. Goodman recalls the day they first switched the system over from the original heaters to the mining system. "We did it live; there was no shutting down the bathhouse." Even though he knew it would work, he says he was glued to the floor in the pump room, heart racing. "I was staring at the temperature display, going, *Oh my god, I lost a degree. Oh wait, coming back up,"* he says. "It does feel a little like magic, because they're just computers and they're heating our pools." Here, Goodman explains exactly how his whole operation works, and why it's an eco-friendly way to mine bitcoin.

For a spa-owner, you must be constantly explaining how bitcoin mining works. What's your trick for breaking it down?

I tell people that the miners are like bitcoin's military. If you have something of tremendous value, it needs to be defended. The U.S. dollar also has an army, but it's a real army with guns. Gold requires huge vaults to defend it. This is a more peaceful defense, where all the miners work in aggregate to run algorithms and solve puzzles that actually make blocks in the blockchain. The miners — the army — create an enormous wall of computing power around the Bitcoin Network, so that nobody can climb over it. That's why nobody's ever successfully attacked the Bitcoin blockchain. When Satoshi Nakamoto invented bitcoin, they designed it for an adversarial environment. They knew that if it worked, then people would try to hack it. So there was a question around how we could make bitcoin impenetrable to attacks, but still decentralized, so there's nobody in control. Anybody can join this army. Anybody can do this in their house.

And Bathhouse has enlisted in this army?

We're contributing a few soldiers to the army, and we're getting our little share of bitcoin out of it in return.

What gave you the idea? Are you a crypto guy?

I'm not a trader. I don't want to try and figure out how to be good at that. I'm more of a tinkerer who likes to build things. But in 2020, during the early part of the pandemic, I became very concerned about huge inflation. It was very obvious what was going to happen: The government was going to print more money, so monetary inflation would occur. I started wondering, *how am I going to protect myself from inflation, and how bad is it going to get?* I started looking into bitcoin. Not to flip it, just to understand how mining works and how decentralization works.

Then I came across a podcast from this guy named Marty Bent, who worked with a company called Great American Mining. They basically show up at oil fields, where there are chimneys with flames coming out, burning off natural gas. These flares coming off the chimney are wasted energy. Bent hooks up a generator and just runs bitcoin miners right there with wasted energy. That really opened up my eyes, because energy is used and energy is wasted. Whether you like it or don't like it, the economies of the world depend on oil and that oil is going to be drilled and that flare gas is going to be flared. But what Bent showed is that you can capture that energy and do something with it.

Which is a big deal, because one of the central concerns around bitcoin mining is how much it contributes to greenhouse-gas emissions.

Right, so if you can take something that is waste and turn it into something that can create value, it's such a huge win. It takes real engineering, and those guys had to go make those relationships at the oil fields, and then actually show up and operate it. I was very impressed. Then I started thinking: I spend 99 percent of my time running a bathhouse, and we have to buy energy to keep the spa running. It takes energy to make pools hot. We have two heated pools at the Williamsburg location, and I have 18,000 watt electric heaters on both of them. If I can run miners using the same wattage, I already know that miners produce heat as a waste product. They take electricity, send electrons across their circuit boards, mine bitcoin with it, and then that energy gets turned directly into heat. So if I could capture that heat and channel it into the pools, I would be using the same amount of energy as before, and I would also be mining bitcoin.

It sounds like a great idea in theory. How did you know it would actually work?

I ran a test, and bought two miners and put them in an immersion tank filled with dielectric fluid, which is like an engineered mineral oil that cannot conduct electricity. You could drop a toaster oven in one and then stick your hand in the fluid. Then I used an indirect hot water heater that's lined with a copper coil that has hot oil flowing through it. The water fills the tank, and the copper coil heats the water. All I did was turn the miners on, and I got a lot of hot water. Once I proved that it would work, and that I wasn't losing heat or energy in the process, I said, *okay, I have two pools I want to heat, and they each need 18,000 watts.* The miners are 3,200-watt devices, so I bought 12 of them, set them up, and the energy from those devices transfers to the heat exchangers for the pools.

We're about to open a new location in Manhattan, and it's a much bigger space. We're going to heat all the pools there with bitcoin mining too, as well as all of the heated hammams. They have these big beautiful marble slabs you can lay on, and they're all heated. The scrub rooms also have heated walls. So we're doing all of that with bitcoin. But for right now, it's just the two pools in Williamsburg.

Now that the miners have been up and running for about a year, how does this change your business? Are you funding the new bathhouse with bitcoin?

No, we're a really small-scale operation. Our holdings aren't nearly big enough to do that. I'm doing this because we can, and because it helps us recover our energy costs. The energy I was already going to buy, I'm now getting some portion of that back in bitcoin holdings. Also, I believe that bitcoin is good for the world and for our society. The more small-and medium-scale miners there are, the more decentralized and distributed the Bitcoin Network becomes. Then bitcoin itself becomes more robust.

And the people who come to Bathhouse, do they know the water is heated through bitcoin transactions?

No, but people never knew how the pools were heated in the first place. They're not thinking about it. I mean, I wouldn't go to a spa and think about how the pool is heated. And you can't see any of the mining at work. The computers live in the back of our office. I have two tanks, and the tanks connect to a heat exchanger that connects to the pool's plumbing. The chlorinated pool water pumps through one loop, and the water that comes out of the heat exchanger from the bitcoin miner pumps through another loop. The water does not mix. Imagine a pipe inside a pipe.

So people aren't bathing in bitcoin water?

Nope. It will not turn you orange.

This interview has been condensed and edited for clarity.
Margaret Rhodes is an editor and writer who covers design and consumer culture and lives in New York.

WITH RAUL LOPEZ

BTCFW

BITCOIN FASHION WEEK

JUST LIKE BITCOIN, LUAR IS FOR EVERYONE.

LUAR FOUNDER RAUL LOPEZ
HAD A LOFTY GOAL:
PRODUCE AN AFFORDABLE
LUXURY BAG EVERYONE COULD AFFORD.

HE WOUND UP CREATING THE ANA,
AN ICONIC BAG FOR THE PEOPLE.

795,000 SATS / $265

795,000 SATS / $265

795,000 SATS / $265

795,000 SATS / $265

795,000 SATS / $265

“I WANTED TO MAKE A BAG THAT I COULD AFFORD.”

IMAGES BY STEPHANIE SPECHT

WORDS BY ELISE CRAIG

WE ACCEPT CASH CREDIT BITCOIN

The wildest, wackiest, meatiest, most surprising ways people use bitcoin.

There is still a vibe out there in the world that bitcoin is a sketchy currency that people either sit on forever, hoping it will continue to grow exponentially, or use for sometimes questionable purchases they don't want tracked. But that's not actually true—the universe of uses is so much bigger and more interesting, and also more common, than reputation dictates. Bitcoin can be used for almost anything, from the most mundane exchange to the most extravagant purchases. People use it to buy their lunch at Chipotle, or a Bentley at a luxury car dealership. NBA players can get paid in it (technically, players convert their paychecks to bitcoin, but you get the drift.). Exotic dancers prefer it to crumpled dollar bills, dentists accept it, and local farms will let you buy pork chops with it. If there's something you need, a good to purchase, a service to pay for, there's probably a way to use bitcoin for it. To prove how expansive the world of bitcoin is, we tracked down some of the weirdest, coolest, smarties, most unexpected ways people used their bitcoin—and none of it was even close to illegal.

GET PORKCOIN

BERTHOUD , *CO* BRYCE

At Star View Farm, we raise a little bit of everything, as naturally and organically as we can. Beef, pork, lamb. Australian Lowline cattle, which are sometimes referred to as a miniature angus. We also raise British Whites, and Wagyu. The thing that made me take to farming was the quality of the food. The pork chops don't get dry. The turkeys we raise have so much flavor; so juicy and tender. We sell our meat all different ways, but for the most part, people give me a call or text me to see what's on sale. We offer whole pigs and sides of pork, and sides of beef and beef quarters. A lot of people buy them and share them with their families.

We started accepting crypto in 2014. They said it was a sinking ship, and I thought we could take it into port and do something with it.

But no one wanted to spend their crypto. It took about five years until the first person used bitcoin. They put down a deposit on a side of pork. And that person timed it so perfectly. He sent it over, and within an hour, the price started to go down.

Soon, people started asking to pay in crypto more and more. Now as much as 15 % of our sales are in crypto. It's brought in a lot of new customers–a lot of people you'd never expect to show up to a farm to buy something. The crypto people come in groups, and say. "Hey, can we see the animals?" That's the thing that draws them in; the fact that you spend bitcoin is the bonus on top. One person, we call him the Crypto Pirate, he shows up when he thinks the market is going to turn, and spends $50 to $400 at a time. He's one of those people who brings friends along. I think they're serious city people. When they come over, we have baby animals going on. And they love it all. I get a lot of enjoyment seeing the joy on people's faces. Especially city people who have never touched a sheep or a lamb and then they're just exploding with happiness. A couple of them are genuine good, hearted nerds. He knows I'm a nerd too, and we usually have good nerd conversations while enjoying the animals.


It's organic, It's Bitcoin
The Fresh Natural Bitcoin Here
Bitcoin c'est bio et bon

SANTACON IN NEW YORK

MIAMI, *FL* MIKE AKA "MUZZ"

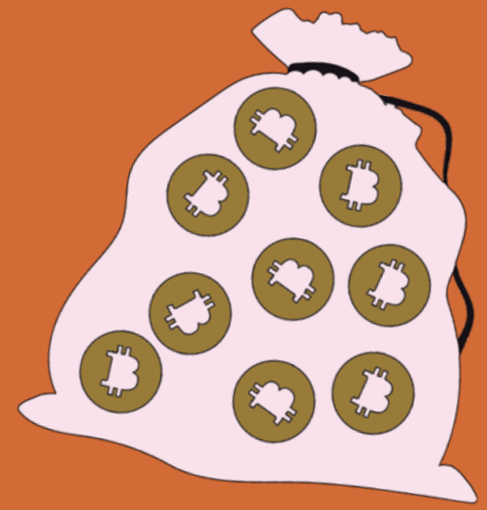
I used to own a tiny bar on the Lower East Side in Manhattan, called Old Man Hustle. We started taking bitcoin early on, in 2013, when there were maybe five businesses in all of Manhattan that accepted it—one flower shop, two bars, one guy renting luxury cars. We did it through these very primitive early websites. And if you were a bitcoiner at the time, you usually strolled through just to see what was going on.

And then one day, it was SantaCon in New York.

Everyone gets up at the crack of dawn, dresses like Santa Claus, and goes and drinks all day.

For that one day, you will see drunk Santas from 8am until close.

This particular SantaCon, I'm in the bar, and it's 11 am and snowing and miserable. There is no business. And then all these Santas start coming in. And all of them are paying in bitcoin. Every drink, every tab. We did hundreds of dollars in bitcoin sales, at a time when a beer was $6. By four p.m., it was a full-on blizzard, and we had to close and send everyone home. But it was a very rare day.



KEENE, *NH* MANDRIK

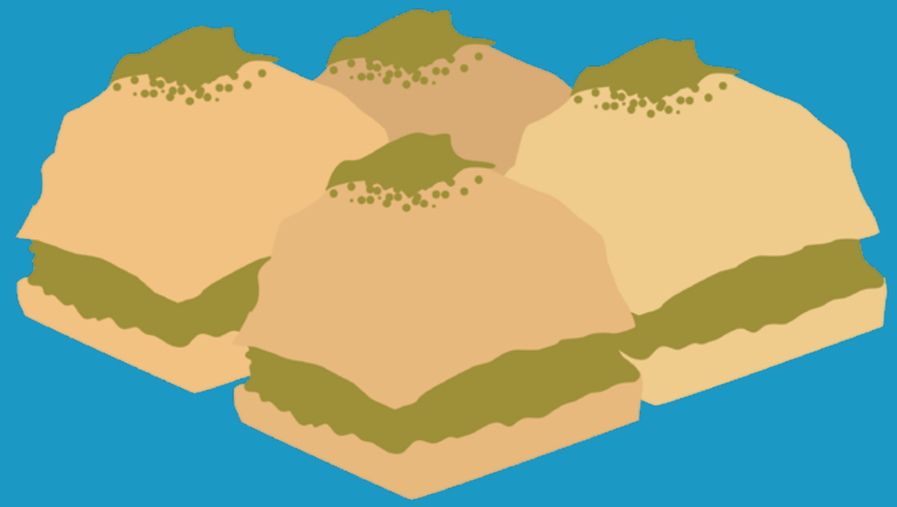
My family is Greek, and I started working in my dad's diner when I was 11. I ended up hanging out with all the women in the kitchen. I learned to bake from my mom and my grandma, and baklava was the first dessert I learned how to make. In my teen years, I was a LARPer, and I would accept in-game money for baklava. That's my origin story.

In 2011, I lost my corporate job and moved to New Hampshire as part of the Free State Project, small-to-no-government types who move there for more freedom in their lives. I didn't want to go back to a corporate job, and just wanted to give something a try. I'd been selling baklava online since 2009, via Etsy, eBay, and crappy websites, so decided to do it full time. If I failed, whatever.

I started advertising on a Free Talk Live, a libertarian radio show based in New Hampshire. A guy named Roger heard it, and asked if he could pay for a tray of baklava in bitcoin. That tray went for 14 bitcoin. As 2012 went on, I was getting more and more baklava orders. At first, I was cashing it out. But over time, I really started to see what made bitcoin special. Eventually, I wanted to earn 100 percent of my income through bitcoin.

In 2012, I decided I was not going to take on some corporate job. As other NH freesters got into bitcoin, I started to be like, "Hey, I'll do personal chef work or clean your house. I literally scrubbed toilets for bitcoin. And I started selling sandwiches at a big festival in the white mountains called the Porcupine freedom festival. People paid two bitcoin each for the sandwiches. And some of them paid in physical bitcoin rounds a guy named Mike Caldwell made in 2011. They're brass coins, with a sticker on the back you could peel off to reveal a mini private key that gave you one whole bitcoin. I had a stack of them, and I saved one. I consider it my family heirloom. Like a restaurant hangs the first dollar on the wall. I'll pass it onto my kids. It's a reminder of where I started.

Interviews have been condensed and edited for clarity.
Elise Craig is a freelance writer and editor based in San Francisco.



The Most Modern Baklava

exists only online

"I CONSIDER IT MY FAMILY *HEIRLOOM*. LIKE A RESTAURANT HANGS *THE* FIRST DOLLAR ON THE WALL. I'LL *PASS* IT ONWTO MY KIDS. IT'S A REMINDER OF WHERE I STARTED."

CALL:
1 (855) 5 - BREAAAD
Cash App

CALL:
1 (855) 5 - BREAAAD
Cash App

BREADZINE.COM