Title: Desperately seeking Satoshi; From nowhere, bitcoin is now worth billions. Where did it come from? Andrew Smithset off to find Satoshi Nakamoto, the mysterious genius behind the hit e-currency
Source: ***Sunday Times (London, England).*** (Mar. 2, 2014): News: p16.
Document Type: Article

http://www.sunday-times.co.uk
Full Text:

it's late 2013; a converted brewery in hip east London, with bare-brick walls and double-espresso musk. For days, online forums have churned with plans for this unlikely 800-strong agglomeration of trend-seekers, geeks and the merely curious to converge from all corners of Britain, and they look a little shocked to be here, as if the focus of their shared fervour only now seems real.

The focus is bitcoin, the bizarre electronic "cryptocurrency" that appeared out of nowhere at the start of 2009 and slowly, strangely, began to attract followers. With no clear reason to be worth anything, it was traded for pennies at the end of the first year, but after two years had achieved dollar parity, then more and as the price began to levitate, extraordinary things happened around it, with exchanges and odd frontier-style businesses grown, robbed, scammed as if in some free-market libertarian fantasy. Vexed economists cried "Bubble!" and predicted the end more loudly with each turn of bad news, after which bitcoin's value would crash, then simply continue its rise, until by the end of 2013 a single "coin" would cost you $1,000. Some investors predicted it would eventually reach $1m; others that it would be spam by the end of this year.

Yet, the most remarkable thing about bitcoin is the robustness of its construction: the fact that this free-floating network, designed to mimic the properties of gold by producing a maximum of 21m coins, "mined" by anyone prepared to download and run a complex algorithmic program on their computers, has through all these machinations remained consistent and intact. Pointedly beyond control of any state or bank-like central authority, bitcoin behaves more like an organism than an institution. But it works, and may only just have begun to reveal itself.

"The first six times you think you understand bitcoin," one awed veteran cryptographer will tell me, "you don't."

Indeed, mathematicians and programmers speak openly of this novel system being a kind of masterpiece, produced by a genius named Satoshi Nakamoto, who dreamt its protocols to life and then disappeared without trace.

So who is this Satoshi? That's just it: we don't know. The only thing we do know is that before he melted away at the end of 2011, someone mined a million bitcoins, now worth around $500m -- and that this someone is likely to have been him.

Where did he go and why has he refused credit for his creation? Is Satoshi Nakamoto a genuine recluse, or fearful of establishment persecution? Sceptics dismiss his work as the most ingenious Ponzi scheme ever devised, but right now it's possible to believe almost anything.

I'M FAR from the first to wonder who Satoshi might be, and the list of suspects is long (see panel, overleaf). Two years ago a New Yorker journalist named Joshua Davis spent four months on the case and settled on Michael Clear, a gifted Irish doctoral student at Trinity College, Dublin -- possibly in league with the so-called Crypto Mano Group, led by Professor Donal O'Mahony. This suggestion wasn't far-fetched, because back in 1997 O'Mahony and two colleagues published a book called Electronic Payment Systems for E-Commerce, which could be a description of bitcoin. Davis subsequently approached Clear at an annual cryptography conference in Santa Barbara, California, and the 23-year-old denied any connection to bitcoin but then he would, wouldn't he? Not long afterwards, Adam Penenberg, a New York University journalism professor writing in the business magazine Fast Company, settled on a trio of computer spods, led by the Munichbased telecommunications consultant Neal J King, after finding a phrase from Satoshi's original outline for bitcoin -- "computationally impractical to reverse" -- echoed in one of several bitcoinylooking patent applications filed a few months before. As grist to the mill, Satoshi's bitcoin.org domain name had been registered in Helsinki just three days after the most incriminating application, and one of the trio's number, Charles Bry, had travelled to Finland six months earlier.

Implicit in both investigators' conclusions was the very reasonable thought that such elegance and depth of invention (and we'll come to this) seemed too miraculous to ascribe to all but the rarest individual. At this stage, I'm inclined to agree.

WHAT IS BITCOIN?

Bitcoin is the first working example of a "cryptocurrency" -- electronic money that exists only as computer code

It is actually more like gold than money, because it has been designed as a finite resource. Only 21m bitcoins will ever be minted, or "mined". As of last month, 12.3m were in circulation Bitcoins are traded from one person to the next directly over the internet, with no need for banks or clearing houses, and stored in your digital wallet

You can buy and sell bitcoins from online exchanges such as MtGox.com, Ripple.com and Bitstamp.net

From June 2011, Bitcoin's value soared as word emerged of its use on "dark web" sites such as Silk Road, where its near-anonymity encouraged the trade of illegal drugs and weapons

After Silk Road was shut down, a predicted collapse in value never came. By the end of last year, each coin was worth a cool $1,000. It now trades at around $500

SATOSHI APPEARED out of nowhere on November 1, 2008, when a post to a rarefied discussion forum called the Cryptography Mailing List stated matter-of-factly: "I've been working on a new electronic cash system that's fully peer-topeer, with no trusted third party." It was signed with the pseudonym Satoshi Nakamoto. Thereafter, he honoured academic tradition by reverting to "we" for the remainder of a summary that began: "Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution."

Cryptographers, who had been trying and failing to create something like this for decades, had seen it all before. Many had concluded that such a system was impossible, and some were openly dismissive of this interloper's scheme. Yet, carefully and patiently, Satoshi answered their questions and the truth dawned that his scheme could work.

Two months later, on January 3, 2009, Satoshi mined the first 50 bitcoins, a tranche now known to fans as the Genesis block. Nine days later, the first transfer of still-worthless bitcoins was made to Hal Finney, one of the first and most distinguished cryptographers to interrogate The Creator and begin to understand. A month later we got the first glimpse of Satoshi's intention when, in a characteristically pithy post, he wrote: "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."

Computer programmers, or coders as they prefer to be called, would later be shocked to find a headline from The Times embedded in the source code like a message in a bottle. Dated January 3, 2009, it read: "Chancellor on brink of second bailout for banks". Satoshi wasn't a mere technician: his motivation was political.

Work went on behind the scenes at bitcoin.org, with a team of enthusiasts assembling to fix bugs and add features and refinements, all overseen anonymously over the internet by Satoshi. As bitcoin began to take off, indications were that he was alarmed: when acolytes welcomed news that Wikileaks would accept donations in bitcoin, their leader responded with a rare show of ardour in a post to the bitcoin discussion forum: "No, don't 'bring it on'. The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to Wikileaks not to try to use bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage."

A week later, on December 11, 2010, he added darkly: "It would have been nice to get this attention in any other context. Wikileaks have kicked the hornet's nest, and the swarm is heading towards us." The next day, Satoshi made his last ever post to the bitcoin forum and his interactions elsewhere began to decrease, until in April 2011 he made his final public statement, saying: "I've moved on to other things." By most accounts, he continued to be in touch with a few key people, such as the project's head developer, Gavin Andresen, offering advice and ideas; a ghost in the machine. But as the year wore on, Andresen claims that replies to his emails became sporadic, until in the end they simply stopped. If anyone has heard from Satoshi since, they're not saying.

EVERYTHING WE can know about Satoshi is contained within his system, and to understand that we need to grasp why he built it. Back in the early 1990s, as the online world loomed, a handful of math and computer bones saw a threat lurking in the matrix. The net brought wondrous gifts, but also the potential for state surveillance and corporate intrusion on an unprecedented scale -- and our best defence against such intrusion, they reasoned, was cryptography.

At this juncture of maths, politics and technology were born the "cypherpunks", whose early mailing list included a young man named Julian Assange. Between them they went on to establish organisations such as the Electronic Frontier Foundation and Wikileaks, and to provide "netizens" with the tools they needed to stay safe, meaning private.

Godfather to the cypherpunks was a brilliant mathematician named David Chaum, a graduate of UC Berkeley, founder of the International Association for Cryptologic Research. Scion of a wealthy family, he had introduced the study of anonymous communication systems a decade before the cypherpunks had a name. In the process of amassing his 17 patents, Chaum also produced the first workable blueprint for untraceable electronic money, which he called ecash, and was in the process of establishing the system when his Netherlands-based company, DigiCash, went bust in 1998. Because he had patented the software, no one else could use it, but cryptographers still discuss ecash admiringly.

By then, many other crypts were thinking along similar lines, as e-commerce took off. One of the glittering prizes would be the enablement of micropayments, which would allow organisations such as newspapers to charge tiny amounts for access to individual articles, offering respite from a collapsing ad-based business model.

But there was a problem. Small payments were unworkable once you'd factored in bank or credit-card charges. Micropayments would require a new electronic system, with electronic cash that could move fast and be near-free of charge. Fine, except that any such form of e-money will effectively be a number or code, and if my virtual Smithcoin is just a number, what's to stop me spending it twice? One answer -- the answer David Chaum chose -- is to have a central authority (a "trusted third party" in crypt-speak) to log transactions and police the network. But why should we trust such an authority more than a government or bank? Chaum's company went bust, and even if it hadn't, why was it more trustworthy than what we have? Why couldn't it be robbed, attacked or compromised, or profit from malfeasance? In principle, it could. But if you fix the problem by removing central authority, then who controls the money supply; who keeps and mediates the ledger of transactions? A classic Catch 22.

By the end of the 1990s, some of the finest minds on earth were working to square this circle, but no one could. When Google found a way to make online advertising pay, the commercial imperative faded and the cypherpunks retreated underground. As far as these nonconformists could see, the corporate-state complex and its central-bank lackeys would rule forever.

From this apparent void emerged bitcoin and its remarkable proof that you could tackle "double-spend" within a decentralised network. It's not clear to me that even Satoshi thought this possible when he set out, because a forum posting from June 18, 2010 reads: "[I've been working on bitcoin] since 2007. At some point I became convinced there was a way to do this without any trust required at all and couldn't resist to keep thinking about it. Much more of the work was designing than coding. Fortunately, so far all the issues raised have been things I previously considered and planned for."

Bitcoin's chief innovation is to use a concept called "Byzantine consensus" to reach an agreed version of history within the network. Roughly speaking, here's how it functions: 1. I buy a coffee in a cafe. At time of writing this costs 0.003811btc (but by the time you read this, who knows?).

2. Details of my purchase are sent to the "mining pool", where one of an army of miners picks it up and uses the complex bitcoin algorithm to check, then process it with other transactions into a "block". Once accepted by a majority of nodes on the system, a coded representation, or "hash", of the previous block is inserted, and the new one becomes part of a fixed, transparent, anonymised chain -- the block chain.

3. I opportunistically try to spend my bitcoin again, but the miners on the system treat my attempt as inconsistent with the established history and simply fail to pick it up for processing. It will die like a seed in the Sahara.

Everything real is logged into the blockchain and open to inspection by anyone, at any time. In fact, go to blockchain.info and you can watch it all happen in real time. Which is more than a little magical.

There are caveats and inconveniences. Even economists who manage to admire bitcoin as a payment mechanism question its value as a currency. If its value is constantly rising, won't we treat it like an asset and hang on to it rather than spend it? More or less seriously, depending on your viewpoint, the cryptocurrency has been shown not to be unconditionally anonymous.

THE USUAL SUSPECTS THE CRYPTO MANO GROUP A collection of crack Dublin computer scientists, led by Professor Donal O'Mahony (pictured) of Trinity College, who got together to explore the concept of e-money

MICHAEL CLEAR A doctoral student and gifted programmer at Trinity College, Dublin, hired by Allied Irish Banks to improve its currency-trading software. In 2011, at the age of 23, he was cited as prime suspect in an investigation by The New Yorker. Clear denies that he is Satoshi JED McCALEB A maverick, super-smart coder who dropped out of Berkeley and set up the MtGox bitcoin exchange, and then the more sophisticated Ripple exchange.

has since sold them, and moved on to new project to rival both -- under the intriguing title secretbitcoinproject.com

NEAL J KING, CHARLES BRY AND VLADIMIR OKSMAN An unusual technical phrase from Satoshi's bitcoin "white paper" was found in a patent application the trio filed concurrently The identity of Satoshi Nakamoto is shrouded in rumour and conspiracy theories involving everyone from the CIA, NSA and GCHQ, to Google, a cabal of European financiers or even Japanese conglomerates (SAmsung-TOSHIba-NAKAmichi-MOTOrola).

A few stand out as plausible contenders

HAL FINNEY An original "cypherpunk" and encryption expert. In 2009, he received the first bitcoin transaction -- Satoshi sent him 10 bitcoins as a test. He is now paralysed by motor neurone disease, but still programmes

SHINICHI MOCHIZUKI A reclusive maths prodigy who entered Princeton at 16 and left with a PhD at 23. He has a history of making mathematical discoveries and then leaving them on the internet for people to find

NICK SZABO Computer scientist and polymath. He developed a system for "bit gold", often seen as a precursor to bitcoin. He carefully controls what information is available about him online, and is one of the few suspects whose picture we could not trace

MARTTI MALMI Young Finn with libertarian leanings, who set up forums and helped with additional programming for bitcoin, before selling his stock and exiting the forums -- at about the same time as Satoshi Lastly, the amount of computing power required to mine bitcoin as difficulty increases and more miners join the network can be viewed as enormously wasteful. Professor Kenny Paterson of the University of London, Royal Holloway, describes the amount of computing power needed to process bitcoin transactions as "insane". Interestingly, this is one of the things that sometime-Satoshi-suspect and founder of the MtGox bitcoin exchange, Jed McCaleb, set out to improve with his Ripple project. More on him later.

SO, SATOSHI is a clever sod. What else do we know? Over his two years of (virtual) visibility, he left behind an estimated 100,000 words, most of them limited to technical discussion with followers and peers. Nonetheless, it's hard not to be struck by how stylishly he writes, with care taken in the placement of commas, choice of words. Much has been made of some obviously British inflections -- words ending with "our" rather than "or" (colour), and "ise" rather than "ize" (minimise), not to mention reference to a "mobile" rather than "cellphone" and one use of the word "bloody", as in: "Sorry to be a wet blanket. Writing a description for [bitcoin] for general audiences is bloody hard. There's nothing to relate it to."

Combining this with the fact that Satoshi's communications tended to happen immediately after UK office hours, the New Yorker's Joshua Davis not unreasonably took this to suggest that Satoshi was native to the British Isles. All the same, my own combing of the text turns up a few instances of words ended "ize" ("decentralize", "summarize"), although these are acceptable on both sides of the Atlantic. So Satoshi exists within the British sphere of grammatical influence? Maybe. Against that, his name suggests Japanese heritage and I soon find the bitcoin domain to be registered in Finland, where Martti Malmi, one of the core developers early on in the project, lives.

And of course, the closing of offices in the UK coincides with their opening in, say, California. I send an email to Michael Clear, the New Yorker's prime suspect, but get a reply saying he's under a lot of stress and can't speak.

Elsewhere Satoshi says things like: "A generation ago, multi-user time-sharing computer systems had a similar problem" And: "The Hunt brothers famously bankrupted themselves trying to corner the silver market in 1979," suggesting he occupies a milieu where mention of said Hunt brothers can be expected to draw a knowing smile rather than blank looks. A separate reference to Usenet, an early, unmediated online discussion forum, also suggests someone with a sense of history rare in your forward-facing, monomaniacal coder cowboy. Perhaps someone of a certain age.

Then there's the code itself. Professional programmers will tell you that, as with prose or speech, everyone has their own set of ticks and tendencies. Internet gossip has long suggested Satoshi's code to be clunky and unprofessional, but in 2011 a security expert named Dan Kaminsky spent four months trying to find cracks through which thieves or vandals might slip, and was astonished to fail -- an extremely rare occurrence.

"Bitcoin is a very novel system," Kaminsky explains. "It was a new implementation of a new design that had pretty profound implications if it was done poorly. In my work, you learn where to look for the weaknesses, and the first time you look at bitcoin, you think there are 15 things that are immediately gonna take it down. And then you go through the system and see that each of those things has been dealt with. What this has done is push attacks on bitcoin away from the core and into the surrounding support code."

Meaning the exchanges, or bitcoin "wallets" on unsecured home computers. So the code was skilfully written? "The core is really solid. I'd say it's better than your average professional code -- in fact significantly better. But it should be. It knows it's going to come under attack. But so far no bugs have been found. It's worked."

A fellow programmer who claims to have reviewed the source code back in 2008 claims that its consistency of style (and of some minor quirks) suggest the work of one person rather than a group. He further points out that teams working together tend to leave comments for each other, explaining what they've done so as not to confuse co-workers, but he saw nothing from Satoshi save a few terse reminders to self. A third coder claims the style suggests someone who learnt their craft in the 1970s or '80s. From a range of possible programming languages, the consensus is that Satoshi chose the purist option of C++ because it offers little by way of shortcuts, but is more predictable as a result. Also commonly agreed is an impression that C++ wasn't "his" native programming language.

THE TIDE is turning against the notion of Satoshi as a group. The trio headed by Munichbased Neal J King received a fillip when I learnt that the email address used by Satoshi -- which, remarkably, appears to remain live -- is hosted by a German-built mail service which, in 2008, was new and little-used elsewhere. Now that I better understand the workings of Satoshi's system, however, the patent applications that Professor Penenberg thought "bitcoiny" no longer look so to me. I show them to a few of my new crypt chums, who all agree: these would have no place in bitcoin. King, Bry, Oksman -- it's not them.

NOVEMBER 1, 2008 Satoshi Nakamoto posts plans to a cryptography mailing list for an electronic currency called bitcoin MAY 22, 2010 The first real-world bitcoin purchase, of two pizzas for 10,000btc. Today, each pizza would be valued at roughly $2.5m. Regrets? No, "it was really good pizza," said Laszlo Hanyecz from Florida

APRIL-MAY 2011 Satoshi posts his last statement: "I've moved on to other things." A fresh round of euro bailouts increases interest in bitcoin. Its price rises tenfold

JANUARY 3, 2009 The so-called Genesis block of 50 bitcoins is mined. Days later, Satoshi sends the programmer Hal Finney 10 bitcoins as a test -- the first transaction FEBRUARY 2011 Bitcoin hits dollar parity.

1btc now equals $1 APRIL 2013 The multimillionaire Winklevoss twins, famous for accusing Harvard classmate Mark Zuckerberg of having pinched the idea for Facebook from them, buy up $11m in bitcoin, calling it "gold 2.0"

A BRIEF HISTORY OF BITCOIN (US$) Cap Market 27 NOVEMBER, 2013 As the value of a single bitcoin reaches $1,000 for the first time, James Howells from South Wales realises he has thrown away an old hard drive containing 7,500btc

OCTOBER-NOVEMBER 2013 The FBI shuts down the drugs-and-guns emporium Silk Road, and admits it now owns 1.5% of the world's bitcoin stock. In a letter to the Senate Homeland Security Committee, it announces a change of heart on bitcoin: seems it's not so bad after all

DECEMBER 4, 2013 Bitcoin peaks, with a single coin valued at US$1,238 DECEMBER 5, 2013 Bitcoin plummets after China bars its financial institutions from handling the currency APRIL 2013 After a massive spike in interest, bitcoin peaks at $265, then corrects to around $180 a coin

SEPTEMBER 2013 An anonymous software engineer launches an "Assassination Market" site on the dark web. Allows users to anonymously contribute bitcoins to bounties on the heads of politicians and public figures

JANUARY 2014 The singer Lily Allen confesses to having once turned down "hundreds of thousands" of bitcoin in payment for a "virtual" concert, for which she wouldn't even have had to leave home

FEBRUARY 2014 Bitcoin's value drops sharply to around $500 after a flaw is discovered in the software of some wallet systems I call Professor O'mahony in Dublin and have an interesting discussion which nonetheless leaves me with a gut feeling that Satoshi is nothing to do with him, either. I now know that when he and colleagues from the Crypto mano Group wrote the book Electronic Payment Systems for E-Commerce back in 1997, e-currencies were a crypto Holy Grail. But bitcoin is different: bitcoin comes with a philosophy attached. O'mahony's interest was in micropayments more than politics, and he laughs amiably at the idea of himself or his team as Satoshi. He also surprises me by confessing that he doesn't know his young fellow Dubliner michael Clear well enough to be able to exclude him for me.

Nonetheless, the original bitcoin white paper is written in an academic style, with an index of sources at the end. I go to Wei Dai, an original cypherpunk, the proposer of a late-1990s e-currency called b-money and an early correspondent of Satoshi. When, in the first of several late-night chats, I ask him how many people would have the necessary competencies to create something like bitcoin, he tells me: "Coming up with bitcoin required someone who, a) thought about money on a deep level, and b) learnt the tools of cryptography, c) had the idea that something like Bitcoin is possible, d) was motivated enough to develop the idea into something practical, e) was technically skilled enough to make it secure, f) had enough social skills to build and grow a community around it.

"The number of people who even had a), b) and c) was really small -- ie, just Nick Szabo and me -- so I'd say not many people could have done all these things."

a sudden frisson. Szabo, an american computer scientist who has also served as law professor at George Washington University, developed a system for "bit gold" between 1998 and 2005, which has been seen as a precursor to bitcoin. Is he saying that Szabo is Satoshi? "No, I'm pretty sure it's not him."

you, then?" "No. When I said just Nick and me, I meant before Satoshi" So where could this person have come from? "Well, when I came up with b-money I was still in college, or just recently graduated, and Nick was at a similar age when he came up with bit gold, so I think Satoshi could be someone like that."

"Someone young, with the energy for that kind of commitment?" "yeah, someone with energy and time, and that isn't obligated to publish papers under their real name."

Of course! academics are under constant pressure to publish. I check Donal O'mahony's publication list to find it full of papers from 2007-9. another academic in the frame is the reclusive mathematics genius Shinichi mochizuki -- but I find his publication list for the period even fuller than O'mahony's. leading us back to who? Jed mcCaleb.

Except that mcCaleb's Ripple system, while preserving anonymity, unapologetically reinstates central authority. The CEO he left behind at Ripple labs, Chris larsen, tells me that mcCaleb was deeply disturbed by "the fact that [Bitcoin mining] burnt so much electricity," adding: "I don't think it was Jed, frankly, because Jed writes in C++ and my understanding is that Satoshi wrote in procedural C." Hmm. as we know, Satoshi wrote in C++, but in a way that suggested it wasn't his native language. Plus, would the surfy, entrepreneurial mcCaleb have presented his plan in the manner of a seasoned academic researcher? mcCaleb has all the right qualities, but writing bitcoin for free in order to profit from the mtGox and Ripple currency exchanges sounds too much like the plot of a Bond film to me.

one night while combing Satoshi's posts, something pulls me up. This will seem small to anyone else, but I spent my first 13 years in the US and am attuned to the different British/american grammatical conventions simply because I fall foul of them so often, forgetting which is which. So when I see a line that reads: "you can enter as long of a message as you like," I instantly recognise it as an americanism, because this side of the atlantic no one would include an "of".

Indeed, combine this slip with the Japanese name, Finnish-registered domain, German mail address, and it starts to suggest a pattern of systematic obfuscation aimed at throwing us offthe scent. One is tempted to further infer that Satoshi, having pointed us in the directions of the British Isles, Finland, Germany and Japan, is unlikely to come from any of these places, least of all from the first.

I contact michael Clear again. Stressed because he's completing his PhD, as it turns out, he tells me that he is very interested in bitcoin from a technical perspective, then refers me to a page of "clarifications" on which he says that the cryptocurrency's anarchocapitalist overtones unsettle him; that his political leanings are to the left. He good-naturedly admits that he is wary of journalists now, and wants this all to go away. There is no way on earth that Clear is Satoshi; nor is martti malmi, whose written English is flawless, but not in the way of a native-born speaker.

I think Satoshi is american. Hal Finney? Finney was one of the first to interact with Satoshi, who clearly had respect for him -- at one point responding to a word of praise with: "That means a lot coming from you." another, unhappier fact is that in 2008 the great cypherpunk was diagnosed with motor neurone disease, a condition he has blogged movingly about at lesswrong.com, and which progressed with cruel rapidity. as he himself has asked, with such limited time left, why would he disown his own masterwork? Which leaves Nick Szabo, who meets the evidence on every count -- and, interestingly, was one of the few suspects whose picture we could not source online. a polymath with an impressive range of interests and an authoritative writing style notably similar to Satoshi's; someone with all the right specialisations and what is bitcoin mining? Bitcoins are generated all over the internet by anybody running a free application called a "bitcoin miner". Collectively, they verify all bitcoin transactions, and record the details in files called "blocks" Once a block of the most recent transactions is complete, and a complex mathematical puzzle unique to that block is solved, 25 new bitcoins are released to the miner (or group of miners) as a reward, plus a small fee The block reward decreases over time -- it started out at 50 bitcoins per block and halves every 210,000 blocks. This brings new coins into the system at a steady and predictable rate. The last bitcoin will be released around the year 2041 The computing power required for mining is high -- and the chances of individual miners finding a block are low, so miners often pool their resources There's currently an arms race in bitcoin mining, with an ever-growing array of hardware on offer, including USB devices containing chips custom-built for the job (pictured) to the right of the political spectrum (his essays at szabo.best.vwh.net incorporate a whole page of Ronald Reagan quotes). I go back to Szabo's pal, Wei Dai. "Wei," I say, "the other night you said you were sure Nick Szabo wasn't Satoshi. What made you sure?" "Two reasons," he replies. "One: in Satoshi's early emails to me he was apparently unaware of Nick Szabo's ideas and talks about how bitcoin 'expands on your ideas into a complete working system' and 'it achieves nearly all the goals you set out to solve in your b-money paper'. I can't see why, if Nick was Satoshi, he would say things like that to me in private. And, two: Nick isn't known for being a C++ programmer."

Perversely, a point in Szabo's favour. But Wei forwards me the relevant emails, and it's true: Satoshi had been ignorant of Szabo's bit-gold plan until Wei mentioned it. Furthermore, a trawl through Szabo's work finds him blogging and fielding questions about bit gold on his Unenumerated blog on December 27, 2008, while Satoshi was preparing bitcoin to meet the world a week later. Why? Because Szabo didn't know about bitcoin: almost no one outside the Cryptography Mailing List did, and I can find no evidence of him ever having been there. Indeed, by 2011, the bit-gold inventor is blogging in defence of bitcoin, pointing out several improvements on the system he devised.

AT THIS frustrating moment, a bolt of inspiration.

For obvious reasons, almost everyone I speak to suggests canvassing the views of David Chaum, the aforementioned Godfather of internet cryptography -- although cypherpunk vets tend to add: "Of course, he won't talk to you."

Accordingly, I've sent a couple of emails and am about to hit "send" on a third when the thought suddenly occurs: why not him? All at once his near-complete lack of mention as a candidate for Satoshi seems astonishing. Is it because he's kept such a low public profile since the traumatic fall of DigiCash? Chaum was a brilliant academic mathematician, who saw that cryptography would become the key to everything and turned his attention to it. Freedom-loving and vocally appalled by state snoops such as the NSA, even back in the 1990s, he was naturally inclined not just to think, but to set his ideas in motion, both in academia and later in business.

He filed patents and founded DigiCash as the dotcom boom approached. Fellow cypherpunks thought he'd sold out, but those close to him say he was more concerned with control than wealth, because he thought society was at a crossroads and that if citizens weren't given the tools they needed to protect themselves, "1984" might happen for real in 2024. Or 2014.

A Dutch colleague from the DigiCash days tells me that while Chaum could be difficult and demanding, "his achievement was to bring cryptography to non-state agencies"; to help arm us for the battle ahead. Private, untraceable, incorruptible money was key to this quest -- it was not an issue of convenience, but of survival.

Then DigiCash went bust, let down by investors and the market. Did Chaum decide that he couldn't rely on the state or the private sector? Did he decide that the only way to realise his dream of an anonymous peer-to-peer currency was to return to those ornery, cypherpunk roots and give us the tools, let us learn to save ourselves (because bitcoin can be anonymous if treated with sufficient care or combined with a software program called the Tor browser, of which Chaum is a champion)? Perhaps no one has mentioned Chaum because he's found a way to realise his dream quietly and with complete creative autonomy.

I ask the cypherpunks and none had considered the possibility. All seemed intrigued: none dismissed the thought out of hand. Here was someone with the requisite range of abilities; a proven theorist and doer. How confident am I of this theory? Not very. I can find no evidence pointing to Chaum, even circumstantial -- which, given his status, seems rather odd. Far more surprising, however, is my near certainty that all the other candidates are red herrings.

I send another email to Chaum, then another, but get nothing back. At which point I realise that cryptography is the science of keeping secrets and Satoshi is a master cryptographer; that we may never know The Creator's identity for sure, even though we will know if and when "he" starts spending his bitcoins.

The more remarkable discovery? That bitcoin may but hint at the depth of his work. When I contact a crypt named Ray Dillinger, one of Satoshi's early (and initially sceptical) interlocutors, he insists that, "intellectually speaking", approaching Satoshi's creation is "like being on the coastline of a new continent, wondering what the eventual complete map will contain it will take decades, perhaps a century or more, before new refinements and ideas become even remotely difficult to come up with."

What does Dillinger mean? Starting from the proposition that the most corrosive crimes against society and individuals in the data age tend to involve falsification, whether at the hands of Enron, Bernie Madoffor bankers flogging bent mortgages, Dillinger observes: "The rules of a consensus-history system could, in principle, be as minimal or complete as we are able to express in a programming language. It is possible, therefore, to extend the idea of a universally consistent history -- in which attempts to misrepresent simply fail -- much further than simply recording monetary transactions. Can you imagine a society in which most forms of falsification simply fail? "We can't build that yet. But with Nakamoto's protocol, we are starting to see how such a thing could be built."

At which point the question of who Satoshi is suddenly seems secondary. What Dillinger describes is an internet in which all information does not look the same. The dawn of Web 3.0. And perhaps by the time we have that, we'll also have the name of its creator | Andrew Smith is the author of Totally Wired: the Wild Rise and Crazy Fall of the First Dotcom Dream, and Moondust. @wiresmith

LET'S GET PHYSICAL

Physical bitcoins, known as Casascius Coins, have been minted with digital bitcoin keys hidden inside them. But the one-man mint, Mike Caldwell of Utah, was forced to stop selling them in November The world's first bitcoin ATM, Robocoin, opened in a coffee shop first coffee in Vancouver, Canada, last October. You put cash in, and it puts bitcoins in your digital wallet in return. The machine can also scan a QR code on your mobile phone and dispense cash (for a fee). Robocoin ATMs are due to appear in London this month

IS THIS SATOSHI NAKAMOTO? DAVID CHAUM

A brilliant mathematician, a graduate of Berkeley and founder of the International Association for Cryptologic Research. Produced the first workable blueprint for untraceable e-money, which he called ecash

"Wikileaks has kicked the hornet's nest, and the swarm is heading towards us." The next day, Satoshi made his last post on the bitcoin forum

Source Citation (MLA 7th Edition)
"Desperately seeking Satoshi; From nowhere, bitcoin is now worth billions. Where did it come from? Andrew Smithset off to find Satoshi Nakamoto, the mysterious genius behind the hit e-currency." *Sunday*