

Benjamin Wallace Tajemný pan Nakamoto



Pátrání
po záhadném
vynálezci
kryptoměn

host

Brno 2026

**přeložil
Jakub
Hovorka**

**Benjamin
Wallace**

**Tajemný
pan
Nakamoto**



**Pátrání
po záhadném
vynálezci
kryptoměn**

Automatizovaná analýza textů nebo dat
ve smyslu čl. 4 směrnice 2019/790/EU
je bez souhlasu nositele práv zakázána.

The Mysterious Mr. Nakamoto
Copyright © 2025 by Benjamin Wallace

All rights reserved including the right of reproduction
in whole or in part in any form. No part of this book may
be used or reproduced in any manner for the purpose
of training artificial intelligence technologies or systems.
This work is reserved from text and data mining
(Article 4(3) Directive (EU) 2019/790).

This edition published by arrangement with Crown,
an imprint of the Crown Publishing Group,
a division of Penguin Random House LLC

Translation © Jakub Hovorka, 2026
Czech edition © Host — vydavatelství, s. r. o., 2026
(elektronické vydání)
ISBN 978-80-275-3187-5 (PDF)
ISBN 978-80-275-3188-2 (ePUB)
ISBN 978-80-275-3189-9 (MobiPocket)

Nicole a Lucindě

Je to on

Pokud byl muž, o kterém jsem si myslel, že je Satoši Nakamoto, opravdu vynálezcem Bitcoinu vystupujícím pod tímto pseudonymem, nikdy by to nepřiznal. Pravděpodobně by se se mnou odmítl bavit. A setkat se s ním znamenalo strávit dvacet hodin v letadle a pak ještě dalších osm hodin jízdy autem. Ale já jsem s ním mluvit potřeboval, a to osobně.

Nakamoto zmizel na jaře 2011. Já se o jeho existenci dozvěděl v létě téhož roku, když jsem pro časopis *Wired* psal jejich první obsáhlý článek o Bitcoinu,¹ internetové měně fungující bez vazby na jakoukoli vládu nebo banku. O dvanáct let později zůstávala identita tvůrce Bitcoinu neznámá a jeho ohromný majetek netknutý. Kdyby vystoupil z anonymity, mohl si užívat slávy i bohatství, ale z těžko pochopitelných důvodů se obojího zříkal. V moderních dějinách bychom nenašli podobný případ, kdy se tvůrce převratné technologie nepřihlásil k autorství.

Fanoušci Bitcoinu tudíž přišli o možnost oslavovat člověka z masa a kostí a byli nuceni svoji úctu projevovat pouze Nakamotovu jménu, čímž získalo status legendy. V roce 2022 jste například v Beverly Hills mohli spatřit Kanyeho Westa, jak vystupuje ze svého vozu Cadillac Escalade a na hlavě má kšiltovku se Satošiho jménem.² V Budapešti zase stoupenci Bitcoinu odhalili první Nakamotovu sochu, která jej zobrazuje jako zahalenou, téměř přízračnou

postavu vyvedenou v bronzu.³ Na souostroví Vanuatu v jižním Tichomoří začali developeři prodávat vlastnické podíly na utopickém ráji, který pojmenovali Satošiho ostrov.⁴ A trojice libertariánů koupila starou výletní loď, pokřtila ji MS Satoši a začala shánět osadníky pro první nezávislé společenství postavené na Bitcoinu.⁵ Nejedem technologický expert navrhoval, aby Satošimu Nakamotovi byla udělena Nobelova cena.⁶

Navzdory veškerému úsilí však Nakamotova identita odolávala odhalení. Spekulovali o ní mimo jiné i Elon Musk nebo Peter Thiel.⁷ Fanoušci posedlí pátráním po Nakamotovi se pokoušeli získat nové indicie nebo již známá fakta přesvědčivěji poskládat. Všehovšudy padlo podezření na více než stovku osob.

S tajemstvím Nakamotovy identity si neporadily ani moderní technologie. Ve světě, kde se před internetem nic neskryje, nemá podobná záhada obdoby. Víme už například, kdo tajně dodával informace Bobu Woodwardovi.⁸ Našli také důkaz Velké Fermatovy věty.⁹ A víme, že Thomas Pynchon si pro bagely chodil nejspíš do pekařství u Zabara.¹⁰

Když jsem se poprvé rozhodl o Nakamotovi napsat, vůbec mě nenapadlo, že i po více než deseti letech zůstane jeho identita poslední velkou hádankou. Ještě absurdnější by mi však přišlo, kdyby mi někdo tvrdil, že příběh o přízraku stojícím za první kryptoměnou na světě a usilovná snaha o jeho odhalení budou nějakým způsobem souviset se soudními spory, automobilovou honičkou, vypsáním peněžité odměny, jměním v hodnotě sedmdesáti pěti miliard dolarů, pokusy o vydírání, výhrůžkami smrtí, nasazením zásahové jednotky SWAT, sebevraždou, prchajícím obchodníkem se zbraněmi, profesionálním padělatelem, tajnou společností, jejíž členové jsou natolik paranoidní, že budou známi jen pod svými přezdívkami, dobrosrdečným

géníem, jehož nemoc uvěznila ve vlastním těle, jaderným bunkrem někde v Evropě, zmrzlými těly v arizonské poušti a britským špiónem zamčeným ve sportovní tašce.

Předchozí pokusy odhalit Nakamotovu identitu selhaly — některé přímo spektakulárně. Dokonce i pořad *60 Minutes*, který disponuje nepředstavitelnými zdroji a zaměstnává tým ostrílených investigativních novinářů, nakonec pátrání vzdal s prohlášením, že je to „mission impossible“. ¹¹ A přesto, navzdory všem překážkám, jsem byl přesvědčený, že mně se tuhle záhadu rozlousknout podařilo.

Byl jsem nervózní z toho, co to pro mě může znamenat. Svět Bitcoinu nebyl investigaci tohoto druhu nakloněn. Ale to mi zase takové starosti nedělalo. Když jsem se dopátral Nakamotovy skutečné identity, zaskočilo mě, že nepatřil mezi ty, které jsme celou dobu podezírali. Tenhle člověk vynaložil obrovské úsilí, aby ho nebylo možné najít. A to, co jsem se o něm dozvěděl, mě zneklidnilo. Vůbec nebyl takový, jak si ho lidé představovali. Opakovaně o sobě prohlašoval, že je nebezpečný. A měl zbraně.

Než jsem se vydal na druhý konec světa, abych se s ním setkal, musel jsem si být jistý, kde přesně ho najdu. Vlastnil nejméně čtyři nemovitosti na dvou různých kontinentech. Zprvu jsem se domníval, že se ukrývá v odlehlé části největšího havajského ostrova. Později jsem však dospěl k přesvědčení, že žije na východním pobřeží Austrálie, v malé komunitě sdružené kolem pláže severně od Brisbane. Pomalu mi začalo docházet, že si budu muset najmout soukromé detektivy, kteří by to místo sledovali a potvrdili mi, že se tam opravdu nachází.

V době, kdy jsem si s tím lámal hlavu, jsem se sestrou zašel na večeři do mexické restaurace na Manhattanu a svěřil se jí s tím, co se mi podařilo zjistit.

„Je to on,“ reagovala bez zaváhání, ale já si tak jistý nebyl.

Klidně usrkávala svoji margaritu, zatímco já jsem nejspíše pobrumlával, že třeba je všechno jinak.

„Je to on,“ zopakovala.

Pověděl jsem jí, z čeho mám strach, měla totiž s podobnými záležitostmi mnohem větší zkušenosti. Dvacet let pracovala jako producentka v televizním zpravodajství. Během svého působení v pořadu *24 Hours* byla osobně přítomna, když FBI v Montaně zatýkala Unabombera.

Navrhla mi, abych si s sebou vzal profesionální ochranu. A abych nezapomněl na neprůstřelnou vestu. A taky abych o svých plánech informoval místní policii.

„Díky,“ zamumlal jsem.

Cítil jsem se o něco lépe. Měl jsem alespoň nějaký plán. Televizní reportéři tohle podstupují pořád. Nebála se. Nemusel jsem si tedy dělat starosti ani já.

Nad ránem mi od ní přišla zpráva.

„Nevím proč, ale nemohla jsem spát.“

Bylo 4.09.

„Napadly mě dvě věci. Možná ho konfrontuj někde na veřejnosti, pokud tedy někdy vychází z domu. A taky bys s sebou měl mít někoho, kdo vaše setkání z bezpečné vzdálenosti natočí. Jako důkaz.“

Absolutní legenda

O osmnáct měsíců dříve, na silvestra 2021, mi do e-mailové schránky přišla zpráva s předmětem: Nové informace o Satošim.

Od chvíle, kdy jsem napsal zmíněný článek pro časopis *Wired*, mi takové e-maily občas chodily. Bitcoin a širší kryptoměnový průmysl, který z něj vzešel, stále představovaly relativně nový fenomén, takže pokud jste je nakoupili třeba ještě v roce 2017, řadili jste se mezi „OG bitcoinity“.* Novináři, kteří o Bitcoinu psali v jeho počátcích, pak byli za zkušené kryptokronikáře, a tudíž na ně cílil každý, kdo chtěl něco ze svých dohadů o Satošim vytěžit. A zájemce se vždy našel.

Obvykle jsem těmto e-mailům nevěnoval velkou pozornost. Zprávy o Nakamotovi ve mně vždy na chvíli vzbudily naději, že se dozvím něco nového, ale nakonec se pokaždé ukázaly jako nevěrohodné. Smířil jsem se tedy s tím, že záhada jeho identity zůstane nevyřešena. A tenhle e-mail rozhodně důvěryhodně nepůsobil, chyběl mu podpis. Přesto jsem ho otevřel. Obsahoval jen odkaz na blogový příspěvek nazvaný: „Jsem stážista ze společnosti SpaceX, co přišel s tím, že Satoši je Elon Musk. A ještě jsem

* Pozn. překladatele: Výraz „OG“ je zkratka anglického spojení „original gangster“ a označuje osobu, která je průkopníkem v určité oblasti a zaslouží si úctu ostatních.

neřekl všechno.“¹ Autor blogu, Sahil Gupta, o čtyři roky dříve způsobil na internetu menší rozruch, když ve svém předchozím příspěvku tvrdil, že existuje jistá „pravděpodobnost“, že Nakamoto je Musk.² Nyní předkládal další důkazy. Popisoval komunikaci s vedoucím Muskovy kanceláře Samem Tellerem. Text mě nepřesvědčil, a tak jsem na zprávu neodpověděl.

O dva dny později mi z téže adresy přišel další anonymní e-mail. Byl v něm odkaz na stránku na GitHubu³ — webové platformě, kde softwaroví vývojáři sdílejí svoji práci — a tam jsem našel podrobné zdůvodnění Guptovy teorie, proč Musk musí být Nakamoto. Možná to bylo tím, že se v té době Musk hojně objevoval v médiích, a tak jsem se v následujících týdnech přistihl, že nad touhle teorií přemýšlím. Guptovy argumenty měly rozličný charakter, od vágních až po velmi odborné, a já si nebyl jistý, co si o tom všem mám myslet. Nakonec jsem mu odepsal. Bylo zjevné, že ty e-maily poslal on. Koneckonců si vybral právě mě, abych jeho spekulace publikoval.

„Díky, že jste si na mě udělal čas,“ zahájil Sahil naši konverzaci. „Napsal jsem stovkám novinářů.“

Seděl u sebe doma nedaleko San José a mluvili jsme spolu prostřednictvím videohovoru. Měl na sobě tmavěfialové tričko, na uších stříbrná sluchátka a na tváři strniště.

„Je fascinující, jak pokroucenou a negativní představu si lidé o Muskovi vytvořili,“ pokračoval Sahil poněkud nervózně. „Myslí si, že sestrojil raketu a vybudoval automobilovou společnost úplnou náhodou.“

A potom mi Sahil začal vyprávět, jak odhalil Nakamotovu skutečnou identitu.

V roce 2015 během studia na Yaleově univerzitě zaujal Sahila program společnosti SpaceX a podařilo se mu zís-

kat letní stáž ve výrobním závodě na rakety v Hawthornu v Kalifornii, kde pracoval na vývoji softwaru pro skladovou evidenci. „Byla to úžasná zkušenost,“ vzpomínal Sahil. Musk trávil v kanceláři asi tři dny v týdnu a Sahil ho občas zahlédl na chodbě. Po „rychlém neplánovaném rozpadu“, jak se interně hovořilo o výbuchu jedné z raket, byl Sahil při tom, když Musk ve svém projevu slíbil, že SpaceX použítou technologii zdokonalí a problém vyřeší. „Bylo to velmi inspirativní,“ popisoval Sahil.

Spojitosť mezi Muskem a Bitcoinem Sahila napadla až po skončení stáže. Jako student informatiky ve své diplomové práci spolupracoval se dvěma dalšími studenty a společně pro centrální banku Spojených států navrhli digitální měnu zvanou fedcoin. „Co kdyby Spojené státy vzaly ty nejlepší vlastnosti Bitcoinu a vylepšily jimi dolar?“ vysvětloval mi později Sahil. Ve své práci nezapomněl Satošimu Nakamotovi poděkovat za to, že je „absolutní legenda“.⁴

Během přípravy své diplomové práce se Sahil ponořil do studia literatury o kryptoměnách, počínaje devítistránkovou bílou knihou, ve které Nakamoto koncept Bitcoinu poprvé popsal. O tom, že Nakamotova skutečná totožnost je záhadou, se Sahil dozvěděl jen krátce předtím. Při svém studiu si všiml určitých podobností mezi texty tvůrce Bitcoinu a jazykem, který používal Elon Musk. Oba mluvili o „řádech velikosti“ a používali výraz *bloody* (zatracený). Oba své teze opírali o „základní principy“. Nakamoto hovořil o penězích jako konceptu, stejně jako Musk, když byl na začátku nového tisíciletí ředitelem PayPalu. Sahil také zjistil, že Musk i Nakamoto v minulosti programovali v jazyku C++ a mají dobré znalosti ekonomie a kryptografie. Nakamoto navíc dokázal ve snaze o dosažení cíle projevít jistý druh sebezapření. „Stejně se chová i Musk,“ prohlásil Sahil. Začalo

mu to vrtat hlavou. Měli jsme snad vynálezce Bitcoinu celou dobu na očích a jen nás oslnila záře jeho slávy?

Když Sahil dokončil své univerzitní studium, rozhodl se, že chce pracovat přímo pro Muska, v jeho kanceláři. Několikrát proto Muska e-mailem oslovil, až se mu podařilo domluvit si telefonický pohovor s Tellerem, vedoucím jeho kanceláře. Sahil Tellerovi pověděl o svém vzdělání a zkušenostech, ale Teller mu řekl, že se na danou pozici nehodí. Hledali administrativního asistenta a Sahil by podle něj udělal lépe, kdyby si založil vlastní firmu.

„Radil mi dobře,“ řekl mi Sahil.

Když se rozhovor s Tellerem chýlil ke konci, Sahil se rozhodl zariskovat a zeptal se:

„Je Elon Satoši?“

„Teller asi patnáct vteřin mlčel,“ líčil Sahil. „A pak odvětil: No, co vám na to mám říct?“

„To byla další velká indicie,“ pokračoval Sahil. „Jako by to bylo naprosto jasné. Zaskočil jsem ho. Jeho odpověď jsem si nemohl vyložit jinak.“

Později toho roku Sahil na svém blogu publikoval příspěvek „Elon Musk pravděpodobně vynalezl Bitcoin“. Vynechal v něm informace o soukromém rozhovoru s Tellerem, ale popsal ostatní podobnosti, které objevil. Tvrdil také, že bitcoinové komunitě by prospěl návrat jejího zakladatele, který by jí v době sporů o to, zda a jak Bitcoin masově zavádět, pomohl ukázat cestu. Několik blogů o kryptoměnách Sahilovu teorii převzalo a zprávu o ní přinesla i agentura Bloomberg News.⁵ Samotný Musk reagoval tweetem: „Není to pravda. Kamarád mi před pár lety část [bitcoinu]* poslal, ale vůbec nevím, kam jsem ji dal.“⁶

* Slovo Bitcoin se píše s velkým písmenem, pokud máme na mysli systém, a s malým písmenem, pokud mluvíme o měně.

Sahil nakonec pro Muska opravdu pracoval — v roce 2018 ho společnost zaměstnala, aby pomáhal s programováním cloudového softwaru Tesly. Fascinovala ho Muskova strategie, kdy softwaroví inženýři pracovali pod jednou střechou s dělníky z výroby, což odporovalo běžné praxi v automobilovém průmyslu. Tesla právě navyšovala výrobu Modelu 3 a Sahil mohl na vlastní oči vidět, jak Musk usiloval o naplnění svých vizí a nenechal se zvíkat skeptickými hlasy. Sahil se mi svěřil, že jeho přesvědčení, že Elon je Satoši, mu v práci nikdy nepůsobilo potíže: „Netajil jsem se tím. Opravdu věřím, že Elon je nový Ben Franklin. Myslím, že se mě na to manažer zeptal jenom jednou.“

Časem Sahil z Tesly odešel a založil si vlastní společnost, která se věnovala virtuálnímu 3D modelování pro platformy, jako je Shopify. Ale jak roky ubíhaly a Sahil přidával další dílky do své skládačky, jeho domněnka, že Musk je Nakamoto, se proměnila v jistotu. Jednou narazil na něco, co během panelové diskuse v Davosu řekl Luke Nosek, spoluzakladatel PayPalu: uvedl, že původním cílem společnosti bylo vytvořit měnu, která by nebyla závislá na bankách.⁷ Kromě toho dostal tip, že Musk — stejně jako Nakamoto — ve svých textech za tečkou vždy píše dvě mezery. Jeden jeho kolega se zmínil, že Musk pravidelně létá z letiště Van Nuys, což až podezřele odpovídalo jedinému bezpečnostnímu přešlapu, kterého se kdy Nakamoto dopustil. V začátcích bitcoinové éry totiž Nakamoto psal jinému vývojáři a v důsledku momentální nepozornosti jeho e-mail prozradil IP adresu svého odesílatele: severní část Los Angeles.⁸ Sahil se dozvěděl, že první vývojáři Bitcoinu o Satošim říkali, že „má potřebu mít vše pod kontrolu“, a totéž platilo i v případě Muska. A co bylo typické pro Muska jako byznysmena v době, než koupil Twitter? Nebál se dělat obtížné věci jako vyrábět elektrická auta, která

budou vypadat skvěle, nebo přistát s raketou *na plovoucí plošině*.

Na konci roku 2021 se Sahil rozhodl, že nadešel čas opět vystoupit na veřejnosti. Nakamoto byl už téměř všemi vnímán jako dobrosrdečný génius a Sahil cítil, že se naskytla vzácná příležitost, kdy by média mohla konečně přijmout jeho teorii, že Nakamoto a Musk jsou jedna a tatáž osoba. Společnost SpaceX právě úspěšně připojila svoji kapsli k Mezinárodní vesmírné stanici a Musk byl nedávno vyhlášen osobností roku časopisu *Time*. Dokonce se na Twitteru žertovně vyjádřil ke kryptoměně dogecoin, jež byla inspirována internetovým memem. Když Sahil zveřejnil svůj nový příspěvek, na základě kterého následně poslal e-mail nejen mně, ale i stovkám dalších novinářů, vůbec poprvé zde popsal svoji komunikaci s šéfem Muskovy kanceláře.

Z obrazovky počítače mi nyní tvrdil, že si je svojí teorií „na devadesát devět procent jistý“. Pochybnosti ostatních podle něj pramení z jejich předsudků vůči Muskovi. „Překvapuje mě, že lidé podceňují Muskovy schopnosti. To jen ukazuje, že v naší společnosti jsou hluboce zažitá stereotypy a lidé nejsou schopni dívat se na fakta objektivně.“

Chtěl jsem se ho zeptat na několik otázek. Musk byl bezpochyby výjimečně schopný člověk, ale sám kdysi označil rok 2008, kdy se zadlužil, rozvedl a tři jeho rakety Falcon v řadě selhaly při startu, za nejhorší rok svého života.⁹ Nakamoto přitom bílou knihu o Bitcoinu vydal právě v roce 2008. Bylo vůbec možné, aby Musk měl dostatek času a sil na vytvoření první životaschopné kryptoměny na světě a následně osobně řídil s ní spojený softwarový projekt po dobu téměř dvou let? A to vše ve chvíli, kdy se zároveň snažil vybudovat průmysl s elektromobily a úspěšnou soukromou kosmickou společností?

Sahil měl připravenou odpověď na každou moji otázku. Prý viděl rozhovor, ve kterém Musk tvrdil, že v roce 2007 trávil prací pro Teslu jen tři dny v měsíci. A není snad všeobecně známo, že Musk má neuvěřitelný talent pracovat na několika nesouvisejících projektech zároveň? Vždyť měl za sebou dokonce i zkušenost s publikováním bílé knihy. V roce 2013 Musk bez jakékoli předchozí publicity na internetu zveřejnil osmapadesátistránkový dokument, v němž detailně popsal nový druh dopravního systému známý jako „hyperloop“.¹⁰

Ale Musk vždy vystupoval pod vlastním jménem a rozhodně nebyl skromný, tak proč by popíral, že je Nakamoto, pokud opravdu stál za Bitcoinem? Sahil v tom rozpor neviděl. Naopak, pro něj to byl další důkaz, že Musk ví, co dělá. „Na rozdíl od klasické firmy, která potřebuje marketing, Bitcoin zpočátku těžil z aury anonymního zakladatele, což mu pomohlo získat více uživatelů a rychleji růst.“

A proč Sahil považoval za důležité podělit se se světem o Muskovo tajemství? „Je to neuvěřitelný příběh,“ odpověděl Sahil. Přál si, aby se Muskovi dostalo uznání, které si zaslouží. Jeho cílem bylo dosáhnout „dostatečně silného tlaku veřejnosti, jenž by Muska přinutil přiznat, že je tvůrcem“ Bitcoinu.

Ačkoli jsem nedokázal posoudit, zdá má Sahil se svojí teorií pravdu, rozuměl jsem, proč je jí tolik posedlý. Bitcoin jen chvíli předtím dosáhl svého historického maxima, kdy se jedna mince prodávala za téměř sedmdesát tisíc dolarů a celková tržní hodnota všech bitcoinů v oběhu přesáhla bilion dolarů. V Salvadoru byl mezitím bitcoin uznán za zákonné platidlo. Nebylo až tolik překvapivé, že v roce 2011 nikdo neznal Nakamotovu totožnost. Ale jak je možné, že ji nikdo neznal ani dnes?

O šest měsíců později jsem dal v práci výpověď, abych se mohl naplno věnovat rozluštění záhady, která mě poprvé uchvátila před deseti lety.

Internetové rádobypeníze

„Slyšel jsi někdy o Bitcoinu?“ zeptal se mě Jason Tanz.

To slovo mi nic neříkalo.

„A znáš Silk Road?“

Ani v tomto případě jsem nevěděl, o čem mluvím.

Jason byl redaktorem časopisu *Wired*. Psal se červen 2011.

Pověděl mi o nedávném článku, jenž byl zveřejněn na blogu *Gawker* a který se Silk Roadu věnoval. Silk Road bylo online tržiště na darknetu, kde bitcoin coby „nevystopovatelná digitální měna“ fungoval jako oficiální platidlo.¹ Ačkoli Bitcoinu ještě nebyly ani tři roky, měl už za sebou tři fáze vývoje. Z utopického softwarového projektu na samém začátku se postupem času stala komodita s překvapivým denním obratem sto třicet milionů dolarů, která však následně získala pochybnou reputaci a byla spojována se zločinem, skandály a krachem cen. Nicméně Bitcoin byl produktem své doby podobně jako hnutí Occupy Wall Street, jež mělo přijít jen o několik měsíců později. A Jason mi vysvětlil, v čem je Bitcoin opravdu převratný. Předchozí pokusy o vytvoření digitální hotovosti selhaly, protože to, co dělalo internet opravdu revolučním — tedy okamžitá distribuce informací v prostoru bez jakýchkoli hranic nebo centrální autority —, zároveň vedlo k takzvanému

problému dvojí útraty. Pokud si představíme, že internet je kopírkou a digitální hotovost řetězcem bitů, co by zabránilo tomu, aby někdo jen nekopíroval jeden a ten samý řetězec pořád dokola? Byl to právě Satoši Nakamoto, architekt Bitcoinu, kdo přišel s důmyslným řešením tohoto problému.

„Zajímá tě to?“ zeptal se mě Jason.

Vystudoval jsem angličtinu a o informatice jsem nevěděl vůbec nic. Vždy mi trvalo neuvěřitelně dlouho, než jsem si zvykl používat nějakou novou technologii. Když v devadesátých letech začal internet získávat na popularitě, vůbec jsem tomu nerozuměl. Považoval jsem ho jen za další vynález v řadě a nechápal jsem, proč si všichni ostatní myslí, že tato technologie zásadně změní vzorce našeho chování. „Je to přece úplná banalita, nic převratného,“ posmíval jsem se.

„Zní to úžasně,“ odpověděl jsem Jasonovi.

Časopis *The Economist* vydal o Bitcoinu článek jen o chvíli dříve a detailně v něm popsal, jak tato měna funguje.² A podle významného investora do fondů rizikového kapitálu Freda Wilsona bylo možné Bitcoin přirovnat k fenoménům, jako byly WikiLeaks nebo arabské jaro, s nimiž ho spojoval potenciál změnit současný svět.³ Pro novináře tudíž Bitcoin představoval téma, které si nebylo možné nechat ujít. Představa neoficiálního, paralelního peněžního systému připomínala tajnou poštovní službu z románu *Dražba série č. 49* Thomase Pynchona. Tuto asociaci umocňovala i různorodá kyberpunková směsice lidí, kteří za Bitcoinem oddaně stáli a mezi nimiž bychom našli hackery, gold bugy,* anarchisty i fanoušky autorky

* Pozn. překladatele: Anglický termín „gold bug“ označuje osoby, které podporují návrat ke zlatému standardu a věří, že klasické peníze nemají žádnou hodnotu a jsou podvod. Termín může označovat také investory do zlata.

Ayn Randové. Mě osobně naprosto uchvátila záhada Nakamotovy identity.

Vždy mě fascinovalo, že bez ohledu na to, jak detailní dnešní mapy jsou, pořád na nich můžeme najít prázdná a nepopsaná místa. Jako dítě jsem měl pod nočním stolem schovanou velkou knihu plnou fantaskních ilustrací a zrnitých černobílých fotografií, které zobrazovaly lochnesskou příšeru nebo bermudský trojúhelník a podobné záhady, pro něž jsme neměli vysvětlení. Postupem času můj zájem o tyto legendy s nádechem něčeho nadpřirozeného vystřídal fascinace jistým druhem osobností, jichž v sedmdesátých a osmdesátých letech dvacátého století rozhodně nebylo málo. Šlo o lidi na útěku před spravedlností nebo stranící se společnosti, kteří se chtě nechtě stali populárními ikonami. Patřili mezi ně například členové organizace Weather Underground a skupiny Baader Meinhof, kteří byli na útěku před policií. Nebo bývalí příslušníci třetí říše, kteří se ukrývali v paraguayské džungli. Ale i unesená dcera bohatých rodičů Patty Hearstová, jež se samopalem v ruce vyloupila banku. Nebo světoběžník Šakal Carlos. A určitě nesmím zapomenout na spisovatele, jako byl Thomas Pynchon a J. D. Salinger, kteří se úzkostlivě stranili pozornosti médií. Příběhy těchto a jim podobných lidí nás nejen obklopovaly, ale i utvářely. Možná jsem si v mládí, kdy jsem dychtivě hltal jeden román Roberta Ludluma za druhým, vytvořil pro tyto příběhy slabost. Nicméně nepolapitelný Satoši Nakamoto — ať už existoval, nebo ne — mi v tuto chvíli přišel jako někdo, kdo všechny zmíněné předčil převratností svého objevu.

Začal jsem tedy obvolávat lidi zabývající se Bitcoinem a vyrážet za nimi metrem z Brooklynu, kde jsem tehdy bydlel. Setkal jsem se například s majitelem společnosti věnující se produkci internetových videí, který byl

Bitcoinem naprosto posedlý a za nímž jsem musel do špinavé kanceláře v pátém patře budovy v centru Manhattanu. Jindy jsem zamířil do kavárny prodávající bubble tea poblíž Union Square.

Podařilo se mi zjistit, že o Halloweenu roku 2008 Nakamoto v obskurním diskusním fóru o kryptografii, které bylo neoficiálně známé jako Metzdown,⁴ zveřejnil krátký text, v němž načrtl svoji představu „peer-to-peer elektronického peněžního systému“.⁵ Popsal zde nový druh peněz, jež měly fungovat na síti složené z počítačů, které by k tomuto účelu propůjčili dobrovolníci. Síť by byla otevřená všem, kdo by měl zájem se do ní zapojit, a každý by z ní mohl kdykoli odejít. Problém dvojí útraty měl být vyřešen pomocí transparentní veřejné účetní knihy, jež by byla kolektivně spravována v rámci samotné sítě, aniž by bylo nutné spoléhat se na bankovní nebo vládní databáze pohledávek a závazků. Nakamoto připojil též odkaz na detailnější formální popis tohoto systému, který vešel ve známost jako „bílá kniha Bitcoinu“, ale tohle byla jeho hlavní myšlenka.

Nakamoto nemohl spuštění své alternativní měny načasovat lépe. Mnoho lidí bylo právě tou dobou na banky velmi našťavaných, jelikož banka Lehman Brothers požádala jen o měsíc dříve o ochranu před věřiteli, což mělo za následek největší bankrot v amerických dějinách,⁶ a americký Fed použil peníze daňových poplatníků na záchranu AIG, jedné z největších pojišťoven na světě.⁷ Decentralizace nebo diverzifikace investic se tak stala lákavější než kdykoli předtím.

Nakamotův výběr fóra, na němž Bitcoin představil, byl rovněž velmi zdařilý. Díky svému zaměření na kryptografii byla diskusní skupina Metzdown ideálním místem pro setkávání technicky zaměřených libertariánů, tedy

lidí, kteří jednak vynikali v informatice, jednak nesnášeli autority. Skutečnost, že nikdo předtím o Satošim Nakamotovi neslyšel, nikomu z členů Metz Dowdu nepřišla divná. Fórum často navštěvovali lidé, kteří se věnovali matematice šifrování. Byli tedy zvyklí používat pseudonymy.

Několik členů této diskusní skupiny, jež vize digitální měny obzvláště zaujala, okomentovalo Nakamotův software a on jejich zpětnou vazbu bez váhání uvítal: „Díky, že jsi mě na to upozornil,“⁸ stojí v jedné z jeho odpovědí. „Vážím si tvých otázek,“ píše jindy v soukromém e-mailu a pokračuje: „Ve skutečnosti jsem to dělal tak nějak pozpátku. Musel jsem nejprve napsat celý kód, než jsem sám sebe přesvědčil, že dokážu vyřešit všechny problémy. Knihu jsem napsal úplně nakonec.“⁹ Na začátku ledna 2009 Nakamoto na webové platformě SourceForge zveřejnil alfa verzi softwaru.¹⁰ V té době to byla oblíbená platforma pro projekty založené na open source softwaru, do nichž se v rámci kolektivní práce mohl zapojit každý programátor. Podle jednoho z prvních bitcoinerů si hned první den stáhlo Bitcoin 127 lidí.¹¹

Mezi prvními uživateli bylo mnoho programátorů, kteří zastávali názor, že peníze jsou zastaralé a už dávno potřebují aktualizaci. Bankovky a mince měly řadu nevýhod, mohly vyblednout, zmačkat se nebo roztrhnout, opotřebovat se nebo ušpinit, a navíc zde bylo riziko přenosu bakterií. Peníze také existovaly pouze v předem určených hodnotách, bylo možné je padělat a obtížně se s nimi manipulovalo ve velkém množství. Bitcoin představoval peníze verze 2.0, tedy odolné, nepadělatelné a téměř donekonečna dělitelné. Mohla by se tak konečně naplnit představa internetového obchodování prostřednictvím mikrotransakcí. Lidé by mohli kamkoli okamžitě poslat jakoukoli částku.

Mnozí z těch, kteří se zapojili do první bitcoinové vlny, pevně věřili v osobní svobodu. Bitcoin jako cloudová měna založená na nulách a jedničkách, spravovaná obyčejnými lidmi rozptýlenými po celém světě, byla imunní vůči zásahům centrálních orgánů. Na rozdíl od zlatých cihel nebylo možné bitcoiny zabavit. Na rozdíl od bankovních účtů nemohl bitcoin nikdo obstavit. Na rozdíl od národní měny nebylo možné, aby národní banka jen tak devalvovala jeho hodnotu nebo aby jej diktátoři mohli svévolně regulovat. A na rozdíl od kreditních karet a bankovních převodů s ním nebyly spojené přehnané poplatky za transakce.

Za rozhodnutím prvních uživatelů vyzkoušet Bitcoin stála vždy ryze individuální kombinace různých důvodů a přesvědčení. Ukázkovým příkladem výjimečnosti každého z nich byl Dustin Trammell, který na internetu vystupoval pod přezdívkou Druid. Dustin byl třicetiletý hacker, jenž se rád učil novým věcem tak, že se do nich aktivně zapojil. Když neseděl u počítače, nadšeně se ve svém volném čase věnoval cosplayi. Koketoval s alternativními měnami kryptými drahými kovy, například s liberty dolarem, a nevyužitou výpočetní kapacitu svých počítačů zpřístupnil pro účely projektu SETI@home, dlouholetému experimentu Kalifornské univerzity v Berkeley. Tento projekt využívá crowdsourcing k analyzování dat z radioteleskopů ve snaze najít inteligentní mimozemský život. Jakmile se Dustin do slechl o Bitcoinu, rozhodl se, že si ho stáhne a nechá běžet na polovině svých počítačů, a to jen proto, že to považoval za zajímavý technologický projekt. Teprve později se začal zajímat o libertariánské názory na peněžní systém. S Nakamotoem si Dustin vyměnil hned několik e-mailů, v nichž se tvůrci Bitcoinu svěřil, že „elektronická měna a kryptografie

jsou dvě věci, které mě velmi zajímají“,¹² a nabídl mu pomoc s jeho projektem. „Rozhodně máme podobné zájmy!“ odpověděl mu Nakamoto a dodal:

Myslím, že v devadesátých letech se o tyto věci zajímalo daleko více lidí, ale protože se systémy založené na důvěryhodné třetí straně (DigiCash atd.) více než deset let potýkaly s neúspěchy, považují lidé tyto projekty za předem odsouzené k nezdaru. Doufám, že si uvědomí, že toto je poprvé, alespoň co já vím, kdy se snažíme vytvořit systém, který není založený na důvěryhodné straně.¹³

Jádrem Nakamotova vynálezu bylo něco, čemu se říká blockchain — neustále se prodlužující záznam všech transakcí (nákupů, prodejů atd.), které uvnitř daného systému proběhly. Přibližně každých deset minut je nejnovější skupina záznamů o transakcích spojena do „bloku“ a tento blok je spojen do „řetězce“ s blokem, jenž mu předcházel. To celé se děje s použitím sofistikované matematiky, jež brání komukoli, aby se mohl vrátit a provést v obsahu jednotlivých bloků změny. Tuto databázi nebo účetní knihu by v tradičním finančním systému spravovala instituce typu vlády nebo banky, ale v případě Bitcoinu je databáze spravována sítí počítačů, které patří jednotlivým uživatelům a na nichž běží software Bitcoinu. Každý počítač tak komunikuje s ostatními počítači v síti a ukládá víceméně identické a neustále aktualizované kopie účetní knihy. Aby se počítač mohl do této sítě připojit, musí nejprve vyřešit matematickou rovnici, již systém každých deset minut generuje. Podobně jako se internetové stránky ptají uživatelů, na kterých obrázcích v mřížce je vyobrazen

most, aby tak odlišily lidi od robotů, brání tento požadavek nazývaný „proof of work“ (doslova „důkaz o práci“) nebezpečným subjektům převzít nad systémem kontrolu. A proč by se někdo namáhal plýtvat výkonem svého počítače na řešení těchto zvláštních úkolů? Nakamoto navrhl svůj systém natolik chytře, že první počítač, který jednotlivou rovnici vyřeší, obdrží jako odměnu několik bitcoinů. Jedním tahem se mu tak podařilo vyřešit problém, jak nalákat lidi s upřímným zájmem o zapojení se do systému a odradit ostatní, a zároveň vytvořit předvídatelný mechanismus pro vydávání nových bitcoinů do oběhu. Ačkoli hlavním cílem soutěžení v řešení rovnic bylo zajistit bezpečnost systému, začalo se této aktivitě přezdívat „těžení“, protože každý uživatel mohl získat odměnu ve výši několika bitcoinů. (S těžbou nicméně souvisí obrovská spotřeba energie, kterou stovky tisíc počítačů spotřebují na řešení těchto rovnic, a to je jeden z důvodů, proč má Bitcoin špatnou pověst mezi ochránci životního prostředí.)

Laikům to celé může znít dost ezotericky, ale je důležité si uvědomit, že decentralizované peníze byly opravdu něčím naprosto novým. A jejich objev byl dílem génia. Zooko Wilcox začal být posedlý myšlenkou decentralizovaného peněžního systému už v době, kdy jako devatenáctiletý student a programátor se zájmem o politiku navštěvoval Coloradskou univerzitu v Boulderu. Dokud se o deset let později neobjevil Bitcoin, nepřemýšlel téměř o ničem jiném, než jak takový systém vytvořit. „Byla to jedna z nejoblíbenějších aktivit, kterým jsem se věnoval, než jsem šel spát. Dvanáct let, nebo kolik to přesně bylo, jsem se snažil vymyslet, jak to udělat,“ svěřil se mi Zooko. „Domnívám se, že propojení Nakamotova konsenzu s motivačními mechanismy je natolik originální, že by na to nikdo jiný nepřišel. Trvalo by to dalších sto let.“

Ať už jste bitcoiny těžili, nebo je od nějakého těžaře kupovali, být jedním z prvních mělo své zvláštní kouzlo. Nakamoto ve svém softwaru nastavil strop pro množství bitcoinů, které bude moct být vytěženo — celkem dvacet jedna milionů mincí —, a předpokládalo se, že systém tohoto čísla dosáhne někdy v roce 2140.¹⁴ Oproti jiným měnám zde nehrozí riziko inflace nebo hyperinflace, jelikož bitcoin je ze svého principu deflační. Dokud se technologie bude šířit, budou se vaše bitcoiny zhodnocovat. „Fascinuje mě představa virtuálních komunit, které nejsou svázané s žádným konkrétním místem a experimentují s novými ekonomickými modely,“ napsal Nakamoto v příspěvku na sociální síť P2P Foundation.¹⁵

Dělalo mi potíže pochopit, jak Bitcoin funguje, ale to bylo dáno převratností jeho koncepce, byl jako portál do nového světa nebo nový pohled na stávající svět, o němž jsem nevěděl, že je možný. Libertariáni, kteří cítili, že nemají nic společného se světem mainstreamu, nahlíželi na tradiční peníze jako na pouhou *fiat* měnu — vyslovovali to slovo s jasně slyšitelným pohrdavým akcentem —, jejíž hodnota byla odvozena pouze od nařízení vlády. Ale pro nás ostatní bylo setkání s měnou, která existovala mimo známý kontext, podobné situaci, již popsal David Foster Wallace ve svém příběhu o rybě, která nevěděla, že plave ve vodě¹⁶ — a teprve až když jsme z tohoto obvyklého prostředí byli náhle vytaženi a začali jsme lapat po dechu, poprvé jsme *prohlédli*.

Co určovalo hodnotu bitcoinu? Americký dolar byl zákonným platidlem, za nímž stála jedna z nejstabilnějších vlád na světě. Mohli jste ho používat k placení daní a obchodníci měli povinnost přijímat v něm platby. Ale proč by měl mít jakoukoli hodnotu řetězec číslic a písmen? Když byla v říjnu 2009 spuštěna bitcoinová burza s názvem

New Liberty Standard, obchodoval se na této burze jeden bitcoin (BTC) za méně než desetinu britské pence a tato cena byla odvozena od spotřeby elektřiny, kterou jeho těžba vyžadovala. Cena bitcoinu však časem začala žít svým vlastním životem. Na začátku roku 2011 překročila tržní cena hranici jednoho dolaru a v době, kdy mě Jason kontaktoval, stál jeden bitcoin více než sedmnáct dolarů.¹⁷ V raných dnech bitcoinu převážná část této hodnoty vycházela z přesvědčení, že bitcoin má potenciál stát se digitální obdobou zlata na celosvětovém trhu, a byla dána bezostyšným finančním spekulantstvím.

Co mě osobně na Bitcoinu přitahovalo, byl průkopnický zápal, který s ním byl spojený. „Je fascinující rozjíždět novou měnu,“ řekl mi Jeff Garzik, programátor Bitcoinu, jenž žil a pracoval v obytnáku Fleetwood Southwind z roku 1984 někde v Severní Karolíně.¹⁸ „Je to zřejmě první globální měna na světě.“ V Brooklynu jsem se potkal s Markem Suppesem, kutilem, který ve svém loftovém bytě ve čtvrti Bedford-Stuyvesant pracoval na bitcoinovém bankomatu. Jen o několik metrů dál byl další jeho kutilský projekt — podomácku vyrobený fúzní reaktor. Vousatý anarchist a sátek na hlavě, který na YouTube přispíval pod pseudonymem The Real Plato, vyjel z Connecticutu do Kalifornie ve stylu Jacka Kerouaca a celou cestu se snažil financovat pouze z bitcoinů. A sběratelé vzácných mincí snili o daleké budoucnosti, kdy budou lidé obchodovat s cennými bitcoiny — například s těmi z takzvaného Genesis bloku, prvního bloku v řetězci — stejně dychtivě, jako by to byly mince Double Eagle z roku 1933.¹⁹

I když jsem se nechal strhnout nadšením, jež bylo s Bitcoinem spojené, některé aspekty mi stále unikaly. Dokázal jsem pochopit, jak tyto nové peníze mohou být lákavé například pro někoho v Argentině, kde byla hyper-

inlace a měnové intervence realitou. Nebo v Mexiku,²⁰ na Filipínách,²¹ případně ve velké části Afriky, kde více než šedesát procent obyvatel nemělo bankovní účet.²² Ale nechápal jsem, co tolik štvě americké bitcoinery na tradičních finančních institucích. Federální pojištění vkladů fungovalo docela dobře a bankomaty byly snadno dostupné. Co tito lidé měli proti bankám?

Také mi dělalo problém pochopit technické principy, na kterých byl Bitcoin postavený, a způsob, jakým jsou spolu jednotlivé části systému provázané. Během setkání s lidmi z bitcoinové komunity se občas stalo, že někdo začal mluvit o „jednosměrné hašovací funkci“ nebo „Nashových rovnováhách“ a mně nezbylo než tiše přikyvovat, aniž jsem doopravdy věděl, o čem mluví. Jakmile jsem se vrátil domů, ponořil jsem se i na celé hodiny do studia těchto termínů, dokud mě z toho nebolely oči. A i když jsem si myslel, že jsem to konečně pochopil, jakmile jsem se to o pár dní později pokusil někomu vysvětlit, zjistil jsem, že je to nad moje síly. Když mi tedy Garzik, jeden z hlavních softwarových vývojářů projektu, řekl, že „Bitcoin je opravdu velmi těžký na pochopení“, pomohlo mi to zachovat si alespoň trochu sebevědomí.

Nakupování, ukládání, používání i samotné držení bitcoinů však také nebylo nijak snadné. A hodnota bitcoinu byla extrémně nestabilní.²³ Jen v měsíci, kdy jsem se o něm poprvé dozvěděl, nakrátko ztratil více než devadesát devět procent své hodnoty a klesl ze sedmnácti dolarů za minci na jeden cent. Internetové burzy, které nebyly nijak regulované a za své nakládání s bitcoiny nenesly žádnou odpovědnost, se často ukázaly být pochybnými podniky a jejich anonymní majitelé přijímali vklady od zákazníků, aby pak jednoho dne i s těmito penězi zmizeli. Dokonce i Mt. Gox, největší burza na světě, se stala obětí hackerů,

kteří z ní ukradli pětadvacet tisíc bitcoinů v hodnotě půl milionu dolarů.²⁴ Byl to právě tento útok, co způsobilo prudký propad ceny bitcoinu.

Pokud jste si nepřáli mít své bitcoiny uložené na burze, mohli jste mít soukromé klíče, obvykle řetězce padesáti jedna číslic a písmen, které byly kryptografickou obdobou hesla, uložené v takzvané „vlastní správě“ v bitcoinové „peněženke“, jež byla spíše takovým kroužkem na klíče. Své klíče jste si mohli opsat na kousek papíru, vyleptat na ocelovou destičku, kterou jste zakopali na zahradě, uložit na nový počítač nebo si je jednoduše zapamatovat. To byl samozřejmě nejlepší způsob, jak dosáhnout absolutně nezávislé kontroly nad svým majetkem. Představa, že si stačí zapamatovat svůj klíč, překročit mezinárodní hranice a v podstatě tak přesunout své peníze z jedné země do druhé, byla fascinující.

Samozřejmě nikdo vám nedoporučoval, abyste to takto dělali, protože i jediná zapomenutá číslice by znamenala, že o své peníze nadobro přijdete. Ačkoli tedy byla vlastní správa považována za ideál, který se promítl i do motta kryptoměnových nadšenců „Bez klíčů nejsou mince“, měla i své slabiny. Švýcarský programátor Stefan Thomas si uložil kopie klíčů ke svým 7 002 bitcoinům na tři místa. Svoji hlavní peněženku uložil na „virtuální stroj“, který byl zcela izolovaný od internetu, a zálohoval ji jak pomocí softwaru TrueCrypt, tak na zařízení IronKey, což je bezpečný hardwarový nosič dat připomínající USB flashdisk. Avšak během aktualizování svého operačního systému se mu jednou omylem podařilo smazat i virtuální stroj. A když se přihlásil do programu TrueCrypt, který měl uložen v Dropboxu, zjistil, že i ten byl vymazán. Ukázalo se, že mohl být přepsán ve chvíli, kdy byly více než dva stroje přihlášeny současně. A k nosiči IronKey jednoduše

ztratil heslo. Hodnota ztracených mincí v té době činila sto čtyřicet tisíc dolarů. „Strávil jsem celý týden tím, že jsem se snažil svá data zachránit,“ řekl mi Stefan, ale se svou snahou neuspěl. „Ta ztráta opravdu bolela.“

Na konci roku 2021 by tyto mince měly hodnotu 473 milionů dolarů.²⁵ Stefan však nebyl jediný, komu se něco podobného přihodilo. Podle odhadu analytické společnosti Chainalysis se ztratilo dvacet procent všech bitcoinů, které byly v oběhu.²⁶

Za svého prvního průvodce tímto ezoterickým světem jsem si vybral sympatického Gavina Andresena. Táhlo mu na jednačtyřicet, hnědé vlasy měl sčesané přes čelo a na nášivce jeho polokošile stálo „Ajťák“. Byl to tichý otec dvou dětí, který bydlel na předměstí.²⁷ Zatímco většina lidí svoji horší paměť okomentuje stylem: „Moje žena by vám mohla vyprávět, co všechno dokážu zapomenout“, a tím by toto téma uzavřeli, Gavin cítil potřebu ho dále rozvést: „Díval jsem se na data z výzkumu, která ukazovala, jak nespolehlivá naše paměť může být“, a vše vám podrobně vysvětlit.²⁸ A samozřejmě jezdil na jednokolce.²⁹

Bitcoin vstoupil do Gavinova života v příhodnou chvíli. V roce 2009 si jeho žena Michele, profesorka geologie na Massachusettské univerzitě, vzala tvůrčí volno a Gavin odešel z placené pozice na univerzitě, kde se zabýval strojovým učením, aby se k ní připojil.³⁰ Celá rodina se následně přestěhovala do Austrálie. Příštích šest měsíců strávil Gavin v Queenslandu, kde se ve svém volném čase věnoval mimo jiné žonglování s kokosovými ořechy, běhání po pláži, šnorchlování, ale stal se i obětí písečných mušek, zachránil vodnáře kobřího, vypil nespočet piv a po sedmnácti letech se rozhodl oholit si bradku.³¹ Ačkoli plánoval, že si po návratu do Spojených států založí start-up,

v květnu 2010 stále ještě nebyl pevně rozhodnutý, co konkrétně by mělo být jeho náplní.

Potom si však na blogu věnovaném technologiím přečetl příspěvek o několika projektech založených na open source softwaru,³² mezi nimiž byl i Bitcoin. Gavin vystudoval Princetonskou univerzitu a pracoval pro firmu Silicon Graphics. Seděl v zastupitelstvu malého města v Nové Anglii,³³ kde bydlel, aktivně se zajímal o místní školskou politiku³⁴ a jako dobrovolník pomáhal s webovými stránkami Amherstské ligy voliček.³⁵ Ale představa peněz, které nejsou kontrolovány elitní skupinou z Fedu, jej zaujala. Před hierarchickou strukturou řízení shora dolů dával přednost individuální svobodě, moudrosti davu a procesům, jež vycházejí od obyčejných lidí. Před revolucí dával přednost evoluci a věřil, že „lepšího světa dosáhneme malými kroky“.

Později se mi svěřil, že když se o Bitcoinu dozvěděl, nebyl si hlavně jistý, *jak takový systém vůbec může fungovat*. Lámal si hlavu nad tím, jak systém generuje nové mince a jak může zabránit dvojí útratě. Zkusil slovo „Bitcoin“ zadat do Googlu a dostal jen čtyři stránky výsledků. Tak si stáhl kód a začal ho číst. Bylo jasné, že jeho autor věděl, co dělá. Gavin si tedy software zkusil pustit a vytěžil několik mincí. Stejně „jsem nad tím stále přemýšlel, abych se přesvědčil, že tam nejsou žádné bezpečnostní slabiny“. Avšak v době, kdy jsme spolu mluvili, si byl už „ztraceně jistej, že tam žádná zásadní chyba není“.

Měsíc poté, co se o Bitcoinu dozvěděl, si Gavin založil platformu Bitcoin Faucet. Jeden bitcoin měl tehdy hodnotu půl britské pence. Gavin utratil celkem padesát dolarů za deset tisíc mincí a založil si webové stránky, kde je mohl rozdávat. Kdokoli tak na těchto stránkách mohl vyřešit CAPTCHA a získat pět bitcoinů zdarma. Smyslem

tohoto projektu bylo nalákat na tento experiment více lidí. Gavin si byl vědom, že peníze mají hodnotu jen tehdy, když je lidé používají.

Koncept platformy Bitcoin Faucet zapadal do rané fáze Bitcoinu, kdy mělo obchodování s touto měnou povahu poněkud svérázného komunitního projektu. Gavin například jednoho dne obědval s Davidem Forsterem, místním farmářem, který prodával ponožky z alpaky a jako platbu přijímal bitcoiny.³⁶ Mnoha bitcoinerům se také doslova protočily panenky, když Laszlo Hanyecz, jenž bydlel na Floridě, zaplatil deset tisíc bitcoinů v pizzerii Papa John's za dvě velké pizzy.³⁷ V pozdějších letech lidi nikdy neomrzelo přepočítávat cenu těchto pizz podle aktuální hodnoty bitcoinu — pizza za 690 milionů dolarů! „Vůbec toho nelituji,“ svěřil se mi Laszlo v době, kdy hodnota utracených bitcoinů byla přibližně osmdesát pět tisíc dolarů. „Ta pizza byla opravdu dobrá.“

Netrvalo dlouho a Gavin se aktivně zapojoval do diskusí na bitcoinovém fóru a Nakamotovi posílal části kódu, aby mohli společně opravit jakékoli díry, které se nevyhnutelně najdou v každém novém softwaru. O samotném Nakamotovi nevěděl skoro nic. Nikdy se nesetkali ani si spolu nevolali. Vše, co Gavin o svém spolupracovníkovi věděl, byly informace pocházející z jejich psané korespondence. Z těchto e-mailů a soukromých zpráv Gavin nabyl dojmu, že Nakamoto je systematický a soběstačný génius, který však někdy dokáže být trochu nedůtklivý. Co však Gavinovi dělalo větší starosti, byly právní záležitosti spojené s Bitcoinem. Americká vláda již v minulosti tvůrce alternativních měn trestně stíhala. Hrozilo mu snad zatčení? Ať už bylo nebezpečí jakékoli, Gavin této měně brzy věnoval všechny svůj čas, a to přesto, že si ho jeho žena Michele ráda dobírala slovy o „internetových rádobypenězích“.³⁸

Gavin na tomto projektu pracoval jednak ze zájmu, ale také proto, že obdivoval, jak chytrě se Nakamotovi podařilo Bitcoin přizpůsobit lidské povaze. Jakmile jste totiž bitcoiny vlastnili, chtěli jste se do celého systému zapojit — začali jste bitcoiny těžit, používat, propagovat nebo spolupracovat s ostatními na psaní kódu —, protože jen tak mohla být zítřejší hodnota vašich bitcoinů vyšší než ta dnešní. S každým růstem ceny se tak Gavinovi dostávalo odměny v reálném čase. Jeho zapojení do projektu bylo v podstatě „osvíceným sobectvím“.³⁹ Gavin se domníval, že by se bitcoin mohl stát hlavní světovou měnou a časem možná i nahradit dolar jako světovou rezervní měnu.⁴⁰

Ačkoli byl Bitcoin open source projektem, který vyžadoval zapojení každého jednotlivého člena, což jej alespoň teoreticky činilo odolným vůči individuálním zájmům, bylo nezbytné, aby se do jeho čela někdo postavil. A prvních dvacet měsíců v jeho čele stál právě Satoši Nakamoto. Byl to on, kdo publikoval novou verzi kódu. Ostatní vývojáři navrhovali patche a on vybíral a zapracovával ty, které se mu líbily.

Čtyři měsíce poté, co Gavin začal s projektem pomáhat, se zdálo, že se mu svojí oddaností, solidní znalostí informatiky a upřímným vztahem k bitcoinové komunitě podařilo získat si Nakamotovu důvěru. Nakamoto dal Gavinovi nejprve přímý přístup ke zdrojovému kódu.⁴¹ Poté, někdy kolem září 2010, se mu svěřil, že má hodně práce s jinými projekty a v příštích měsících mu předá kontrolu nad úložištěm zdrojového kódu na SourceForge⁴² a klíčem⁴³ k projektu, který umožňuje rozesílání naléhavých zpráv na všechny stroje, na nichž běží bitcoinový software. V případě open source projektů je možné právě tyto dva nástroje považovat za něco, co vám v nich propůjčuje vedoucí pozici. Gavin se tak fakticky stal hlavním vývojářem

projektu a vedl tým pěti dalších dobrovolníků, kteří v něm působili jako programátoři.⁴⁴

Během následujících několika měsíců se Nakamoto občas ozval, aby pomohl s řešením technických otázek, ale jeho izolacionistické sklony se dostávaly do stále většího konfliktu s Gavinovou otevřeností. Poté, co PayPal a Visa obstavily účty organizace WikiLeaks,⁴⁵ jedna frakce bitcoinerů navrhla, aby Bitcoin této kontroverzní organizaci pomohl, přičemž jejich spojení by mohlo ve výsledku pomoci s propagací Bitcoinu. „Pusťme se do toho,“ napsal jeden z nich na fóru nazvaném BitcoinTalk.⁴⁶ Nakamoto však tato výzva popudila:

Ne, do ničeho se pouštět nebudeme. Náš projekt se musí vyvíjet krok za krokem, aby jeho software mohl být postupně vylepšován. Vyzývám tímto lidi z WikiLeaks, aby se nepokoušeli využít Bitcoin. [...] Problémy, které byste s sebou přinesli, by nás v této fázi pravděpodobně zničily.⁴⁷

Myšlenka, že by WikiLeaks mohly přijímat dary v bitcoinech, se dostala až do časopisu *PC Magazine*, jenž tomuto tématu věnoval článek.⁴⁸ Ačkoli někteří bitcoineré měli radost z pozornosti, které se Bitcoinu takto dostalo, Nakamoto mezi ně rozhodně nepatřil. „Bylo by hezké, kdyby se nám této pozornosti dostalo v jiné souvislosti,“ napsal. „Ve WikiLeaks koplí do vosího hnízda a roj se teď žene na nás.“⁴⁹

Pro novináře, kteří o Bitcoinu psali, se Gavin přirozeně stal člověkem, jemuž volali jako prvnímu. Měl klidné, rozumné vystupování, uměl se držet politicky ve středu a nevadilo mu pracovat pod svým skutečným jménem, což z něj dělalo ambasadora Bitcoinu, jímž se Nakamoto nikdy

stát nemohl. Nicméně se zdálo, že Nakamoto Gavinovy styky s médii nese se stále větší nelibostí. Koncem dubna 2011 jej přes e-mail upozornil: „Byl bych rád, kdybys o mně pořád nemluvil jako o záhadné a tajemné postavě. Tisk toho využívá, aby nás popisoval jako pirátskou měnu.“⁵⁰

Bylo to naposledy, kdy Nakamoto s Gavinem komunikoval. Když jsem s Gavinem v červenci téhož roku poprvé mluvil, řekl mi, že s Nakamotem nebyl v kontaktu už „dva měsíce“. Poté, co jej 26. dubna Gavin e-mailem informoval — aniž si uvědomoval, že dělá něco, s čím Nakamoto nesouhlasí —, že o Bitcoinu promluví v ředitelství CIA v Langley ve státě Virginie, protože se její zástupci chtějí o této kryptoměně dozvědět víc, Nakamoto už na jeho zprávy nikdy neodpověděl.⁵¹ Zhruba ve stejnou dobu ještě napsal několik e-mailů alespoň jednomu dalšímu programátorovi, který byl do projektu zapojen.⁵²

A pak se odmlčel.

Zajímavý mýtus

„Takže víte, kdo je Satoši?“ zeptal jsem se.

Pokud to někdo věděl, musel to být Gavin.

„Neznám jeho skutečné jméno,“ odpověděl. „Doufám, že se jednoho dne rozhodne vystoupit z anonymity a já se s ním setkám, ale moc pravděpodobné to asi není.“

Gavin a další vývojáři se na některých věcech ohledně Nakamota shodli. Druhé místo, na kterém Nakamoto svoji bílou knihu zveřejnil, byla webová stránka P2P Foundation,¹ což je nezisková organizace podporující všechny druhy peer-to-peer sítí. Ve svém profilu na této stránce Nakamoto uvedl jako své bydliště Japonsko. Ale nikdo mu nevěřil, že je doopravdy Japonec. Jeho angličtina byla příliš dokonalá a byla z ní patrná přirozená jistota, která je typická pro rodilé mluvčí. Jeho projev naznačoval, že by mohl být Brit, nebo alespoň pocházet ze zemí Commonwealthu. Genesis blok měl v sobě uložen titulky z londýnských *Timesů* a jak ve zdrojovém kódu k Bitcoinu, tak ve svých příspěvcích na fóru BitcoinTalk Nakamoto upřednostňoval britský pravopis anglických slov, jako jsou *colour* (barva) a *optimise* (optimalizovat). Titulek z *Timesů* také ukazoval na možnou Nakamotovu motivaci při založení Bitcoinu: „Ministr financí se chystá poskytnout bankám druhou finanční injekci.“²

Bylo také pozoruhodné, jak důkladně se Nakamoto snažil svoji totožnost utajit. Při registraci domény bitcoin.org použil anonymizační službu nazvanou anonymousspeech.com, která sama byla registrována přes poskytovatele krátkodobého ubytování v Tokiu.³ Tato služba mu vytvořila e-mailovou adresu na doméně vistomail.com, jež umožňovala upravit datum a čas odeslání e-mailu. Třetí e-mailová adresa, kterou Nakamoto používal, patřila pod doménu gmx.com, dalšího poskytovatele bezplatného e-mailu. Michael Marquardt, který provozoval BitcoinTalk pod pseudonymem Theymos, byl přesvědčený, že Nakamoto skrýval svoji IP adresu pomocí systému TOR, stejného softwaru pro anonymní pohyb na internetu, jenž byl vyžadován pro přístup na stránky na darknetu, jako byl například Silk Road.⁴ A Nakamoto evidentně uměl komunikovat tak, aby neprozradil nic, co nechtěl. Gavin dosvědčil, že když Nakamoto odpovídal na technické otázky, bylo to, jako když „jeden aйтák mluví s druhým“, avšak jakýkoli pokus přimět ho, aby o sobě řekl něco osobního, byl vždy ignorován.⁵

Nakamotův kód byl příběhem sám o sobě. Gavin se domníval, že každý programátor má svůj vlastní autor-
ský styl,⁶ který jej odlišuje od ostatních programátorů, podobně jako se styl Kurta Vonneguta liší od stylu Jackie Collinové. Existovaly zde například náznaky, že Nakamoto může být o něco starší. Jeho styl kódování připadal Gavinovi trochu zastaralý⁷ a irský vývojář Mike Hearn, který pracoval pro Google ve Švýcarsku, si povšiml, že Nakamoto používal maďarskou notaci,⁸ což je konvence pro pojmenovávání proměnných, která byla v devadesátých letech oblíbená zvláště mezi programátory ve Windows. Bylo trochu neobvyklé, aby windowsák vedl open source projekt, protože hnutí za open source projekty

vzniklo převážně v reakci na uzavřené systémy, jako jsou právě Windows.

Pak zde byly další Nakamotovy vlastnosti, na nichž se však již vývojáři většinou neshodli. Podle Gavina patřil Nakamoto vzhledem ke svým schopnostem mezi nejlepších deset procent programátorů na světě.⁹ Ale Amir Taaki, jeden z prvních vývojářů Bitcoinu a hacker se zálibou v anarchismu — jednu dobu žil ve squatu v Londýně,¹⁰ později se stal aktivistou za výrobu zbraní na 3D tiskárnách¹¹ a také bojoval na straně Kurdů v syrské občanské válce¹² —, mi řekl, že si myslí, že Nakamoto nemá žádné vzdělání v oblasti informatiky. Ačkoli Amir považoval koncept Bitcoinu za dobře vymyšlený, kód byl podle něj špatně napsaný a vše bylo splácené do dvou nepraktických souborů, místo aby to bylo rozděleno do modulárních částí, jak by to zorganizoval profesionál. To ho přivedlo k domněnce, že Nakamoto by mohl být profesor:

Když strávíte programováním hodně let a pracujete s týmem lidí, začnete přemýšlet nad tím, jak byste mohli napsat daný zdrojový kód tak, aby byl srozumitelný co největšímu počtu lidí. Naučíte se tak shrnout věci jen na to nejdůležitější, abyste je udělali jasnými a pochopitelnými — naučíte se základní návrhové vzory a běžné způsoby organizace —, to však jsou zkušenosti, které akademici nemají. Inženýři si vždy kladou otázku: *Jak můžu danou věc vytvořit bez chyb a tak, aby byla snadno pochopitelná?*

Amir vystudoval matematiku a při četbě bílé knihy měl pocit, že její autor suverénně ovládá matematické a statistické nástroje.

Gavin se domníval, že kód Bitcoinu napsala malá skupina lidí, nebo dokonce jen jeden člověk.¹³ Když programátoři spolupracují v týmu, mají tendenci do svého kódu pravidelně vkládat komentáře, v nichž si navzájem vysvětlují, čeho má každý blok instruktivně docílit. Software Bitcoinu obsahoval jen minimum těchto komentářů. Byli zde však další, kteří tvrdili, že Bitcoin je příliš sofistikovaný a od samého začátku fungoval příliš hladce, než aby mohl být dílem jen jednoho člověka. Navíc bílá kniha používala první osobu množného čísla „my“. Z toho podle nich jasně vyplývá, že za jménem Satoši Nakamoto se musí skrývat skupina lidí nebo instituce.

V době, kdy jsem se o Bitcoinu dozvěděl, se někteří členové této nové komunity začínali ptát, kdo by Nakamoto mohl být. Avšak spekulace samozřejmě předcházely i jeho zmizení. V lednu 2011, tedy krátce předtím, než se nadobro vypařil, začali někteří bitcoineři Nakamotovi otevřeně projevovat úctu. Když začalo být jasné, že bitcoin potřebuje menší jednotky, rozhodla se komunita nazvat jednu setinu bitcoinu „satoši“.¹⁴ Ve stejném měsíci si někdo všiml, že Nakamotův poslední příspěvek na BitcoinTalku byl z 13. prosince.¹⁵ Propukla panika. Bylo možné, že Nakamoto z projektu odešel? Nebo snad zemřel? Kdo je nyní pověde? A několik lidí poprvé začalo přemýšlet o Nakamotově skutečné identitě.

Někdo přišel například s myšlenkou, že Nakamoto byl „něco jako Nicolas Bourbaki“,¹⁶ což byla malá skupina francouzských matematiků, kteří pod tímto kolektivním pseudonymem vydávali články v třicátých letech minulého

* Používání jednotky satoši se nakonec ustálilo na jedné stamiliontině bitcoinu.

století. Někdo jiný upozornil na to, že tato záhada Bitcoinu prospívá, protože ho dělá zajímavějším.¹⁷ Další zase tvrdil, že Nakamoto „jen potřebuje trochu soukromí. A to je dobře, protože to jasně ukazuje, že mu nejde o slávu, ale o ideály. Podle mě bychom to měli respektovat a jeho identitou se nezabývat“.¹⁸ Ale lidé si nemohli pomoci a dál přicházeli se jmény osob, které by se mohly za Nakamotovým pseudonymem skrývat.¹⁹ Mohl být Nakamotem spisovatel Neal Stephenson, jehož *Kryptonomikon* předpověděl existenci digitálních peněz? Nebo Australan Julian Assange, který založil WikiLeaks? Nebo snad ruský génius Grigorij Perelman, jenž žil poustevnickým životem a odmítl převzít cenu za přínos matematice, která byla spojena s odměnou ve výši jednoho milionu dolarů?

Ukázalo se však, že nebyl žádný důvod k panice. Gavin 13. ledna komunitu ujistil sdělením, že mu Nakamoto toho dne napsal e-mail, aby ho upozornil na „základní chybu [...] A měl jen hodně práce“.²⁰ O tři měsíce později, 16. dubna 2011, však účastník BitcoinTalku, který vystupoval pod jménem Wobber, poznamenal, že „od posledního [Nakamotova] příspěvku na tomto fóru uplynula už dlouhá doba“, a spustil nové vlákno nazvané: „Kdo je Satoši Nakamoto?“

Wobber poukázal na širokou škálu odborných znalostí, jíž Nakamoto disponuje, a zároveň na jeho podivné chování — vymyslel naprosto inovativní systém, odmítl za něj přijmout uznání nebo využít svého postavení a zmizel, aniž komukoli cokoli řekl. Někdo přirovnal Nakamota k Zorrovi nebo Davidovi v masce, který namířil svůj prak na Goliáše v podobě bank a vlád. Někdo jiný se zase zamyslel, jestli Nakamoto ve skutečnosti nemohl být Gavin Andresen.²¹ U Gavina rozhodně existovala spojitost s Austrálií, protože se tam narodil a do Ameriky se odstěhoval až později v dětství,²² což by mohlo vysvětlit Nakamotovo charakteristické

používání amerického i britského pravopisu. Ale byly zde i pochybnosti: Copak by se Nakamoto namáhal vytvořit falešnou postavu jen proto, aby mohl komunikovat sám se sebou?

Vzhledem k minimálnímu množství indicií se hledači Nakamotovy pravé identity vrhali i po té nejmenší stopě. Mohlo je snad k němu dovést jeho jméno? Volně přeloženo z japonštiny může Satoši Nakamoto znamenat spojení „ústřední zpravodajská služba“.²³ Možná to naznačovalo, že do založení Bitcoinu byli zapojeni špioni. Možná Národní bezpečnostní agentura rozehrála velkou hru a založila finanční síť, pomocí níž by mohla vyplácet své agenty v terénu. Nebo se jí chystala použít jako past, která by v jejich protivnicích vytvořila falešný pocit bezpečí, a zatímco na ní budou obchodovat, špioni ve Fort Meade budou sledovat každý jejich pohyb.

Ta myšlenka nebyla tak šílená, jak mohla znít. Americká námořní výzkumná laboratoř vytvořila The Onion Router, anonymizující software známý jako TOR, který umožnil přístup na darknet.²⁴ FBI později tajně vytvořila svoji vlastní komunikační službu ANOM a řadu šifrovaných telefonů, které byly nevědomky používány členy organizovaných zločineckých skupin, což vedlo k více než osmi stům zatčených osob.²⁵ A pak tu byl případ tří výzkumných pracovníků z kryptologické divize kanceláře pro výzkum a technologii zabezpečení informací v rámci NSA, kteří v létě roku 1996 vydali jako interní dokument dlouhou studii s názvem: „Jak vytvořit mincovnu: kryptografie anonymní elektronické hotovosti“, která byla později zveřejněna.²⁶

Anglickou podobu Nakamotova jména lze také vykládat jako kufříkové slovo složené z názvů velkých technologických firem — SAMSUNG, TOSHIBA, NAKAMICHI,

MOTOROLA²⁷ —, takže v pozadí možná stál tajný spolek obchodních korporací. Uživatelé Redditu ve snaze dešifrovat jeho jméno spojili své síly a přišli s teorií, že by mohlo být přesmyčkou mimo jiné následujících vět: „Ma, I took NSA’s oath“ (Mami, složil jsem slib NSA) a „So a man took a shit“ (Takže se muž vysral).²⁸

Tehdy se lidé začali zabývat otázkou, proč Nakamoto vlastně použil pseudonym. Bylo to snad kvůli nepříjemnostem spojeným se statusem celebrity? Nebo kvůli minulosti, kdy vlády kryptografy pronásledovaly? Snažil se vyhnout šikaně? Nebo „nepřátelům, kteří mohli s Bitcoinem přijít“? „Možná si přál jen zůstat v anonymitě.“ Možná nechtěl, aby byl tento riskantní podnik spojován s jeho dalšími podnikatelskými aktivitami.

V květnu téhož roku se programátor a autor Gwern Branwen, který sám vystupoval pod pseudonymem a psal blogy, jež byly oblíbené mezi čtenáři v Silicon Valley, pokusil načrtnout svoji představu o Nakamotově původu. „Satoši může být *kdokoli*,“ napsal. Bitcoin podle něj nevyžadoval „žádné velké intelektuální objevy matematického či kryptografického rázu“, šlo spíše o chytré propojení stávajících technologií. „Satoši tudíž nemusí mít žádné odborné vzdělání v oblasti kryptografie a může být jen programátorem samoukem!“²⁹

Stefan Thomas, švýcarský bitcoiner, jenž ztratil více než sedm tisíc bitcoinů, přistoupil k hledání odpovědi na tuto otázku metodicky a vytvořil graf, který mapoval časová razítka každého z více než pěti set Nakamotových příspěvků na fórech.³⁰ Tento graf ukázal na znatelný pokles aktivity během nočních hodin v Severní Americe. „Mike přísahá, že má britský přízvuk,“ řekl mi Stefan a měl samozřejmě na mysli vývojáře Bitcoinu Mikea Hearn. Stefan sám měl vágní představu o tom, kdo by měl Nakamoto

být — i kdyby to nebyl Američan, měl by to být člověk žijící ve Spojených státech. „Occamova britva,“ řekl. Jednoduché vysvětlení má vždy přednost před komplikovanějším.

Když však Stefan zveřejnil svůj graf na BitcoinTalku, setkal se jeho příspěvek s vlnou nesouhlasu. Nebylo snad pravděpodobnější, že Nakamoto trávil čas na Bitcoinu v době, kdy *nepracoval*? V takovém případě by doba, kdy zveřejňoval své příspěvky, odpovídala západní Evropě. „Odkdy hacker v noci spí?“ namítl někdo. Někdo jiný zase poznamenal, že by se tento vzorec chování měl o víkendech lišit, ale nelišil.

Dan Kaminsky, dvaatřicetiletý výzkumník zabývající se zabezpečením počítačů, který se proslavil o tři roky dříve odhalením technické chyby, jež mohla ohrozit celý internet,³¹ se domníval, že Nakamoto by mohla být skupina lidí pracujících v bance. „Mám podezření, že za Satošim stojí malý tým v nějaké finanční instituci,“ řekl mi Dan. „Mám prostě takový pocit.“

Nakamoto byl „zajímavý mýtus“, dodal Dan. „Ale nemyslím si, že by pro Bitcoin byl zas tak důležitý. Bitcoin je větší než Satoši.“ Tento názor jsem slyšel lidi zmiňovat opakovaně. Představa Nakamota jako neznámé bytosti, která se schovává za pseudonymem a zřekla se své hmotné podoby, se stala neoddělitelnou součástí koncepce Bitcoinu.

Neustále jsem musel o Bitcoinu přemýšlet. Neustále jsem musel přemýšlet o člověku, který jej vymyslel. Možná nemuselo být tak těžké ho najít. Někdy to vypadá, že se na internetu jen dokola recykluje stejný obsah. Sherlockové s notebooky vytvářeli grafy časových razítek a zkoumali nejrůznější jména, ale nikoho z nich nenapadlo zvednout telefon a jednoduše zavolat. Domněnky, které jsou

na internetu považovány za fakta, se často rozplynou, když je konfrontujete s realitou. Třeba Nakamoto celou dobu někde sedí na ergonomické herní židli, netrpělivě do stolu bubnuje prsty, na nichž má mozoly od klávesnice, a čeká, až někdo jako já zavolá. Napsal jsem mu tedy na adresu `satoshin@gmx.com`, o které mi Gavin řekl, že ji dříve používal, a požádal ho o rozhovor.

Zatímco jsem čekal na jeho odpověď, kontaktoval jsem dvě osoby, u nichž existovala vysoká pravděpodobnost, že by Nakamotem mohly být. Jednou z nich byl britský kryptograf Adam Back, jenž v devadesátých letech vytvořil software Hashcash, který chránil před spamem a používal výpočetní hádanky — takzvané *proof of work* —, aby jiné stroje přiměl prokázat, že mají „čestné úmysly“. ³² Jednalo se o stejnou technologii, kterou Nakamoto později použil v Bitcoinu. O Backovi bylo veřejně známo, že i když sám Nakamota neznal, byl prvním člověkem, jehož Nakamoto v srpnu 2008 kontaktoval, aby se zeptal, jak má správně citovat Hashcash ve své bílé knize. ³³

Vyměnili jsme si několik e-mailů a já se přiklonil k názoru Amira Taakiho, který mi řekl, že „Adam má svůj zažitý styl napříč všemi svými projekty. A jeho styl se od Satošiho liší“. Amir mi vysvětlil, že Back se řídí běžnými konvencemi programování, píše v jazyku C a programuje v Unixu/Linuxu, zatímco Nakamoto je, co se týče stylu, nevyzpytatelný, píše v jazyku C++ a používá Windows. Back byl tou dobou také znám jako stoupenec absolutního práva na soukromí, tedy někdo, komu by pravděpodobně vadily kompromisy, které Bitcoin učinil v oblasti ochrany anonymity. Skutečnost, že každý mohl vidět vše, co se na blockchainu odehrává, byla paradoxně jak smyslem, tak i rizikem tohoto systému. Nemohl jsem také uvěřit, že by někdo, kdo se snaží vyhnout odhalení a ve své bílé