THE BACKDOOR FORK

How Satoshi Changed Bitcoin's Rules in Secret — Three Times.

And Why the 1MB Hidden Commit May Have Broken the Partnership That Built Bitcoin.

SOURCE: IAN GRIGG — FINANCIAL CRYPTOGRAPHY IN 7 LAYERS, 2000

"The Issuer of the security cannot change the terms of the contract in any way without offering to the user terms for exchange."

AUTHOR

By Niraj Sinha

Founder & Creator, UCPI | Oxford Blockchain Strategy Programme, Saïd Business School

May 2026

SERIES CONTEXT

This is the second investigation in the Ghost in the Timechain series. The first established a forensic case — built entirely from primary sources — identifying Ian Grigg as the probable economic architect of Bitcoin, with Gary Howland as the original candidate for the cryptographic co-author. An update on Howland's status is provided in this report.

Every claim in this article is anchored to a primary source. Where a claim is interpretive — connecting verified evidence to a reasoned theory — it is explicitly identified as such. That distinction is the line between forensic journalism and conspiracy theory. This investigation will not cross it.

TABLE OF CONTENTS

PART ONE

The Vocabulary Bitcoin Never Gave You

You think Bitcoin is decentralised. You've been told no single person controls it. You've been told the community decides. You've been told the rules can only change if everyone agrees.

You were misled.

Not by a conspiracy. Not by a cover-up in the dark. But by something far more uncomfortable — a documented historical record sitting in the Bitcoin Wiki, in GitHub commit logs, in archived cypherpunk emails, and in the words of the people who were actually there. A record that has been publicly available since the events happened, that nobody has ever assembled into a single framework — until now.

Three times in Bitcoin's first thirteen months, the consensus rules were changed without telling anyone. Three times, the community woke up to a different protocol than the one they went to sleep with. Once, those who found the code were explicitly told to keep their mouths shut.

The word for what happened doesn't exist yet in Bitcoin's vocabulary. **It does now.**

DEFINING THE THREE FORK TYPES

A Hard Fork changes Bitcoin's rules in a way that creates a chain split. Old nodes reject the new blocks. The community divides. Hard forks are loud, contentious, public. Visible to everyone because they have to be.

A Soft Fork tightens Bitcoin's rules in a backward-compatible way. Old nodes still accept new blocks. It requires majority miner support, signalling, coordination, public discussion. Soft forks are quieter than hard forks, but they are not silent. The community knows they are happening.

And now: the category nobody in seventeen years of Bitcoin journalism has formally named.

DEFINING THE BACKDOOR FORK

A Backdoor Fork is a protocol rule change that:

1. Is deployed without public announcement or community knowledge.
2. Is hidden inside misleading commit messages designed to conceal what the code actually does.
3. Is enforced — when discovered prematurely — by instructing discoverers to maintain silence.
4. Gives the deployer unilateral control over the network's development trajectory.
5. Cannot be challenged, debated, or reversed by the community because the community does not know it is happening.

■ DEFINING MOMENT

This is not a metaphor. This is a precise description of three documented events in Bitcoin's first thirteen months. All three are sitting in primary sources that anyone can verify right now. The Bitcoin Wiki's own documentation calls the commits "sneaky." The people who were there have been on the public record about the silence they were asked to maintain since at least 2015. The Backdoor Fork happened. Three times. And nobody ever gave it a name — until now.

PART TWO

The Three Backdoor Forks

Primary Source Evidence

BACKDOOR FORK #1

The Block 31,000 Time-Bomb

November 2009

Bitcoin launched on January 3, 2009. By November 2009 it had been running for ten months. The community was tiny — a few dozen technically sophisticated people running nodes, testing the system, watching the blockchain grow block by block. They believed they understood what they were running.

They did not know that a protocol rule change was hardcoded inside the software, set to fire automatically when the blockchain reached block 31,000.

SOURCE: BITCOIN OPTECH — BITCOINOPS.ORG/EN/TOPICS/SOFT-FORK-ACTIVATION/

> *"The earliest known soft fork was implemented in Bitcoin 0.1.6 (released November 2009) and was hardcoded to activate at block 31,000, which occurred on 22 December 2009. This hardcoded height activation mechanism was used for at least one other early soft fork when most development was done by Satoshi Nakamoto."*

On 21 December 2009, every person running a Bitcoin node was operating under one set of rules. On 22 December 2009, block 31,000 was mined, and the rules changed. Nobody voted. Nobody was consulted. Nobody was warned.

The mechanism was a time-bomb embedded in the code — a predetermined trigger that would fire at a predetermined moment, changing the behaviour of every node on the network, regardless of what any of those node operators wanted or knew. This is the prototype Backdoor Fork. The creator of Bitcoin established in the very first software release that protocol governance was a unilateral decision.

BACKDOOR FORK #2

The Hidden 1MB Block Size Limit

July–September 2010

This is the one that broke everything. Not immediately. Not obviously. Not in a way that anyone saw coming in 2010. But the block size limit introduced in two hidden commits in the summer of 2010 is the direct cause of the block size war — Bitcoin's most destructive internal conflict. The 2017 chain split that created Bitcoin Cash. The fee crisis. The Lightning Network's existence as a second-layer workaround. Fifteen years of governance paralysis.

DATE	COMMIT HASH	STATED MESSAGE	ACTUAL CHANGE	WIKI LABEL
Jul 15, 2010	a30b56e	"fix openssl linkage probl	Embedded MAX_BLOCK	"Sneaky" UASF commit
Sep 7, 2010	8c9479c	"don't count payments un	Enforced block size at co	"Sneaky" UASF commit

■ DOCUMENTED EVIDENCE

SNEAKY. That is the Bitcoin Wiki's own word. Not a critic's characterisation. Not an opposition blogger's editorial. The official reference documentation for Bitcoin's most controversial protocol change describes its introduction as SNEAKY. The Bitcoin Scalability FAQ states: "Neither the July nor the September commit message explains the reason for the limit."

THE SUPPRESSION ORDER

SOURCE: THEYMOS, 2015 — CITED IN COINTELEGRAPH, 2017

"Satoshi never used IRC, and he rarely explained his motivations for anything. In this case, he kept the change secret and told people who discovered it to keep it quiet until it was over with so that controversy or attackers wouldn't cause havoc with the ongoing rule change."

■ FORENSIC FINDING

He kept the change secret. He told people who discovered it to keep it quiet. The creator of a supposedly decentralised, trustless, community-governed protocol made a unilateral architectural decision that would define Bitcoin's scalability for the next fifteen years — hid it in commits whose titles described something else entirely — and personally suppressed its disclosure until after deployment.

THE ORIGIN OF THE 1MB LIMIT — HAL FINNEY'S DoS CONCERN

SOURCE: RAY DILLINGER (CRYDDIT), FEBRUARY 2015

"I'm the guy who went over the blockchain stuff in Satoshi's first cut of the bitcoin code. Satoshi didn't have a 1MB limit in it. The limit was originally Hal Finney's idea. Both Satoshi and I objected that it wouldn't scale at 1MB. Hal was concerned about a potential DoS attack though, and after discussion, Satoshi agreed... But all 3 of us agreed that 1MB had to be temporary because it would never scale."

The creator of Bitcoin initially objected that 1MB wouldn't scale. He was persuaded by Hal Finney's denial-of-service argument. He then implemented the limit secretly, in misleading commits, with instructions to discoverers to stay quiet — and left the project before the community grew large enough to challenge it. A temporary emergency measure, deployed without announcement, became the permanent architectural constraint that tore the Bitcoin community in half seven years later.

BACKDOOR FORK #3

The Alert Key — A Master Switch Nobody Voted For

August 2010

On August 15, 2010, an unknown attacker exploited a critical vulnerability in Bitcoin's code. Block 74,638 contained a transaction that created 184,467,440,737 bitcoins — 184 billion, against a total supply cap of 21 million. For a brief, terrifying window, the foundational scarcity guarantee of Bitcoin had been broken.

But in the aftermath, something was added to the protocol that nobody had asked for and nobody had been told about: a master cryptographic key that could broadcast signed emergency messages to every node on the Bitcoin network simultaneously — and force those nodes into a restricted "safe mode", disabling normal transaction operations across the entire global network with a single signed message.

DETAIL	THE ALERT KEY SYSTEM
Source	Bitcoin Wiki, Alert System article
Implementation	Hastily implemented by Satoshi Nakamoto after the value overflow in
Key Holders	Three named individuals: Satoshi Nakamoto, Gavin Andresen, They
Active Period	Bitcoin 0.1 (2010) through Bitcoin 0.13.0 (2016) — six years
Uses	Twelve emergency broadcast uses, 2012–2014
Resolution	Private key published in 2018 to ensure it could never be used again

■ FORENSIC OBSERVATION

A supposedly decentralised currency with no central authority had, built into its protocol without community knowledge, a cryptographic master switch that three individuals could use to push the entire global network into safe mode with a single signed message. One key. Three holders. Six years. Twelve uses. This is structurally identical to a central bank's emergency intervention power — the very kind of centralised override mechanism that Bitcoin was supposedly designed to make impossible.

PART THREE

Update: Gary Howland Eliminated

In the first Ghost in the Timechain report, Gary Howland — co-founder of Systemics with Ian Grigg, designer of the SOX capabilities-based payment protocol, and the strongest unpursued candidate for Bitcoin's second author — was identified as the most credible forensic match for the cryptographic layer of Bitcoin's genesis codebase.

Subsequent research has definitively eliminated him as a candidate.

✗ CANDIDATE ELIMINATED

Gary Howland died in 2002. This is confirmed by an obituary post authored by R.A. Hettinga in December 2003 on the mac_crypto mailing list, archived at doomedengineers.wordpress.com. Howland's death predates Bitcoin's known development window by at least five years. He cannot be a co-author of Bitcoin's code.

This elimination redirects the inquiry toward the next most credible candidate for the cryptographic author of Bitcoin's protocol layer. That candidate has been hiding in plain sight — named in the Bitcoin whitepaper itself, confirmed as the first person Satoshi Nakamoto ever contacted, identified in the 2026 New York Times investigation by John Carreyrou as the most likely Satoshi candidate, and documented in direct mailing list contact with Ian Grigg since 1997.

His name is Adam Back.

PART FOUR

Adam Back as Bitcoin's Second Author

The Forensic Case

Adam Back is the inventor of Hashcash — the proof-of-work function that Bitcoin adopted as its consensus mechanism. He is the only person cited by name in the body text of the Bitcoin whitepaper. He is the first human being Satoshi Nakamoto ever contacted — before the whitepaper was even published.

SOURCE: ADAM BACK — CONFIRMED PUBLIC STATEMENT

"I got the first email that anybody got from Satoshi in August 2008 before the Bitcoin paper was released."

Five Back–Satoshi emails were published via UK court filing in February 2024, reported by Bitcoin Magazine. They confirm that Satoshi reached out to Back before reaching out to any other figure in the cryptography community — before Wei Dai, before Hal Finney, before Nick Szabo.

In April 2026, the New York Times investigation by John Carreyrou — the most rigorous Satoshi identification attempt ever published by a mainstream outlet — named Adam Back as the most likely Satoshi candidate. Back denied it. But the Times documented that when confronted with specific evidence, Back was unable to adequately explain it beyond categorical denial and refused to provide the metadata attached to his early emails with Satoshi.

■ FORENSIC OBSERVATION
A man with nothing to hide provides the metadata.

THE CRYPTOGRAPHIC PROFILE MATCH

FORENSIC CRITERION	ADAM BACK'S PROFILE
Proof-of-work mechanism	Inventor of Hashcash (1997) — the direct PoW predecessor Bitcoin a
Adversarial systems thinking	Entire career built on DoS prevention via computational cost
Cryptographic expertise	University of Exeter PhD; decades of academic cryptography
First Satoshi contact	Confirmed: August 2008, before the whitepaper was released
NYT identification	Named by Carreyrou (2026) as highest-confidence Satoshi candidate
Whitepaper citation	Only person cited by name in the whitepaper body text
Mailing list → Grigg	Documented 1997 cypherpunk thread — 11 years before Bitcoin
Blockstream CEO	2014–present; business model depends on small blocks

PART FIVE

The Grigg–Back Partnership

And Why the 1MB Commit May Have Broken It

THE GRIGG PRINCIPLE — WHAT THE HIDDEN COMMIT VIOLATED

SOURCE: IAN GRIGG — FINANCIAL CRYPTOGRAPHY IN 7 LAYERS, 2000 | IANG.ORG/PAPERS/FC7.HTML

"This ensures that the Issuer of the security cannot change the terms of the contract in any way without offering to the user terms for exchange."

This is the philosophical bedrock of Grigg's entire body of work. The Issuer — the creator of the instrument — cannot unilaterally change the rules. Any change requires offering holders an exchange. This is Bitcoin's immutability principle as Grigg articulated it in his own theoretical framework.

Now look at what actually happened in September 2010. The hidden 1MB block size limit was deployed unilaterally, secretly, without community knowledge, without any process, without asking anyone. **This directly and comprehensively violates Grigg's own stated foundational principle.**

■ FORENSIC INTERPRETATION

If Grigg is the economic architect of Bitcoin — the designer of its contract layer, its monetary philosophy, its governance model — then the hidden 1MB commit is not consistent with his design philosophy. It is consistent, however, with the priorities of a cryptographer whose primary concern is network security and DoS prevention. Someone who, faced with transaction flooding attacks of mid-2010, made a rapid unilateral technical decision using the adversarial systems thinking that has defined his entire career. That is Back's decision-making profile. Not Grigg's.

THE PROBABLE RUPTURE

The interpretive claim — explicitly marked as such — is the following: if Bitcoin was built by a two-person partnership between Ian Grigg (economic architect) and Adam Back (cryptographic implementer), the September 2010 hidden 1MB commit represents the moment that partnership fractured.

Grigg designed Bitcoin to serve ordinary users with fast, cheap, scalable transactions. His published philosophy is explicit: the system should scale to meet demand, the issuer cannot unilaterally restrict the terms, the network serves its users. Back deployed a unilateral block size cap — in secret, without community knowledge, without Grigg's published governance philosophy — as an adversarial security measure.

The interpretive conclusion: Back made a decision that violated Grigg's architectural principles. And because the decision was made secretly, in misleading commits, there was no mechanism for Grigg to challenge it publicly without revealing who he was. The very operational security that had protected the project now made it impossible for one co-author to publicly object to the other's decision.

SOURCE: IAN GRIGG (@IANG_FC) — X POST, MARCH 4, 2025 (REPLY TO CAMERON WINKLEVOSS ON US STRATEGIC BITCOIN RESERVE)

"Bitcoin is lost."

That is not an investor's lament. That is not a developer's frustration. That is an architect watching his building get renovated into something he never intended, by forces he cannot publicly challenge without revealing who he is.

Two words. Fifteen years of accumulated grief. "Bitcoin is lost."

PART SIX

The Block Size War Reframed

A Dispute Between Co-Authors

For fifteen years, Bitcoin's most destructive internal conflict has been described as a genuine technical debate between smart people with different visions for the network. Big blockers versus small blockers. On-chain scaling versus second-layer solutions. That framing is not wrong. But it is incomplete.

The block size war is also the story of what happens when a hidden decision — made unilaterally, deployed secretly, without community knowledge — eventually comes into contact with a network that has outgrown it.

Satoshi himself indicated on the public record in 2010 that the 1MB limit was temporary. Gavin Andresen stated in 2014: "The plan from the beginning was to support huge blocks. The 1MB hard limit was always a temporary denial-of-service prevention measure." Ray Dillinger confirmed this. Every person who was in the room when the limit was introduced has said, on the public record, that it was never meant to be permanent.

And yet, when the time came to change it, the small-block position held. Lightning Network was built instead. Bitcoin Cash split off. The 1MB limit remained.

Who was the most prominent, most technically credible, most institutionally powerful voice for keeping blocks small? Adam Back — CEO of Blockstream, the company that employs much of Bitcoin Core's development team and whose entire product suite depends architecturally on Bitcoin's base layer remaining constrained.

■ FORENSIC IMPLICATION

If Adam Back is one of Bitcoin's co-authors — the person whose security instincts drove the unilateral decision to impose the 1MB limit in the first place — then his decade of advocacy for keeping blocks small is not merely a governance position. It is a defence of his own unilateral decision. The Backdoor Fork he deployed in September 2010 became the Blockstream business model in 2014. The temporary emergency measure became a permanent revenue architecture.

The block size war was not a community disagreement. It was the economic architect and the cryptographic implementer — separated by fifteen years of pseudonymous distance, unable to acknowledge each other in public — fighting about a decision that was made in private, in secret, in September 2010.

— Forensic interpretation

PART SEVEN

The Documented Connections

Mailing List Evidence

For a two-author model to hold, Grigg and Back must have known each other well enough, and for long enough, to co-build one of the most consequential pieces of software in financial history. The cypherpunk mailing list archive provides the primary source evidence. All of the following is verifiable at mailing-list-archive.cryptoanarchy.wiki.

GRIGG ↔ BACK — NOVEMBER 1997

DATE	AUTHOR	THREAD
1997-11-04	Adam Back [University of Exeter]	Re: Copyright commerce and the street musi
1997-11-06	Ian Grigg [Systemics Ltd]	Re: Copyright commerce and the street musi

Both posted. Same thread. Same conversation. Documented. Timestamped. Eleven years before Bitcoin's whitepaper was published.

GRIGG ↔ WEI DAI — DECEMBER 1998

DATE	AUTHOR	THREAD
1998-12-11	Ian Grigg	Re: alternative b-money creation
1998-12-22	Ian Grigg	Re: alternative b-money creation (second po

Wei Dai's b-money = Reference [6] in the Bitcoin whitepaper. Ian Grigg was directly discussing b-money with its creator in December 1998 — a decade before Bitcoin launched. When Satoshi later emailed Dai about Bitcoin, he was reaching out to a man Grigg had been corresponding with for ten years.

FORENSIC SUMMARY

Grigg had documented, timestamped, verified direct contact with both Adam Back (the cryptographic architect) and Wei Dai (author of Bitcoin's most important intellectual predecessor) — a full decade before Bitcoin was announced. The world has been searching for who knew Satoshi. The cypherpunk archive proves Ian Grigg knew everyone Satoshi cited — personally, by email, in active conversation.

THE ALERT KEY — WHERE BOTH AUTHORS' DOMAINS CONVERGE

The Alert Key sits at the intersection of both proposed authors' domains and is forensically revealing about the collaboration structure.

In Grigg's Ricardo system, the Issuer holds emergency authority — an explicit feature of his governance design. The Alert Key is Bitcoin's implementation of exactly this principle. But implementing the key correctly — designing the asymmetric cryptography, ensuring it cannot be forged, ensuring it propagates correctly to every node — requires sophisticated cryptographic engineering. This is Back's domain, not Grigg's.

■ INTERPRETIVE SYNTHESIS — EXPLICITLY MARKED

INTERPRETIVE SYNTHESIS: Grigg designs the governance principle. Back builds the key. Together, they held it. Together, they built the mechanism that gave Bitcoin's creators continued extraordinary power over a network publicly presented as having no centre.

PART EIGHT

The Governance Question Bitcoin Has Never Asked Itself

Bitcoin asks everyone who touches it to trust the code, not the human. The code is the law. The rules are the rules. No individual can override them.

The Backdoor Fork is the primary source evidence that this principle was not applied to Bitcoin's own creation. The rules were changed secretly, three times, in the first thirteen months. The community was not consulted. Discoverers were told to stay quiet. An emergency override key was built in without announcement and held for six years by three named individuals.

Bitcoin became decentralised eventually. It was not born that way.

The question that follows is the one Bitcoin has never seriously asked itself: if the 1MB limit was imposed through a Backdoor Fork — unilaterally, secretly, in apparent violation of the governance philosophy that Bitcoin publicly espouses — does the community have a legitimate claim to revisit it through the open, transparent, community-driven process that should have governed its introduction in the first place?

That is not a technical question. It is a governance question. And it has never been asked in the right frame — because until now, nobody had a name for what happened in September 2010.

It was a Backdoor Fork. And it changed everything.

CURRENT WORKING THEORY — UPDATED MAY 2026

Bitcoin was created by a team of 2+ authors	8.5 / 10
Ian Grigg was the economic architect of Bitcoin	8.0 / 10
Gary Howland — Bitcoin's cryptographic author	✗ ELIMINATED
Adam Back — most credible second author candidate	7.5 / 10 ▲ NEW
1MB hidden commit reflects Back's instincts, not Grigg's	7.0 / 10 ▲ NEW
Grigg–Back partnership fractured over the 1MB Backdoor Fork	6.5 / 10 ▲ NEW

FACT-CHECK TRANSPARENCY

Primary Sources & Verification

BACKDOOR FORK #1 — Block 31,000

Bitcoin Optech, "Soft Fork Activation," bitcoinops.org/en/topics/soft-fork-activation/ — direct quote. Verified and publicly accessible.

BACKDOOR FORK #2 — Hidden 1MB Limit

Bitcoin Wiki Scalability FAQ — cites commit hashes a30b56e (July 15, 2010) and 8c9479c (September 7, 2010). Bitcoin Wiki Block Size Limit Controversy — designates both commits as "Sneaky soft-forking UASF commits." Theymos 2015 statement — Cointelegraph 2017. Ray Dillinger 2015 — maxlaumeister.com.

BACKDOOR FORK #3 — Alert Key

Bitcoin Wiki, Alert System article. Three key holders, twelve uses 2012–2014, retired 2016, key published 2018. Confirmed across Bitcoin Wiki, TradingView News, Bitnewsbot.

GARY HOWLAND DIED 2002

R.A. Hettinga obituary post, December 2003, mac_crypto mailing list. Archived at doomedengineers.wordpress.com.

ADAM BACK — FIRST SATOSHI CONTACT

Back's own confirmed public statement. Five Back–Satoshi emails published via UK court filing, February 2024, reported by Bitcoin Magazine.

2026 NYT CARREYROU INVESTIGATION

Confirmed across Adam Back's Wikipedia article, Brave New Coin, Coinpedia, and multiple outlets. April 2026.

GRIGG FC7 PRINCIPLE

Ian Grigg, "Financial Cryptography in 7 Layers," 2000. Available at iang.org/papers/fc7.html and mirrored at the Satoshi Nakamoto Institute.

GRIGG–BACK 1997 MAILING LIST

Cypherpunk archive at mailing-list-archive.cryptoanarchy.wiki — "Re: Copyright commerce and the street musician protocol," November 1997. Both iang@systemics.com and aba@dcs.ex.ac.uk appear in thread.

GRIGG–WEI DAI 1998 MAILING LIST

Same archive — "Re: alternative b-money creation," December 11 and 22, 1998. Ian Grigg posted twice.

GRIGG "BITCOIN IS LOST"

Screenshot confirmed. X post by @iang_fc, March 4, 2025, in reply to Cameron Winklevoss post on Strategic Bitcoin Reserve.

ABOUT THE AUTHOR

Niraj Sinha is the founder and creator of Unified Crypto Payments Identity (UCPI), a graduate of the Oxford Blockchain Strategy Programme at Saïd Business School, University of Oxford.

He is an active blockchain developer and former cryptocurrency miner with deep hands-on experience on Bitcoin Core's wallet encryption layer — including the CKey and CMasterKey classes that define how Bitcoin's private keys are stored and protected.

Prior to his blockchain work, he served as a Sarbanes-Oxley (SOX) Auditor at Reuters, where he developed the forensic discipline of tracing every transaction back to its originating control. He brings this same audit methodology to his investigation of Bitcoin's origin and governance.

Based in Delhi, India.

Connect: linkedin.com/in/web3e

THE GHOST IN THE TIMECHAIN | THE INVESTIGATION CONTINUES

news.yesno.fun