Len Sassaman and Satoshi: a Cypherpunk History

evanhatch.eth · Follow

19 min read · Feb 22, 2021

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

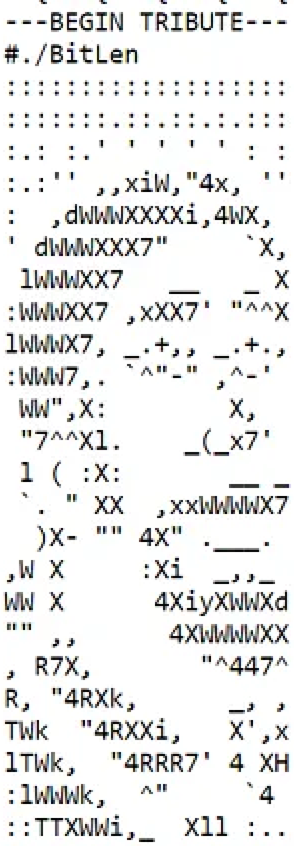
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Try for $5/month



```
---BEGIN TRIBUTE---
#./BitLen
:::::::::::::::::::
:::::::.::.::.:.:::
:.: :.' ' ' ' ' : :
:.:'' ,,xiW,"4x, ''
:  ,dWWWXXXXi,4WX,
' dWWWXXX7"     `X,
 lWWWXX7   __   _ X
:WWWXX7 ,xXX7' "^^X
lWWWX7, _.+,, _.+.,
:WWW7,. `^"-" ,^-'
 WW",X:        X,
 "7^^Xl.    _(_x7'
 l ( :X:       __ _
 `. " XX  ,xxWWWWX7
  )X- "" 4X" .___.
,W X     :Xi  _,,_
WW X      4XiyXWWXd
"" ,,      4XWWWWXX
, R7X,       "^447^
R, "4RXk,      _, ,
TWk  "4RXXi,   X',x
lTWk,  "4RRR7' 4 XH
:lWWk,   ^"     `4
::TTXWWi,_  Xll :..
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

own life at 31, following a long battle with depression and functional neurological disorders.

His death coincided with the disappearance of the world's most famous cypherpunk: Satoshi Nakamoto. **Only 2 months before Len died, Satoshi sent their final communication**:

> *I've moved on to other things and* ***probably won't be around in the future****.*

After 169 code commits and 539 posts in the span of a year, Satoshi disappeared without explanation. They left behind a slew of uncompleted features, raging debates about their vision for Bitcoin, and a still-untouched fortune of $64B in BTC.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Whoever Satoshi was, they were very much ‘standing on the shoulders of giants’ — **Bitcoin was the culmination of decades of accumulated research and discourse within the Cypherpunk community**. In this sense, Len was unequivocally an indirect contributor. Yet one has to wonder who actually wrote the code, ran the first node, and posted using the Satoshi pseudonym.

To synthesize and implement the myriad ideas Bitcoin was based on, that person or group of people would have required a unique combination of expertise spanning public key infrastructure, academic cryptography, P2P network design, practical security architecture, and privacy technology. They would likely have been deeply engrained in the Cypherpunk community and adjacent to the figures who proved to be major influences

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Even in his youth, Len was a self-taught technologist who gravitated towards cryptography and protocol development. Despite living in small-town Pennsylvania, by 18 Len was on the Internet Engineering Task Force

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

headlines for organizing protests against government surveillance, as well as the imprisonment of hacker Dmitri Skylarov.

PGP

Early in his career, Len distinguished himself as an authority in public-key cryptography — the foundation of Bitcoin. By 22, he was presenting at conferences and had founded a public key crypto startup with famous open-source activist Bruce Perens.

After the startup collapsed in the wake of the Dot-com Bubble, **Len joined Network Associates to help develop PGP encryption** central to Bitcoin. Working on the release of PGP7 in 2001, Len set up interop testing for OpenPGP implementations, putting him in touch with many important

Medium

Sign up to discover human stories that deepen your understanding of the world.

Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

At Network Associates, **Len worked on PGP alongside Hal Finney.** Finney was the second PGP developer and helped create the RFC 4880 standard for OpenPGP interoperability. He was also the earliest and most important

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Len and Finney shared one very rare and relevant skillset: they both were developers of the remailer technology that was a precursor to Bitcoin.

Proposed by David Chaum alongside cryptocurrency, remailers are specialized servers for sending information anonymously or pseudonymously. It was very common to use them when contributing to the Cypherpunk Mailing list, which itself was built on distributed remailers.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Not only were remailers a direct technological progenitor of Bitcoin, they were fundamental to its intellectual history. In the essay *Why Remailers*, Finney argued that remailers were the foundation of an anonymous digital economy.

> *Remailers represent the "ground floor" of this house of ideas — the ability to exchange messages privately, without revealing our true identities. In this* ***way we can engage in transactions, show credentials, and make deals,*** *without government or corporate databases tracking our every move.*
>
> *One Cypherpunk vision includes the ability to engage in transactions anonymously, using "digital cash". … this is another area where anonymous mail is important.*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Accordingly, Satoshi’s second post about Bitcoin stated that **pay-to-send email was Bitcoin’s first working use case.**

> *Initially it can be used in proof-of-work applications for services that could almost be free but not quite.*
>
> *It can already be used for pay-to-send e-mail. The send dialog is resizeable and you can enter as long of a message as you like.*

Adam Back

Crossing paths with Len in the small remailer community was Blockstream CEO Adam Back — the first person to communicate with Satoshi.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

> *"[Chaum] stands in the thick of a movement that seems unstoppable — the digitization of money … the wild card in the era of digital money is anonymity, and David Chaum thinks we're in trouble without it"*

While Digicash failed (partially due to a reliance on centralized systems), Chaum wanted to create a second digital currency that would offer a combination of anonymity and practicality.

While many saw its failure as proof that digital cash was infeasible, Satoshi defended the "old Chaumian currencies" while acknowledging the issues caused by centralization.

> *A lot of people automatically dismiss e-currency as a lost cause because of all the*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Pynchon Gate and meta-index + bucket pool architecture

This work was very pertinent to Bitcoin — as work on the Pynchon Gate progressed, **Len became increasingly focused on finding solutions for the Byzantine Fault** (aka Byzantine Generals Problem) that had been a major obstacle for earlier P2P networks.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

During Bitcoin's development in 2008–2010, Len was increasingly active in financial cryptography. He joined The International Financial Cryptography Association and presented at the Financial Cryptography and Data conferences, where he also held a committee seat. The latter was founded by Robert Hettinga, an early and prominent advocate for digital cash, which was a major topic at the conferences.

Satoshi as Academic

Numerous clues suggest that Satoshi was working in academia during Bitcoin's development, an idea embraced by Bitcoin Foundation founder Gavin Andersen.

> *"I think he's an academic, maybe a post-doc, maybe a professor who just doesn't*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

The idiosyncratic construction of Bitcoin's code also suggests that Satoshi had an academic background. It has been described as "brilliant but sloppy", eschewing conventional software development practices like unit testing but exhibiting cutting-edge security architecture and an expert understanding of academic cryptography and economics.

> *Whoever did this had a deep understanding of cryptography … **They've read the academic papers**, they have a keen intelligence, and they're combining the concepts in a genuinely new way.*

When prominent security researcher Dan Kaminsky first reviewed Satoshi's code he tried to pentest it with 9 different exploits, but was amazed to find that Satoshi had already anticipated and patched out all of

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

that Satoshi was based in Europe — the primary focus of an early inquiry by The New Yorker.

Satoshi's writing exhibits spelling and word choices idiosyncratic of British English such as **“bloody difficult”, “flat”, “maths”, grey**”, as well as the dd/mm/yyyy date format. However, Satoshi also refers to Euros rather than pounds.

Bitcoin's Genesis Block also included a headline from that day's copy of *The Times* newspaper *(“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”).* This headline was specific to the print version, which was **only circulated in the UK and Europe**. In 2009, *The Times* was a Top 10 newspaper in Belgium and “heavily used by scholars and researchers

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

and **Len had an unusually early and intimate exposure to all 3**, along with their application to digital currency.

Bram and Len in an interview about CodeCon

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

> *A unit of Mojo represents a slice of the current capabilities of the system as a whole. If you perform work for me now I give you credits, in the future when the network is larger those credits will represent a slice of a much larger pie and so have increased in value when you spend them.*

Satoshi discusses tokenomics in a very similar way:

> *It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.*

While visionary, MojoNation's economy quickly collapsed due to hyperinflation. Satoshi consciously designed Bitcoin to avoid this fate via built-in deflation and non-reliance on a central "mint" server.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Bittorent’s design compared to Napster

Presciently, Len told Bram that “BitTorrent would make him bigger than [Napster founder] Sean Fanning”. **Satoshi would later reference Napster**

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

Digital currency was a prominent subject at the first CodeCon, which included a demonstration involving Adam Back's HashCash as well as Zooko presenting Mnet, a fully open-source and decentralized successor to MojoNation. Mojo wasn't tied to a single company and could be independently audited, both of which Satoshi considered crucial.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

“Zooko’s triangle is a trilemma of three properties that are generally considered desirable for names of participants in a network protocol”

McCoy also is a major influence within cryptocurrency, and Ryan Selkis of Digital Currency Group has stated his belief that McCoy could be Satoshi.

Hacktivism

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

In response to this story, Bram stated that Len had a predilection for anonymous releases

Satoshi alluded to their ideological leanings on a few occasions, saying that said Bitcoin was "very attractive to the libertarian viewpoint" and that it could "win a major battle in the arms race and gain a new territory of freedom for several years".

Len was similarly passionate about the need to defend open knowledge and technological advancement from corporate and governmental

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Despite these challenges, Len continued to work until months before his death, contributing to papers and even presenting at Dartmouth. Sadly, he was successful in concealing the severity of his situation from almost everyone in his life.

> *There were very very few people who had any idea just how far things had gone … the one refrain I heard over and over was "we never knew, it seemed like he was doing fine".*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ **Membership**

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.

When Len's passed away in 2011, it represented a huge loss for the Cypherpunk and the tech community at large, a fact reflected in the huge outpouring of memories and sympathy that followed. One comment in particular still stands out to me: a Hacker News post from "pablos08".

> *I became friends with Len and we were coconspirator cypherpunks at a time when that was a wild frontier. We were reimagining our world, riddled with cryptosystems that would mathematically enforce the freedoms that we treasured. Anonymous remailers to preserve speech without fear of retribution; onion routers to ensure nobody could censor the internet;* ***digital cash to enable a radically free economy. We have schemes to decentralize & distribute everything.***

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Access the best member-only stories.

✓ Support independent authors.

✓ Listen to audio narrations.

✓ Read offline.

✓ Join the Partner Program and earn for your writing.

Cryptocurrency Bitcoin Technology Privacy Fintech

Written by evanhatch.eth

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Access the best member-only stories.
- ✓ Support independent authors.
- ✓ Listen to audio narrations.
- ✓ Read offline.
- ✓ Join the Partner Program and earn for your writing.