Private digital cash is a right. So I am building it.

Cash never asked who you were. It kept no diary of your life, it could not be switched off, and when you handed it over the matter was finished. That kind of money is being taken from us one convenience at a time. What replaces it watches every purchase, answers to whoever controls it, and melts a little in your hand each year. I refuse to accept that as the future. In 2008 Satoshi Nakamoto proved that money does not need a master, and called it electronic cash. MoneroUSD is my attempt to finish that sentence: cash rebuilt for the internet, private and yours the way a banknote in your pocket is yours, with a whole economy around it that nobody can close to you. This page is the reason I am building it.

Cas
Author
One page
Sources online

01 WHY NOW

I only had to read the news.

29 OCTOBER 2026 · BINANCE

$6.3 billion in 20 minutes

The largest theft in crypto's history, from its largest exchange.[1] One company held everyone's keys, and one break was enough.

THE SAME NIGHT

Issuers froze about $2.6 billion of it from their own keyboards.[1] A dollar that can be frozen for a thief can be frozen for anyone.

FEBRUARY 2025 · BYBIT

$1.5 billion, taken through one developer's laptop.[1]

MAY 2025 · COINBASE

Bribed insiders sold the identity files of 69,461 customers.[2] The rules forced that file to exist.

2025 TO 2027 · THE RULES

Developers of privacy tools were sentenced to five and four years.[3] From July 2027 the EU bars privacy coins from every regulated exchange.[4]

2026 · THE ECONOMY

Prices rose 3.7% in a year while real pay fell 0.7%.[5] People are working harder to stand still.

02 THREE RIGHTS

Private digital cash. What you earn and what you buy is nobody's business. Every payment is checked by every node and readable by none: not the amount, the sender or the receiver.

No censor. No account to open, no approval, no freeze switch, no payment pulled back. Nodes speak only over hidden addresses.

The right to a financial system. Saving, paying, borrowing, trading and selling, open to any phone on earth, with nobody deciding who qualifies.

03 MONEY NOBODY PRINTS

Inflation is a decision. Take the decision away.

It is a choice, made in rooms you will never be invited into, by people it does not hurt. Wages and savings pay for it, a few percent at a time.



I want a world where your pay goes up and your prices do not follow it, where saving works again and someone who starts with nothing has a real shot at wealth.

So MoneroUSD has no printer. Every USDm is minted against a larger deposit of Bitcoin or Monero, checked by proof. Beside it sits SAT, named for Satoshi and capped for good at

21,000,000

Take away the power to print and the power to freeze. That is how inflation ends: by giving people the exit.

04 THE DESIGN

I set these rules before the first line, and never traded one for another.

1. **Private by construction.** Nothing to look at: no amounts, no names, no links, no counts.
2. **Post-quantum from the first byte.** `ML-KEM` `ML-DSA` `Poseidon2` `WHIR`.
3. **Proof, never trust.** Sealed notes, one-time spend markers, zero-knowledge proofs.
4. **Small enough for a phone.** Parallel blocks fold into one recursive proof, so the node never grows.
5. **Nobody to ask, and it never stops.** No company or server to depend on.

05 FIVE CONVICTIONS

1. **Privacy and protection belong together.**
   Private, final payments, with an escrow that no company judges.
2. **Crypto does not need permission to be safe.**
   Safety is built, never granted. Every rule that begins as protection ends as reach.
3. **AI can build this.**
   I am building MoneroUSD with AI, and I will not hide it. Nothing here is taken on faith.
4. **And AI will not break it.**
   ~~1 + 1 = 3~~ REFUSED
   No model can make a false proof check. There is nobody to phish, bribe or fool.
5. **Digital cash can replace the card networks.**
   A tenth of a cent, final the moment it lands, from a tap of a phone.

06 BUILT THIS FAR

- The chain and the wallet
- USDm and the Bitcoin and Monero bridge
- Tap to pay and checkout for business
- Ion Swap and Dark Solidity contracts
- Letter, private messages with money inside
- Veil and Sovereign, being built now

It is not finished. It is far enough along that I know it can be.

07 WHO IT IS FOR

The worker whose raise vanished. The shop paying three percent to sell. The person a bank did not want. The saver. Anyone whose life is their own.

Regulated away, or real.

Crypto began as cash for the internet. Then most of it took a deal: hold your customers' keys, collect their passports, add a freeze button, and you may stay in business. This industry has to decide what it is. I choose real. I want a world where pay rises and prices do not, where nobody can be locked out of money, and where the most powerful technology we have ever made protects people instead of watching them. I believe that world can be built, so I am building it.



— Cas
MoneroUSD · November 2026

Sources 1 TRM Labs and Wikipedia, "2026 Binance hack"; BleepingComputer (Bybit, Feb 2025). 2 Coinbase's filing with the Maine Attorney General; Help Net Security, 15 May 2025. 3 Blockworks (Tornado Cash verdict, Aug 2025); The Block (Samourai Wallet sentences, Nov 2025). 4 Regulation (EU) 2024/1624, Article 79. 5 Trading Economics; US Bureau of Labor Statistics (CPI, real earnings, year to Sept 2026). Links to every source, and the full paper, are at **monerousd.org/whitepaper**. MoneroUSD is in development and does not hold real funds yet. This page is its author's vision, not financial or legal advice. Not affiliated with the Monero Project.