



October 31, 2026 · Lexington, South Carolina · For immediate release

The Theft That Took Twenty Minutes

On one night in October 2026, about \$6.3 billion in digital money left the world's biggest crypto exchange in about twenty minutes. Two research firms blame a North Korean hacking crew. No government has said that yet. This release sorts out what is known, who counted what, and why the difference matters to regular people.

This release is our account of the Binance theft of October 29, 2026, and of the public record behind it. It is built from Binance's own statements, statements by the FBI and its partner agencies, a joint statement by the United States, Japan, and South Korea, the final report of a United Nations panel, a United States Treasury sanctions action of October 28, 2026, and the published counts of two research firms, TRM Labs and Chainalysis. It does not claim that any government has blamed North Korea for the Binance theft, because none has. Where the two firms' counts differ, this release prints both, with the firm's name and its years attached.

What happened on the night of October 29

Cryptocurrency is digital money. It does not sit in a vault. It exists as lines in a record book, and that record book is called a blockchain. Thousands of computers keep copies of the same book and check each other, so nobody can quietly rewrite a line.

A wallet is the account that holds the money. An exchange is a company where people buy, sell, and keep cryptocurrency, part bank and part stock market in one place. Binance is the biggest exchange in the world.

On the evening of October 29, 2026, about \$6.3 billion in cryptocurrency left Binance wallets in about twenty minutes. That \$6.3 billion figure is Binance's own. A research

firm named TRM Labs measured the flow more closely and put it at about \$6.36 billion, moving across ten blockchains at once.

Here is what Binance has said. Its first look pointed to a laptop that belonged to one of its engineers and had been broken into. Its later checks found more points of break in. It found no sign that the wallet keys had leaked. A wallet key is the secret code that lets money move out of a wallet. Binance stopped money moving in or out for a time. It told customers their money was safe. It set aside more than \$6.34 billion of its own money to cover the loss.

How the thieves got in, in plain words

Two research firms have studied the theft in public, TRM Labs and Chainalysis. This part rests on TRM Labs' published account. Binance itself has not yet said exactly how the break in worked.

One of the chains hit is called Ethereum. Ethereum has a newer feature that lets a wallet hand control of itself to a helper program. That feature is called wallet delegation. It is meant to make wallets easier to use.

TRM Labs says the thieves got fifty permissions signed ahead of time. Each signed permission was set to fire at a different moment. When the right moment came, one of them fired. The delegation turned a big Binance wallet into a machine that swept money to the thieves. The sweeping kept going for hours, and it caught new deposits as they landed. On the nine other chains, the money moved out through ordinary signed transfers in the same short window.

The lesson is plain. A feature built to make wallets handy became the tool that emptied one.

Who is blamed, and who has not blamed anyone

TRM Labs and Chainalysis both say the theft bears the marks of TraderTraitor. TraderTraitor is the name the FBI uses for a North Korean hacking crew. Both firms say they hold that view with high confidence. Both firms study blockchain records for a living, and their work is respected. It is still their call, not a government's.

No government has blamed anyone for the Binance theft. Binance has named no one. Asked about it on October 31, the President said the United States did not know yet and was looking into it.

We will update this release if and when a government puts its name to the Binance theft. We will also update it when the money's next move is a matter of public record.

Why did the firms reach for that name so fast? Chainalysis says it watched money stolen from Binance end up in the same wallets as money stolen in September 2026 from another exchange, Bitget. The firms had already blamed North Korean actors for the Bitget theft. Money from two thefts landing in the same wallets is the kind of sign the firms work from.

The race to freeze the money

A stablecoin is a kind of cryptocurrency built to hold a steady value. One coin is meant to be worth one dollar. A company issues each stablecoin, and that company can freeze its coins. To freeze a coin means to lock it where it sits, so it cannot move and cannot be spent.

About half the stolen money sat in stablecoins. That gave the good guys a lever, and the race was on. TRM Labs counted the freezes on the public record. Four stablecoin issuers, Tether, Circle, Ripple, and World Liberty Financial, froze about \$2.67 billion. A safety council on one chain forced about \$30 million more out of a thief's wallet. The frozen total comes to about \$2.7 billion. Binance has used a rounder figure, about \$3 billion.

The thieves raced back. They sold stablecoins at a loss of more than ten percent to big trading firms that buy and sell all day. They borrowed Ether against their stablecoins on a lending service called Aave, where people borrow cryptocurrency by putting up other cryptocurrency as security. Ether is the money of the Ethereum chain. Both moves traded value for speed, to escape into forms nobody can freeze.

What the thieves still hold is more than 420,000 Ether and 18,270 Bitcoin, worth about \$2.4 billion. Bitcoin is the oldest and best known cryptocurrency. No company issues Ether or Bitcoin, so no company can freeze them. That does not make the money gone for good. Stolen money still has to be laundered before it can be spent. Laundering means moving money around to hide where it came from. Washing money is slow, and it is where thieves in past cases have been caught.

What governments have put their names to

Governments have blamed North Korea for a string of earlier thefts. That record is solid, and it is worth reading with the years attached.

In February 2025, the FBI said North Korea stole about \$1.5 billion from an exchange called Bybit. The FBI said it calls that crew's work TraderTraitor.

In December 2024, the FBI, a Defense Department crime center, and Japan's national police together blamed the same crew for the \$308 million theft from DMM Bitcoin, a Japanese exchange, in May 2024.

In January 2025, the United States, Japan, and South Korea issued a joint statement. It blamed North Korea for the \$235 million theft from the WazirX exchange in July 2024, and for other thefts that year.

In April 2022, the FBI said North Korean actors it names as Lazarus Group and APT38 stole \$620 million from the Ronin network, a system tied to an online game.

In March 2024, a United Nations panel published its final report. The panel counted 58 suspected North Korean attacks on cryptocurrency companies from 2017 through 2023, worth about \$3 billion. The panel's own word was suspected, and we keep it attached.

One thing this list does not include is Binance. No government has added it yet.

Two firms, two different totals

News stories often print one big number for all North Korean crypto theft. The record does not hold one number. It holds two careful counts that do not agree, and the gap between them is part of the story.

Chainalysis counts about \$1.7 billion stolen in 2022. Its first count for 2023 was about \$1 billion, and it later cut that count to about \$660.5 million. The lower number is the honest one, and the old one still floats around. Chainalysis counts \$1.34 billion in 2024 and \$2.02 billion in 2025. Its total through the end of 2025 is \$6.75 billion. For 2026 so far, Chainalysis says suspected North Korean thefts make up 89 percent of all reported hack losses. It puts the suspected total since 2021 at \$13.24 billion.

TRM Labs counts wider. It puts the total since 2017 at \$12.8 billion, across about 100 thefts. It puts 2026 alone at \$7.4 billion, with the Binance theft the biggest piece of that year.

Put the two side by side. TRM Labs starts in 2017 and reaches \$12.8 billion. Chainalysis starts in 2021, four years later, and reaches \$13.24 billion. A shorter set of years with a bigger total means the two firms are not counting the same set of thefts. Both firms do serious work. They simply draw the lines in different places.

So here is our rule, and it is the same rule as our first release. A total with no name and no years attached is not a number worth repeating. One more figure makes the point. Stories this week have used about \$13.5 billion. That figure comes from one researcher quoted by a news agency. It is not a published count by either firm, and we do not use it.

One comparison is safe to make. One night at Binance roughly equals everything Chainalysis counted through the end of 2025.

The second engine, workers who are not who they say

North Korea also earns money the quiet way. Its state run computer workers take remote jobs under false names. They do the work, and the wages go home.

Sanctions are government penalties. They cut named people and groups off from the money system, so banks and companies must not do business with them. On October 28, 2026, one day before the Binance theft, the United States Treasury put sanctions on ten people and one organization. It accused them of moving money for the worker networks. Two of the men are accused of turning millions of dollars in cryptocurrency into clean money for those networks.

The FBI has said the money from the workers and the money from the hackers both fund North Korea's nuclear and military programs. A United Nations panel estimated the worker scheme brings in \$250 million to \$600 million a year.

The same UN report carries two bigger estimates. Some governments told the panel they estimate that cyber theft brings in about half of North Korea's foreign currency income. Others estimated that illegal cyber work funds about 40 percent of its weapons programs. Those are estimates given to the panel by governments. They are not measurements the panel made, and we print them only with that label on.

What this means for regular people

Most people who lose money in this story never bought any cryptocurrency. Here is how a theft like this still reaches them.

If you keep money at an exchange, the exchange's safety is your safety. Binance set aside its own money to cover its customers this time. A smaller company hit this hard might not be able to do that. Money in a bank account is protected by law up to set limits. Money at a crypto exchange does not carry the same promise.

Frozen money can come back. That is why the freeze race matters to people waiting on money. Money that gets frozen can be returned to its owners. Money that escapes has to be caught while it is being washed, and that can take years.

The cost does not vanish. When billions are stolen, the bill lands in the fees customers pay, in the price of the money itself, and in the police, court, and sanctions work that follows. Taxpayers fund that work.

The door the thieves used is also aimed at regular workplaces. The public record on the earlier thefts shows fake job recruiters, fake coding tests for job seekers, and workers hiding who they really are. Those tricks target ordinary people at ordinary companies, far from the world of crypto.

Two habits help. Be slow with any recruiter who sends you a test or a program to run. And on any account that holds money for you, turn on every safety step the service offers.

SOURCES

Binance, public statements on the October 29, 2026 incident. TRM Labs, incident report and cumulative theft count, October 30, 2026. Chainalysis, 2026 Crypto Crime Report excerpts, December 18, 2025, and figures published October 30, 2026. FBI, Public Service Announcement I-022625-PSA, February 26, 2025. FBI, statement on the Ronin theft, April 14, 2022. FBI, Department of Defense Cyber Crime Center, and Japan National Police Agency, joint statement, December 23, 2024. United States, Japan, and Republic of Korea, joint statement, January 14, 2025. United Nations Panel of Experts on North Korea sanctions, final report, March 2024. United States Treasury, sanctions designations, October 28, 2026.

Contact. Agentic Armor LLC · contact@agenticarmorllc.com · agenticarmorllc.com

The canonical text of this release lives at <https://agenticarmorllc.com/releases/binance-theft-2026/> and the release library stands at agenticarmorllc.com/releases/.