The GoldBS Collapse

How a WebView wrapper and four TRON wallets took 1.53 million USDT from 4,273 people in six days

---

Between 14 and 20 June 2026, a single cryptocurrency wallet on the TRON network received 1,526,142 USDT from 4,273 separate addresses. The money arrived from people across Afghanistan and Pakistan who believed they were funding accounts on a trading platform called GoldBS. No trading ever took place. Deposits were forwarded out of each account within minutes of arrival, and the balances users saw on their screens were figures served from a web page, not holdings in custody.

This report sets out the documentary, blockchain and software evidence in the order it was obtained. Every claim is sourced to a public record, a public ledger entry, or a file whose cryptographic hash is published here so that any reader can independently verify it. Where the evidence does not support a conclusion, that is stated explicitly.

SUMMARY OF FINDINGS — ONE COLLECTION WALLET

Gross collected	1,526,142 USDT (approx. 427,000,000 PKR)
Recycled as payouts	696,141 USDT
Net extracted	830,001 USDT (approx. 232,000,000 PKR)
Unique victim addresses	4,273
Median deposit	242.87 USDT
Collection window	14 - 20 June 2026 (6 days)
Regulator status	BCSC caution list; IOSCO I-SCAN 51040

PKR conversions calculated at 280 PKR/USD, August 2026. These figures cover a single wallet over a single six-day window and are a floor, not a total.

1. What the platform claimed to be

GoldBS presented itself as a cryptocurrency and commodities trading exchange, reachable at goldbs.com and later at a succession of replacement domains. Users deposited USDT, were shown a portfolio dashboard with live valuations and daily earnings, and were encouraged through referral incentives to recruit others. Recruitment was conducted largely through WhatsApp and Telegram groups.

The platform gained particular traction in Afghanistan. TOLOnews reported in June 2026 that thousands of investors had lost access to their funds and that millions of dollars were feared lost. One man interviewed had borrowed 500 US dollars to invest and reported losses exceeding 1,100 dollars once his account was blocked.

Da Afghanistan Bank responded by urging citizens to verify the legality of financial companies before investing. Its spokesperson, Haseebullah Noori, stated that online forex trading is prohibited in Afghanistan and that the central bank has issued no licence to any individual or organisation for such activity.

2. Regulatory warnings on record

The British Columbia Securities Commission added GoldBS Group Limited, also trading as GoldBS Exchange, to its Investment Caution List on 24 March 2026. The stated ground was that it is an unregistered and unlicensed entity offering financial products or services.

That warning was republished internationally on 1 April 2026 through IOSCO's International Securities and Commodities Alerts Network under Warning ID 51040. IOSCO is the global association of securities regulators; entries in I-SCAN are visible to every member authority.

IOSCO I-SCAN 51040	`https://www.iosco.org/i-scan/?id=51040`
BCSC caution list	`https://www.bcsc.bc.ca/enforcement/early-intervention/investment-caution-list/2026/goldbs-group-limited`
Published at NCA	`24 March 2026`
Published at IOSCO	`1 April 2026`
Category	`Unregistered / unlicensed entity offering financial products or services`

3. The UK corporate registrations

Two companies were registered at Companies House whose names correspond to the two applications used in the scheme. Both were incorporated on consecutive days in October 2024 and both were dissolved on the same day in October 2025.

3.1 GOLDBS LIMITED — company number 16011121

Field	Record
Incorporated	10 October 2024
Nature of business (SIC)	82990 — Other business support service activities n.e.c.
Statement of capital	GBP 10,000
Registered office changed	23 June 2025, to Companies House default address, Cardiff
First Gazette (strike-off)	5 August 2025
Dissolved	28 October 2025, by compulsory strike-off
Accounts filed	None
Confirmation statements filed	None

3.2 THOMAS GROUP SERVICE LIMITED — company number 16007931

Field	Record
Incorporated	9 October 2024
Nature of business (SIC)	82990 — identical to the above
Registered office	Companies House default address, Cardiff
Dissolved	28 October 2025, by compulsory strike-off
Accounts filed	None
Confirmation statements filed	None

The replacement of a registered office with the Companies House default address is not a voluntary act. Companies House imposes it when it determines that a company is not entitled to use the address on record, which commonly follows a complaint by the genuine occupant or a finding that the address is fictitious.

3.3 The registered director

Companies House lists a single director for both companies: Mark Brown, nationality American, country of residence United States, date of birth recorded as January 1985. He was appointed to THOMAS GROUP SERVICE LIMITED on 9 October 2024 and to GOLDBS LIMITED on 10 October 2024. These are his only two directorships on the UK register. Both appointments give the same correspondence address: 2081 Lincoln St, Denver, United States, 80202.

Officer record	`https://find-and-update.company-information.service.gov.uk/officers/wrWfCviQda39qrGNZIB3he8JmCI/appointments`
GOLDBS LIMITED	`https://find-and-update.company-information.service.gov.uk/company/16011121`
Filing history	`https://find-and-update.company-information.service.gov.uk/company/16011121/filing-history`

THOMAS GROUP	`https://find-and-update.company-information.service.gov.uk/company/16007931`

3.4 What the register does and does not establish

Companies House does not verify the identity of the people named in company filings. A name, a month and year of birth, a nationality and a correspondence address are accepted as submitted. Every page of the register carries a standing notice stating that Companies House does not check the accuracy of the information filed.

Mandatory identity verification for directors was introduced under the Economic Crime and Corporate Transparency Act 2023 and took effect on 18 November 2025. Voluntary verification opened on 8 April 2025. Both companies were incorporated in October 2024, thirteen months before verification became mandatory, and both were dissolved on 28 October 2025, three weeks before it commenced. Neither ever filed a confirmation statement, which is the event that would have triggered verification for an existing director. No passport, photographic identification or biometric check was performed on these registrations at any point.

Accordingly, the register establishes that the name Mark Brown, an American nationality, a January 1985 birth month and a Denver correspondence address were submitted to Companies House on two filings made on consecutive days. It does not establish that a verified individual of that name exists, nor that such a person operated the applications described in this report. Fraudulent use of stolen and invented identities to register UK companies is a documented and large-scale problem, and it was the principal reason the 2023 Act was passed. Establishing who actually controlled these registrations requires access to the formation agent's anti-money-laundering file, banking records and hosting records — material available only to law enforcement and regulators.

3.5 The timeline problem

Both companies ceased to exist on 28 October 2025. The BCSC warning was issued in March 2026. The deposits documented in this report were collected in June 2026. Investors were funding accounts on a platform whose corporate registrations had been dissolved some eight months earlier. A dissolved company cannot lawfully trade, hold client money or enter contracts. The registrations remained visible on a government website throughout, and that visibility appears to have been their entire function.

4. Domain rotation and app distribution

The operation changed its domain name every few weeks. Each rotation defeats the warnings issued against the previous one: the BCSC listed goldbs.com specifically, so a user searching the current domain finds no regulator alert. It also resets any takedown, blocklisting or payment-processor action already taken.

Two domains are documented here by direct evidence. Both now fail to resolve at DNS level, returning ERR_NAME_NOT_RESOLVED — the records were removed entirely rather than the servers merely going offline.

goldwkx.com/h5/ios	`GoldBS build — DNS records removed`
chzbitga.com/h5/ios	`CHZBIT build — DNS records removed`
goldbs.com	`Original domain named in the BCSC listing`

The applications were distributed as direct APK downloads from the operators' own websites, outside Google Play and outside the Apple App Store. This bypasses store review, developer identity checks and financial-application scrutiny, and it means no store takedown mechanism exists. The identical URL path /h5/ios on both domains is a template artefact: h5 is the conventional route for HTML5 mobile wrappers in off-the-shelf platform kits.

5. Technical analysis of the applications

Both APK files were obtained and examined statically. Neither was executed. The files analysed are identified by hash below so that any investigator can confirm they hold the same artefacts.

chzbitga.apk SHA-256	`59caa94c2b795686c4a9301a1d92aed1fcd8885a c6360a99d81940c1af2c53bb`
chzbitga.apk MD5	`2feffe2431e5dc02b9086bd771ef8bd0`
chzbitga.apk size	`16,450,342 bytes`
goldwkx.apk SHA-256	`974a2d4988331091d0f0ba76b381afd2bdd825e2 39fd2e98a9ad66676d6c3048`
goldwkx.apk MD5	`c29711a0f0aef7be6d57bba6bee4a13c`
goldwkx.apk size	`16,589,597 bytes`

5.1 The two applications share one signing key

Android applications are cryptographically signed by their developer. Both files carry an identical signing certificate, matching to the second of creation.

SHA-256 fingerprint	`4E:D8:CE:A8:E2:8B:BE:27:9D:89:18:22:B5:D2:C6:DA: 19:79:6A:C3:A2:3B:5C:03:B8:8C:DE:EC:67:E6:0A:22`
Certificate subject	`CN=Android Debug, O=Android, C=US`
Key created	`7 July 2025, 10:09:48 GMT`
Serial number	`1`

A signing key cannot be forged or coincidentally matched. Only the holder of the corresponding private key could have produced both files. GoldBS and CHZBIT are therefore the same operation, established cryptographically rather than by inference. When users were told that the GoldBS platform had failed and that they should migrate to CHZBIT and fund the new account with a percentage of their old balance in order to release it, they were being directed by the same party that had built the first application.

The certificate is Android Studio's automatically generated development key. Google Play rejects debug-signed applications outright. Financial software handling customer deposits is never released under a debug certificate. Its presence indicates software that was never intended to pass any review process, and it is the technical reason the applications had to be distributed as direct downloads.

5.2 Neither application is a trading platform

Both are Flutter applications built on the flutter_inappwebview package, whose sole function is to display one remote web page. The main activity in both is com.web.build_web_app.MainActivity, a generic class name from a website-to-APK template. There is no trading engine, no order matching, no price feed, no wallet implementation and no custody code anywhere in either file. Each contains exactly one hardcoded endpoint.

Every balance, chart and earnings figure a user saw was rendered by a remote server and displayed in a browser frame. Changing one value on that server changes what every user sees. Removing the server removes every account, which is precisely what occurred.

5.3 Build metadata records the rotation strategy

Application	Package identifier	Build timestamp
goldwkx.apk (GoldBS)	com.rtbnqg.v20260510222332	10 May 2026, 22:23:32
chzbitga.apk (CHZBIT)	com.pmgyyx.v20260525131107	25 May 2026, 13:11:07

The package identifiers consist of a random six-letter prefix followed by an embedded build timestamp. This is automated generation: each rebuild produces a fresh identifier so that the previous one can be abandoned without consequence. The naming scheme is the rotation strategy, built into the release pipeline.

The dates carry a further implication. The CHZBIT successor was compiled on 25 May 2026, fifteen days after the GoldBS build and roughly three weeks before the deposits documented here were collected. The replacement platform existed before the first one failed. The migration was planned, not improvised.

5.4 Byte-level comparison

Of approximately two thousand files inside each package, only sixteen differ: the manifest, the signature files, the compiled code blob, the resource table and five image assets. Every other file is byte-identical. The two applications are one product with a substituted URL and a substituted logo.

5.5 Requested permissions

Both applications request camera, microphone (RECORD_AUDIO), fine location, background location and full external storage access. A web wrapper displaying a trading page requires none of these. Background location access in an application with no mapping or location-dependent feature is difficult to account for by any legitimate purpose.

6. The money trail

All figures in this section are drawn from the public TRON ledger and can be reproduced by any reader at tronscan.org. The token throughout is genuine Tether USDT on TRON, contract TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t. Users sent real assets; what they received back was a number rendered in an application.

6.1 A single deposit, traced end to end

The following is one documented deposit, used here to establish the mechanism. The depositor sent 159.38 USDT from a Binance account to the address the platform had issued to him.

Time (UTC)	Event	Amount
2026-06-14 08:19:03	Binance hot wallet → deposit address	+159.38 USDT
2026-06-14 08:20:51	Deposit address → collection wallet	−159.38 USDT

One minute and forty-eight seconds. The amount forwarded matches the amount received exactly, with network fees paid by a third wallet that had delegated energy to the address. The deposit address itself was activated minutes before the transfer arrived and has recorded no activity since. It was generated for one depositor, used once, and abandoned.

The funds were never held. No trading occurred, because the money was gone before any trade could have been placed.

Deposit address	`TA7B8M7WrzDbFSVCkcrQq2fDxhFW68dGtG`
Inbound TXID	`e92398b450202ce932d05b2494d33ed1cea2380c d3a4df71818c662426f16f77`
Outbound TXID	`5edc60f490807e23d5ed9e9b229ef5ecc00a66bf 95599d402f37908ec1f4a502`
Binance hot wallet	`TJ5usJLLwjwn7Pw3TPbdzreG7dvgKzfQ5y`

6.2 Layer one — the collection wallet

`TQgMdDtSqsVF8aewPG5MgYBGmdKVB8vDt2`

Measure	Value
Unique depositing addresses	4,273
Total deposits recorded	4,290
Gross USDT received	1,526,142.00
Smallest deposit	3.48 USDT
Median deposit	242.87 USDT
Largest deposit	9,836.00 USDT
Active period	14 – 20 June 2026
Retained balance	Nil — every unit forwarded onward

The median deposit of roughly 243 USDT identifies who was targeted. These were not substantial investors. They were people committing two or three hundred dollars, consistent with the Afghan man who told TOLOnews he had borrowed 500 dollars. There were more than four thousand of them in six days.

6.3 Layer two — aggregation and the payout engine

`TAHAhrTeUG6tjkWatAkgNR6zQ9YpmAgS7u`

This wallet received the entire 1,526,142 USDT from the collection wallet, together with 406,141 USDD from a separate source. It has two inbound counterparties and 4,194 outbound counterparties. Its outflow divides into two distinct functions.

Function	Destination	Amount	Txns
Ponzi payouts	4,192 separate wallets, median 104 USDT each	696,141 USDT	—
Extraction	`TDVLm9ivCsX6Br4iL84rU9Ekn4RDSZstoq`	830,000	26
Extraction	`TBXW4hS5KYjjbJXDpnrPf4zhkLwrpUjbyz`	406,141 USDD	20

The payout branch is the Ponzi mechanism, visible directly in the ledger. Approximately 46 per cent of victim deposits were returned to participants in small amounts — the withdrawals and earnings that sustained belief in the platform and drove further recruitment. They were funded entirely from incoming deposits. No trading revenue exists anywhere in this data because no trading occurred.

6.4 Layer three — conversion out of a freezable asset

`TDVLm9ivCsX6Br4iL84rU9Ekn4RDSZstoq`

This wallet received 841,292 USDT and 550,000 USDD and forwarded the entirety of both. Its significant function is the conversion of USDT into USDD.

That conversion is consequential. USDT is issued by Tether, which maintains the ability to freeze wallet balances at the request of law enforcement and has exercised it on many occasions. USDD is decentralised and possesses no equivalent freeze mechanism. Converting victim funds from USDT into USDD before extraction removes the single technical measure by which they could have been recovered. This is not a routing accident. It reflects specific knowledge of which digital assets can be seized and which cannot.

6.5 Where the trace ends

Beyond this point the funds enter wallets carrying hundreds of millions of dollars across thousands of counterparties — exchange hot wallets, payment processors and, in one case, the USDD issuer contract performing token redemption. These are shared financial infrastructure serving large numbers of unrelated legitimate users. They are recorded here as trace endpoints for subpoena, and are expressly not characterised as participants in the fraud.

This is where every public on-chain investigation ends. The services operating that infrastructure hold know-your-customer records on the accounts that moved these funds. Those records are the identification point, and they are obtainable by law enforcement on legal process. They are the reason this report should reach investigators rather than remain a public document alone.

7. The second extraction: the migration demand

When the first platform stopped functioning, users were contacted through the companion application and instructed to register on a new one. The stated condition for releasing a frozen balance was that the user fund the new account with twenty per cent of the balance held on the old. The balances were never transferred and the promised withdrawals never occurred.

This is advance-fee fraud in its recovery phase, and the technical evidence shows it was designed in advance: the successor application was compiled on 25 May 2026, before the migration was announced and before the deposits documented here were taken, and it was signed with the same private key as the original.

There was never a balance to release. The figures displayed were server-side values in a web page. The twenty per cent was not a fee against a holding; it was a second deposit into the same funnel.

8. Complete address reference

Role	TRON address
Documented victim deposit address	`TA7B8M7WrzDbFSVCkcrQq2fDxhFW68dGtG`
Layer 1 — collection	`TQgMdDtSqsVF8aewPG5MgYBGmdKVB8vDt2`
Layer 2 — aggregation and payouts	`TAHAhrTeUG6tjkWatAkgNR6zQ9YpmAgS7u`
Layer 3 — USDT to USDD conversion	`TDVLm9ivCsX6Br4iL84rU9Ekn4RDSZstoq`
Layer 3 — USDD receiving	`TBXW4hS5KYjjbJXDpnrPf4zhkLwrpUjbyz`
Secondary inflow source (unclassified)	`TSUYvQ5tdd3DijCD1uGunGLpftHuSZ12sQ`
USDT token contract (Tether, legitimate)	`TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t`
Binance hot wallet (legitimate)	`TJ5usJLLwjwn7Pw3TPbdzreG7dvgKzfQ5y`

Any address may be inspected at tronscan.org/address/<address>/transfers. The final two entries are identified as legitimate infrastructure and are listed for completeness of the trace only.

9. Indicators for identifying platforms of this type

- Software distributed as a direct download from the operator's own website rather than through an application store.
- A domain name that changes every few weeks or months.
- Displayed balances that cannot be withdrawn, accompanied by a demand for a fee, tax, upgrade or percentage deposit before release.
- An instruction to migrate to a replacement platform and fund it in order to unlock an existing balance.
- Referral and recruitment incentives forming a significant part of the offering.
- Returns that are consistent, guaranteed or unusually rapid.
- No verifiable licence from any financial regulator in the jurisdictions served.
- Corporate registration in a country where the company does no business, used as a credential.

10. Guidance for those affected

10.1 Preserve evidence immediately

Capture the account dashboard, deposit history and transaction records with the system clock visible. Attempt a withdrawal and record the refusal or fee demand; that refusal is the single most useful document available. Archive the websites and download pages to archive.org before the domains lapse. Preserve all WhatsApp and Telegram correspondence with recruiters, including telephone numbers and display names. Export transaction records from any exchange used to send funds.

10.2 Send no further money

Demands for a withdrawal tax, release fee, unlock charge, verification deposit or account upgrade are not obstacles between a user and their funds. They are the next stage of the same theft. This applies equally to any third party who makes contact offering to recover lost funds. Recovery fraud targets people who have recently been defrauded, and search results for platforms of this kind are routinely dominated by such services presenting themselves as review sites. No legitimate firm guarantees the return of stolen funds or requires payment in advance.

10.3 Report

Jurisdiction	Authority and channel
Pakistan	National Cyber Crime Investigation Agency (NCCIA). Helpline 1799; office 051-9106691; online complaint portal or a regional office. NCCIA replaced the FIA Cyber Crime Wing in April 2025 and now holds exclusive jurisdiction under PECA.
Afghanistan	Da Afghanistan Bank; Attorney General's Office.
United Kingdom	Action Fraud — actionfraud.police.uk or 0300 123 2040. Separately, report the company registrations to Companies House at enquiries@companieshouse.gov.uk, and see gov.uk/complain-company.
United States	Internet Crime Complaint Center (IC3) — ic3.gov. Relevant given the American nationality and Denver address on the UK filings.
Canada	British Columbia Securities Commission — bcsc.bc.ca. An open file already exists on this entity.
Exchange	If funds were sent from an exchange account, submit a fraud report to that exchange's compliance team with the transaction hashes. Exchanges can freeze assets, but the window is short.

Include the transaction hashes, the wallet addresses in section 8, and the file hashes in section 5 with every report. Volume of complaints drives enforcement action; a single report is easily set aside, four thousand are not.

11. Scope and limitations

The figures in this report describe one collection wallet during one six-day period. They are not the total loss attributable to this operation. Earlier and later domains, the companion application, and parallel wallets serving other victim cohorts are outside the data examined here. The true total is higher, in all likelihood substantially so. The figure of 1,526,142 USDT is what can be proven today from a public ledger.

This report does not assert that any named individual committed a criminal offence. It records what public registers, a public ledger and two software artefacts contain. The attribution of conduct to particular persons requires investigative powers that private parties do not hold, and it is properly the function of the authorities listed in section 10.3.

Wallets identified in section 6.5 as exchange, payment-processor or protocol infrastructure are not alleged to have participated in or had knowledge of the fraud. They appear in the trace because victim funds passed through shared financial systems, as such funds ordinarily do.

12. Sources

TOLOnews, 'Gold BS Faces Fraud Allegations as Afghan Investors Report Heavy Losses'

`https://tolonews.com/afghanistan-199535`

IOSCO I-SCAN, Warning ID 51040

`https://www.iosco.org/i-scan/?id=51040`

British Columbia Securities Commission, Investment Caution List, 24 March 2026

`https://www.bcsc.bc.ca/enforcement/early-intervention/investment-caution-list/2026/goldbs-group-limited`

Companies House, GOLDBS LIMITED (16011121)

`https://find-and-update.company-information.service.gov.uk/company/16011121`

Companies House, GOLDBS LIMITED filing history

`https://find-and-update.company-information.service.gov.uk/company/16011121/filing-history`

Companies House, THOMAS GROUP SERVICE LIMITED (16007931)

`https://find-and-update.company-information.service.gov.uk/company/16007931`

Companies House, officer appointments record

`https://find-and-update.company-information.service.gov.uk/officers/wrWfCviQda39qrGNZIB3he8JmCI/appointments`

TRONSCAN blockchain explorer (all wallet data in section 6)

`https://tronscan.org`

Primary evidence held by the author and available to investigators on request: five TRONSCAN transfer exports in CSV format covering the wallets in section 8; both APK files, hashes as published in section 5; application screenshots showing account balances, the withdrawal record and the dead domains; and exchange withdrawal records.

Contact

This report was compiled by an affected user. If you have lost funds to GoldBS, CHZBIT or a platform operating under a related domain, you are welcome to make contact — to compare records, to add your case to a joint complaint, or to be pointed toward the appropriate reporting channel in your country. A coordinated group filing carries considerably more weight with investigators than isolated reports.

Name	`Jahanzaib`
WhatsApp	`+92 304 8086046`

Please note: no fee is charged, and no recovery service is offered or endorsed. Anyone approaching you and requesting payment in exchange for recovering your funds should be treated as a further attempt at fraud.

Compiled August 2026. All blockchain data is verifiable at tronscan.org and all corporate data at Companies House. This document is provided for public awareness and for submission to law enforcement and financial regulators. It does not constitute legal or financial advice.