Federal Improper Payment & Fraud Crisis: The Estimated $5 Trillion Problem *Why Blockchain is Essential for Disaster Relief Payments*

TSIT TREASURY SOLUTIONS IT

FEDERAL IMPROPER PAYMENTS: SCOPE AND TRENDS

Improper payments are those that should not have been made or that were made in an incorrect amount

Fiscal Year 2024 Estimate: $162 billion in improper payments across 68 programs (16 agencies)

- $135 billion (84%) due to overpayments
- $7.9 billion underpayments
- $12.6 billion unknown (uncertain if error or not)
- $5.9 billion technically improper (but legally authorized)

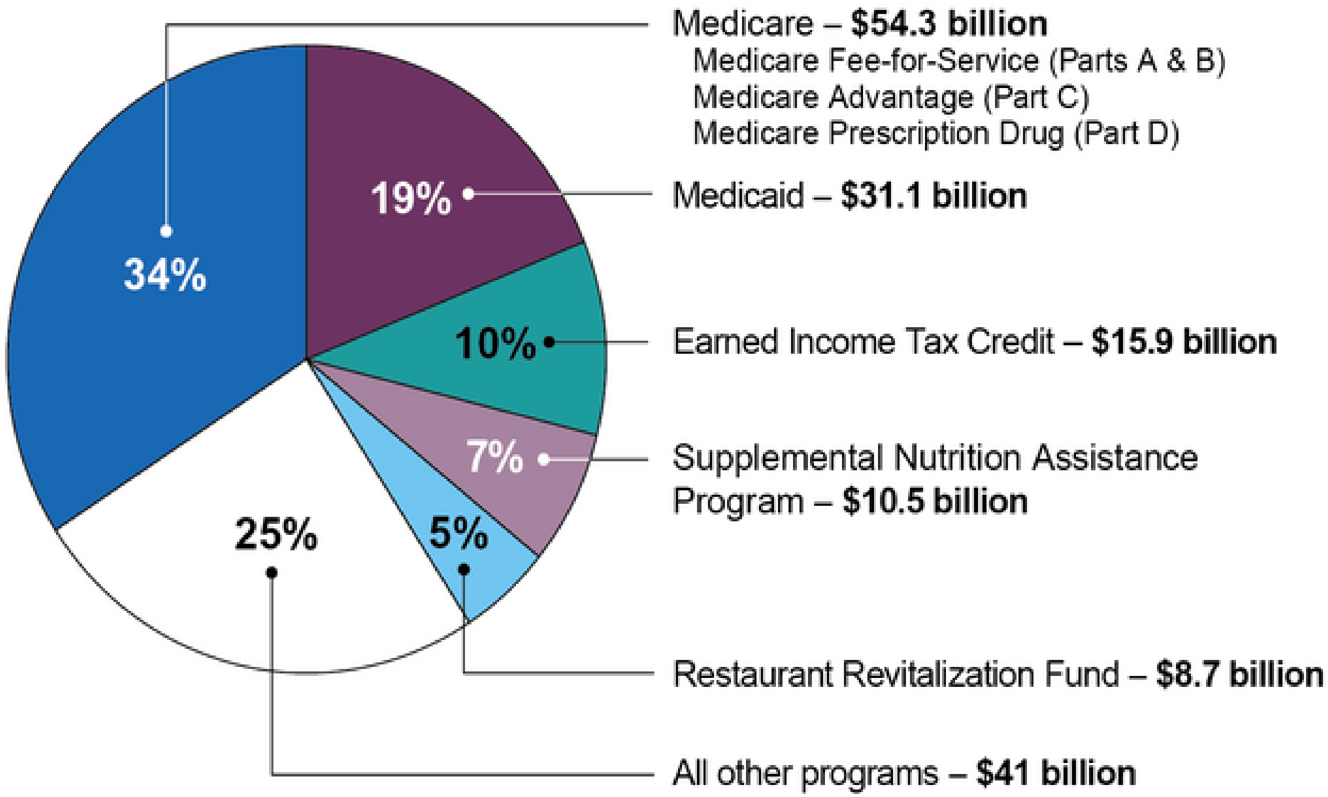
Cumulative Improper Payments (FY 2003-2024):

➢ **Approximately $2.8 trillion**

- FY 2024 saw a decline from the $236 billion improper payments in FY 2023 due to winding down of certain pandemic-related programs

Source: GAO

FEDERAL IMPROPER PAYMENTS: Fiscal Year 2024

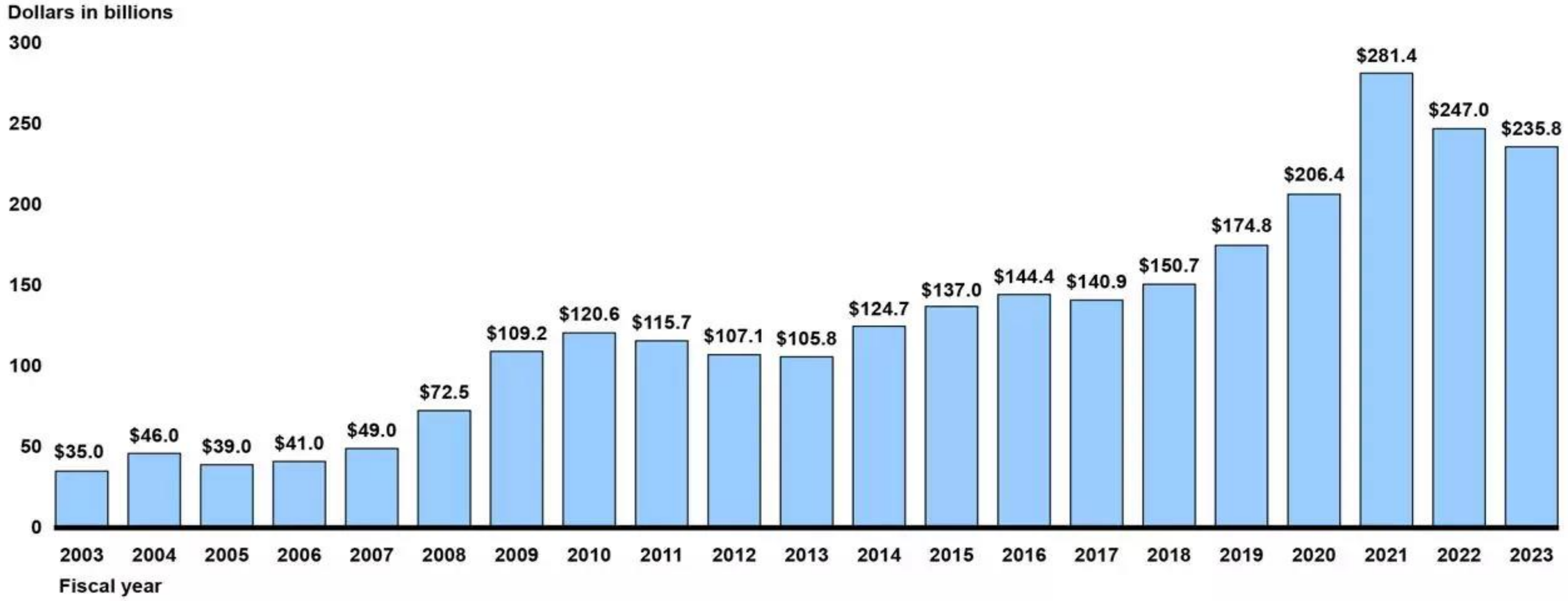


Source: GAO analysis of Office of Management and Budget PaymentAccuracy.gov data. | GAO-25-108172

In Fiscal Year 2025, GAO added "Improving the Delivery of Federal Disaster Assistance" to its <u>High-Risk List</u> of programs and operations with serious vulnerabilities to waste, fraud, abuse or mismanagement, or in need of transformation.

Improper Payments Remain Above Pre-Pandemic Levels and Continue To Grow

Reported Estimates of Government-wide Improper Payments Since FY 2003



Source: GAO. | GAO-24-106927

FEDERAL FRAUD: SCOPE AND TRENDS

Organized fraud groups are targeting federal programs at an increasingly larger volume and with greater speed than individual fraudsters

Annual Federal Fraud Losses (FY 2018-2022): $233 billion to $521 billion per year

Federal losses are estimated to average 3-7% of federal spending for a particular program

COVID-19 programs experienced fraud losses of about $300 billion

Three COVID-19 programs were hit hard by fraudsters: Paycheck Protection Program (PPP); Economic Injury Disaster Loans (EIDL); and Unemployment Insurance (UI)

Federal fraud risk is systemic and increasingly characterized by large-scale and organized fraud groups

The COVID-19 pandemic exposed major vulnerabilities in emergency response federal payment systems

Source: GAO

GROUP-ORGANIZED FRAUDSTERS

- Organized criminal networks play a significant role in federal payments fraud, responsible for nearly half of recent pandemic-related fraud convictions.
- In organized criminal enterprises (”fraud as a business”), one cell may focus on obtaining stolen identities, another on electronically preparing and submitting fraudulent documents, and another on moving and laundering money.
- Opportunistically organized groups (“fraud as a one-off gig”) involve clusters of individuals who come together as opportunities for fraud arise.
- It’s all about the PII: In most cases, fraudsters were convicted of crimes centered around stolen personally identifiable information (PII). Organized groups purchase large volumes of stolen or synthetic identities on the dark web. The stolen PII can come from data breaches, hacking and phishing.

Source: GAO

Blockchain & Decentralized ID: Securing Identities, Preventing Fraud in Federal Disaster Relief Payments

- **Disaster Relief Payments have become the Perfect Storm**
  - Emergency conditions create the ideal fraud environment: rushed payments, relaxed controls, weak verification systems
  - Traditional payment delays create extended fraud opportunity windows
  - Organized fraud rings exploit digital platforms and weak ID systems – using advanced tools (AI, bots, dark web data) to steal and monetize PII at scale
- **Digital identity verification through blockchain eliminates identity theft and impersonation fraud through:**
  - *Cryptographic ID verfication*: validate identity without exposing raw PII
  - ***No "Honey Pot"***: decentralized storage eliminates mass data breach risk
  - *User-Controlled Credentials*: retain and share only what's needed
  - *Tamper-Proof Identity Trails*: Transparent, shared, immutable records prevent synthetic and duplicate IDs

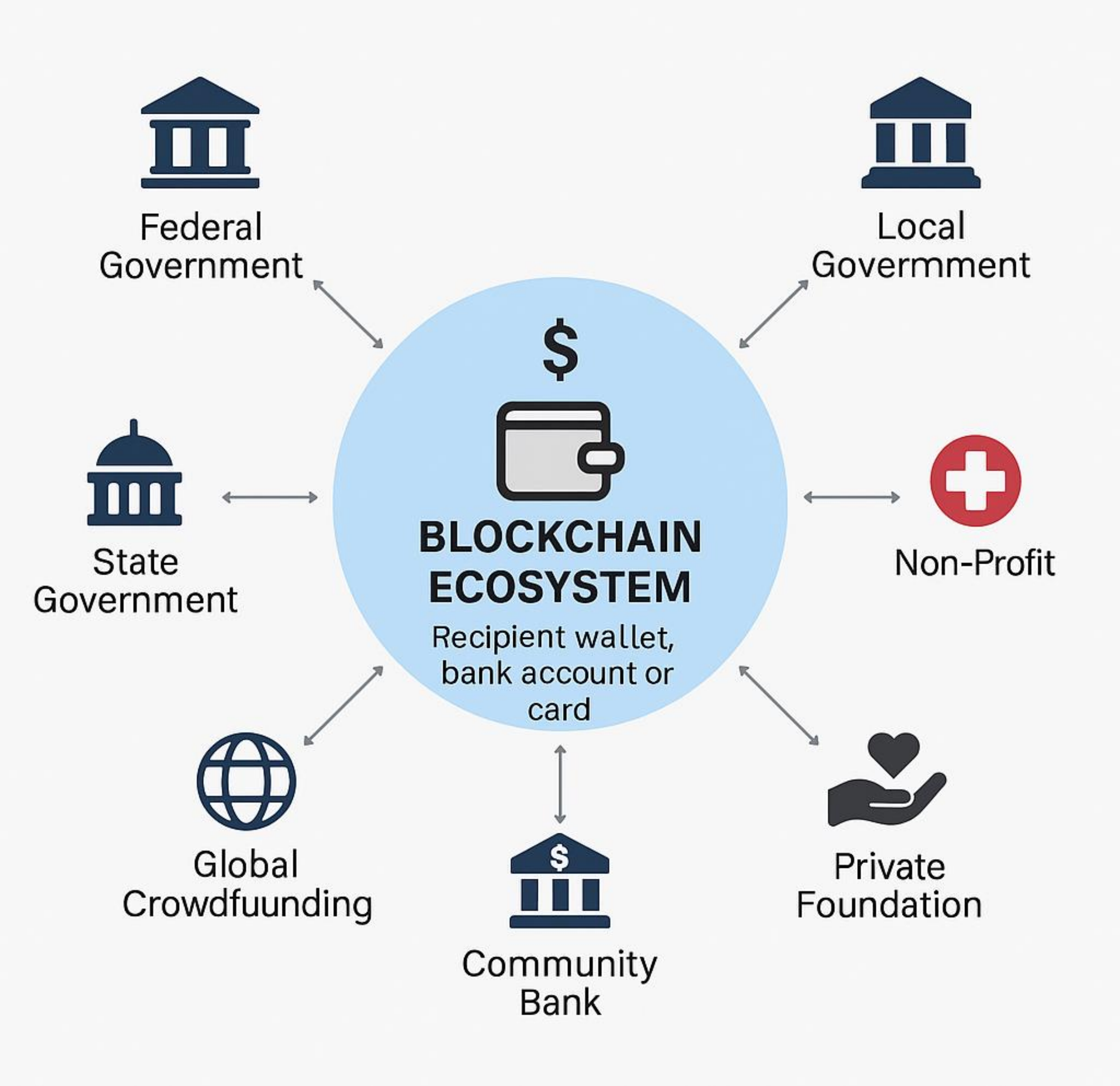
Blockchain As the Foundation for Trustworthy & Secure Government Disaster Relief Payments

How Blockchain Enables Shared Transparency and Data Coordination –

- *Decentralized Ledger*: All parties operate on a shared, tamper-proof ledger
- *Real-time Auditability*: Trace every disbursement from federal to end-user
- *Smart contract & Nodes*: Automate and validate payments with multi— stakeholder governance
- *Privacy-Preserving Digital IDs (DIDs)*: Cryptographically verified identity, stored locally – not centrally in "honeypots"
- No Single Point of Failure: Resilient, distributed architecture across all actors

Blockchain Ecosystem for Faster, Safer Financial Aid Delivery

A decentralized payment infrastructure connects trusted stakeholders through a shared ledger. Each node contributes to a secure, transparent and fraud-resistant financial aid delivery system.



Partnering with States to Achieve Federal Priorities: Stakeholder Action Plan

- *Support State-Federal Data Coordination*: Deploy blockchain nodes to improve transparency and data sharing

- *Advance Decentralized Digital ID Pilots with States*: Partner with states to issue and test cryptographically secure digital wallets and IDs that prevent ID theft

- *Build Tokenized Payment Infrastructure*: Collaborate on programmable token systems tied to disaster relief rules and smart contracts

- *Participate in State-Led Innovation Sandboxes*: Work with states to modernize financial aid delivery through public-private pilots and policy labs.