Strategic Analysis of Global Trade Settlement, Sanctions Enforcement, Alternative Sovereign Rails, and On-Chain Liquidity Infrastructure

An Institutional Assessment of Dollar Clearing, Sanctions Exposure, Sovereign Payment Systems, Stablecoins, CBDCs, and Tokenized Trade Finance

Narmandakh Jargalsaikhan

Working paper, version of 2 November 2026
Comments welcome

For Katya and Mum.

Abstract

Cross-border trade settlement is becoming more heterogeneous as sanctions exposure, correspondent-bank access, national payment policies, and technological development influence the choice of financial infrastructure. This report examines U.S. dollar clearing, ISO 20022 payment data, Executive Order 14114, alternative sovereign systems, countertrade, stablecoins, public-blockchain analytics, multi-CBDC platforms, dual-pool liquidity arrangements, real-world asset tokenization, and privacy-preserving compliance tools.

The assessment argues that alternative arrangements generally redistribute rather than eliminate legal, liquidity, counterparty, governance, and enforcement risks. Sovereign systems may reduce reliance on particular intermediaries while introducing participation and currency-liquidity constraints. Stablecoins combine transferable digital tokens with issuer, reserve, custody, and off-ramp dependencies. Tokenization can improve recordkeeping and transfer processes but does not itself establish the existence of physical assets or the enforceability of associated claims.

A hybrid settlement landscape is a plausible outcome: sovereign networks, public cryptographic infrastructure, legally structured tokenization, and privacy-preserving compliance tools may coexist. Their adoption will depend on operational resilience, reliable liquidity, enforceable rights, data governance, and applicable law rather than technical capability alone.

Contents

1 Executive Summary **4**
1.1 Scope, Method, and Limitations . . . 4
1.2 Related Work . . . 5

2 Legacy U.S. Dollar Clearing, ISO 20022 Payment Data, and E.O. 14114 **5**
2.1 Financial Messaging versus Monetary Settlement . . . 5
2.2 ISO 20022 Structured Payment Data . . . 6
2.3 Sanctions Exposure under E.O. 14114 . . . 6
2.4 OFAC Enforcement Lists: SDN and CAPTA . . . 7
2.5 The OFAC 50 Percent Rule . . . 7
2.6 Correspondent-Bank Compliance Workflows . . . 7

3 Alternative Sovereign Rails, Participation Constraints, and Currency Accumulation **9**
3.1 Sovereign Messaging and Settlement Infrastructure . . . 9
3.2 Project mBridge: Architecture, Liquidity, and Reported Activity . . . 9
3.3 BIS Graduation and Saudi Withdrawal . . . 10
3.4 BRICS Pay, the Proposed Unit, and CBDC Linkages . . . 10
3.5 The Currency-Accumulation Constraint . . . 11
3.6 Currency Structure of Russia's Trade Settlement, 2021–2025 . . . 11

4 Countertrade, Physical Netting, and Terms-of-Trade Costs **12**
4.1 Forms of Non-Cash Settlement . . . 12
4.2 Netting Mechanics . . . 12
4.3 Terms-of-Trade Costs . . . 13

5 Stablecoin Settlement, Issuer Controls, and Network Concentration **13**
5.1 Corporate Use of Fiat-Backed Stablecoins . . . 13
5.2 Issuer Controls . . . 14
5.2.1 Measured Freeze Timing on TRON . . . 14
5.3 Network Concentration on TRON . . . 17
5.4 Risk Substitution . . . 17

6 Public Blockchain Security and On-Chain Analytics **17**
6.1 Base-Layer Security and Censorship Resistance . . . 17
6.2 Protocol Incidents versus Custodial Failures . . . 18
6.3 On-Chain Analytics . . . 18

7 State-Issued CBDCs versus Permissionless Public Blockchains **18**
7.1 Architectural Comparison . . . 18
7.2 Programmability, Data Access, and Privacy Trade-offs . . . 19

8 Retail Settlement Example: Cross-Border Flower Delivery **19**

9 Operational, Legal, and FX Constraints in Dual-Pool Arrangements **20**
9.1 Licensing and Criminal Exposure . . . 20
9.2 Acquiring Constraints . . . 21
9.3 Domestic Capital Controls . . . 21
9.4 Rebalancing Delays and FX Exposure . . . 21

10 Tokenization, the Oracle Problem, and Privacy-Preserving Compliance **22**
10.1 Real-World Asset Tokenization 22
10.2 The Oracle Problem and Enforceability 22
10.3 Zero-Knowledge Proofs and Compliance 22

11 Comparative Settlement Matrix **23**

12 Implications for Stakeholders and Conclusions **24**
12.1 Implications for Stakeholders 24
12.1.1 Corporate Treasuries in High-Risk or Restricted Markets 24
12.1.2 Financial Institutions and Compliance Officers 24
12.1.3 Fintech Builders and System Architects 24
12.2 Conclusions 25

AI Assistance Disclosure and Author Responsibility **25**

References **25**

1 Executive Summary

International trade settlement is evolving through a combination of sanctions policy, correspondent-bank risk decisions, national infrastructure development, and new digital payment mechanisms. These developments are producing a wider range of settlement arrangements, but their legal status, operational maturity, and economic performance vary considerably.

Executive Order 14114 expanded the circumstances in which foreign financial institutions may face sanctions under Executive Order 14024 for specified activities involving Russia's military-industrial base. This exposure can arise without a U.S. dollar payment or a U.S. participant. It must be distinguished from liability for violating a prohibition independently applicable to a particular person or transaction [3].

The report's principal findings are:

- **Layers are distinct.** Messaging, clearing, settlement, and customer access to funds are different functions. Changing a messaging network does not necessarily change the settlement asset, banking dependencies, or applicable law.
- **Sovereign systems are not interchangeable.** Messaging platforms, RMB clearing infrastructure, retail payment links, and wholesale multi-CBDC platforms operate at different layers and serve different purposes.
- **Local-currency settlement has liquidity costs.** It can reduce the need for a vehicle currency, but persistent trade imbalances may create balances that are difficult or costly to deploy.
- **Countertrade shifts rather than removes risk.** It can reduce immediate cash-payment requirements while retaining legal, logistical, valuation, and performance risks.
- **Stablecoins substitute dependencies.** Fiat-backed stablecoins support rapid token transfers but retain issuer, reserve, custody, network, and fiat-conversion dependencies.
- **Public blockchains are transparent, not private.** They resist some forms of interference but do not guarantee privacy, uninterrupted inclusion, or protection from protocol and custody failures.
- **Tokens are not title.** Tokenization does not remove the need to verify physical assets, establish legal rights, and enforce claims.
- **Privacy-preserving proofs are not compliance by themselves.** Their legal sufficiency depends on the requirement being addressed and the reliability of the surrounding system.

The resulting landscape is likely to remain plural rather than converge on a single replacement for correspondent banking. Hybrid architectures are one plausible direction, subject to substantial legal, operational, and commercial constraints.

1.1 Scope, Method, and Limitations

This report is a qualitative comparative assessment, current as of October 29, 2026; the data in Sections 3.6 and 5.2.1 were retrieved on 30–31 October 2026. Apart from those two exhibits it is not an empirical survey, a legal opinion, or investment advice. Descriptions of alternative mechanisms do not endorse their use or establish that any transaction is permissible. Legal outcomes depend on the parties, goods, services, ownership, jurisdictional connections, applicable restrictions, and available authorizations.

Each mechanism discussed is classified by maturity:

- **Operational**: in live use with identifiable participants.

- **Pilot or demonstration**: tested with real participants but not in general production.
- **Proposal**: published by an identifiable sponsor but not implemented.
- **Illustrative**: constructed by the author to explain a mechanism; not an observed case.
- **Forecast**: the author's assessment of a plausible future development.

Sections 3.6 and 5.2.1 are limited empirical exhibits: Section 3.6 reproduces official Bank of Russia statistics (tier E2), and Section 5.2.1 reports the author's own measurements from OFAC and TRON data (tier E1), with the data and scripts deposited at [69]. Numerical examples are labeled as illustrative unless a source is cited. Time-sensitive legal and project-status information is stated as of the report date.

Sources and verification. Claims were drawn from official publications (OFAC, Treasury, the Federal Reserve, the BIS, central banks, statutes, and EU legislation), company and operator documentation, and major news organizations. Secondary sources were checked against primary documents where those were accessible. Claims that could not be traced to an adequate source were removed rather than retained with qualifications. Where only secondary reporting was available, the claim is attributed to that reporting. Legal descriptions summarize statutory and regulatory text and are not legal advice.

1.2 Related Work

This report draws on three bodies of work. Policy research frames payment-system competition as part of geoeconomic fragmentation [49]. Recent computer-science research measures how sanctions operate on public blockchains: block-producer censorship on Ethereum [51], the race between issuer freezes and fund movements in USDT and USDC [50], and the effect of sanctions on privacy tools and sanctioned entities [52, 53, 54]. Surveys of stablecoins and CBDCs cover design choices [56, 57], and proposals for two-layer systems combining central-bank money and regulated stablecoins [58] parallel this report's hybrid forecast. Those studies examine one mechanism at a time. This report compares legal, operational, and economic constraints across settlement arrangements, from correspondent banking to countertrade and tokenized claims, within a single framework.

2 Legacy U.S. Dollar Clearing, ISO 20022 Payment Data, and E.O. 14114

2.1 Financial Messaging versus Monetary Settlement

Cross-border dollar payments require a distinction between payment instructions and the accounts or systems through which obligations are settled.

A customer payment may generate an interbank message such as an ISO 20022 `pacs.008`; financial-institution transfers may use `pacs.009`, subject to the relevant network and usage rules. The message communicates instructions and associated information. It is not itself the movement of money. Swift transmits messages; it does not hold accounts or settle funds.

In correspondent banking, institutions use accounts maintained with other banks to discharge payment obligations. Depending on the route and participants, a payment may involve one or more correspondents, an internal book transfer, a domestic payment system, or offshore dollar infrastructure.

CHIPS and the Fedwire Funds Service perform different settlement roles:

- **CHIPS.** Participants fund prefunded balances held in a CHIPS account at the Federal Reserve Bank of New York; these funds move in and out by Fedwire. During the day,

CHIPS releases payments against those balances using liquidity-saving algorithms, and each released payment settles with finality on the CHIPS ledger. At the end of the day, remaining queued payments are settled after any required supplemental funding, and closing balances are returned to participants by Fedwire [15].

- **Fedwire.** Fedwire settles individual transfers on a gross basis between Federal Reserve accounts; an accepted payment order is settled by crediting the receiver's master account [43].

Fedwire therefore funds and defunds CHIPS positions; it is not a second settlement step for each CHIPS payment.

Many international dollar payments depend on U.S. correspondent institutions and U.S. payment infrastructure. This creates important points of U.S. legal and operational exposure. It is nevertheless too broad to state that every cross-border dollar payment must individually pass through CHIPS or Fedwire. Dollar payments can also settle outside the United States, for example through Hong Kong's USD CHATS, which settles interbank U.S. dollar payments across accounts held with its settlement institution [16], or as book transfers within a single bank. These arrangements can remove the need for a U.S. payment-system leg for an individual transaction. However, the settlement institution's own dollar liquidity is typically held and replenished through U.S. correspondent or Federal Reserve accounts. Offshore settlement therefore changes routing; it does not by itself remove exposure to U.S. law.

Settlement finality should also be distinguished from the time at which a beneficiary can use funds and from completion of the underlying commercial transaction.

2.2 ISO 20022 Structured Payment Data

ISO 20022 supports richer and more structured payment information than many legacy message formats. Relevant elements can include debtor and creditor information, ultimate payment parties, legal entity identifiers (LEIs), and structured address components. Whether an element is mandatory depends on the message, network, implementation rules, transaction circumstances, and effective date [17].

Richer data can improve reconciliation, straight-through processing, screening, and investigation. Its effectiveness depends on completeness, accuracy, preservation through the payment chain, and the receiving institution's controls.

Three limits apply:

- An ultimate debtor or ultimate creditor is a *payment-party role*; it should not be equated with a corporate ultimate beneficial owner.
- An LEI identifies a legal entity but does not, by its presence alone, establish the ownership and control analysis required for sanctions compliance.
- Message validation can identify missing or incorrectly formatted information. It cannot establish that a declared party, address, commercial purpose, or ownership representation is truthful.

Under its Standards Release 2026 plan, Swift had scheduled the removal of fully unstructured postal addresses from CBPR+ payment messages for 14 November 2026 [18]. In late August 2026, Swift deferred the cross-border payments elements of that release, including this removal, and the Federal Reserve correspondingly rescheduled its related Fedwire Funds Service release to November 2027 [44, 45]. As of the report date, no replacement date for the removal had been published [44].

2.3 Sanctions Exposure under E.O. 14114

Executive Order 14114 amended Executive Order 14024 to authorize sanctions against foreign financial institutions engaged in specified activities involving Russia's military-industrial base.

OFAC's guidance identifies activities including certain significant transactions and specified services involving that base. Its June 12, 2024 update states that the scope includes all persons blocked pursuant to E.O. 14024. Available measures include prohibiting, or imposing strict conditions on, U.S. correspondent or payable-through accounts, or blocking the foreign financial institution [3].

Such exposure may arise even where a transaction does not use U.S. dollars or involve a U.S. participant. This differs from a determination that the foreign institution has violated a primary U.S. prohibition applicable to its own conduct. Institutions therefore need to distinguish:

- restrictions directly applicable to the institution or transaction;
- exposure to sanctions designation or correspondent-account measures;
- export-control obligations;
- counterparty and ownership risks; and
- commercial decisions by correspondent banks or service providers.

The legal assessment depends on the relevant authority, counterparties, activity, significance analysis where applicable, and any authorization or exception [6, 7].

2.4 OFAC Enforcement Lists: SDN and CAPTA

The Specially Designated Nationals and Blocked Persons (SDN) List and the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List) identify different types of sanctions measures. Their effects must be read with the applicable legal authority and the designation record. Table 1 summarizes the distinctions.

List status changes over time. For example, Treasury announced the removal of Tornado Cash from the SDN List on March 21, 2025 [20]. Named examples must therefore be checked against list records current at the report date.

2.5 The OFAC 50 Percent Rule

Under OFAC's guidance, an entity owned 50 percent or more in the aggregate, directly or indirectly, by one or more blocked persons is considered blocked even if it is not separately named on the SDN List [21].

Indirect ownership must be assessed according to OFAC's framework, which looks through entities that are themselves owned 50 percent or more in aggregate by blocked persons. The analysis should not be reduced to an unexplained multiplication of percentages across every corporate chain [21].

Ownership and control are distinct. Control without the required ownership does not automatically produce blocking under the 50 Percent Rule, although other authorities, designation risk, and compliance concerns may remain.

Institutions therefore need reliable ownership information, documented aggregation, and procedures for responding to changes in ownership or sanctions status.

2.6 Correspondent-Bank Compliance Workflows

Compliance workflows vary by institution, transaction type, and applicable law. A representative workflow includes:

1. **Data validation.** Check required message fields and identify missing or inconsistent information.
2. **Sanctions screening.** Compare relevant parties, banks, locations, and other identifiers against applicable restrictions, using fuzzy-matching and transliteration methods where appropriate.

Table 1: SDN blocking measures and CAPTA restrictions.

Feature	**SDN blocking measures**	**CAPTA restrictions**
Basic effect	Property and interests in property of the designated person that are in the United States, come within the United States, or come within the possession or control of a U.S. person are blocked. U.S. persons are generally prohibited from dealing in them, subject to licenses and exemptions.	U.S. correspondent or payable-through accounts for the listed institution are prohibited or subject to strict conditions, as specified for each listing.
Persons identified	Individuals and entities; identifying information can include vessels, aircraft, and digital-currency addresses.	Foreign financial institutions.
Authority	Multiple statutes, executive orders, and program regulations.	Multiple program-specific authorities, e.g. 31 C.F.R. part 561, 31 C.F.R. part 566, and Directive 2 under E.O. 14024; the list also cites North Korea, Iran, and E.O. 13846 authorities [19].
Ownership	OFAC's 50 Percent Rule can block qualifying unlisted entities (Section 2.5).	Depends on the authority. Some correspondent-account restrictions expressly extend to entities owned 50 percent or more by a listed institution; others apply only to the named institution. Directive 2 under E.O. 14024, for example, extends to financial institutions owned 50 percent or more by the listed institutions [46].
Asset treatment	Blocking prevents unauthorized transfer or dealing; it is not government confiscation.	A CAPTA restriction is not, by itself, a general asset-blocking measure.
Examples	VTB Bank and Sovcombank, designated under E.O. 14024 on February 24, 2022 [13].	Bank of Kunlun, listed under 31 C.F.R. § 561.201(c) of the Iranian Financial Sanctions Regulations [19].

3. **Ownership analysis.** Assess blocked ownership and other relevant relationships.
4. **Alert review.** Investigate potential matches using dates of birth, identification numbers, addresses, BICs, and supporting records.
5. **Disposition.** Process, reject, or block as required, taking account of applicable authorizations and exceptions.
6. **Reporting and records.** Make required reports and preserve the decision record.

Matching thresholds are institution-specific and require calibration, testing, and governance; no universal threshold is assumed here.

A screening alert does not itself establish a prohibited transaction or a blockable interest. Blocking must be distinguished from rejecting a transaction that is prohibited but contains no property interest requiring blocking. OFAC requires initial blocking reports within ten business days [22]. The handling of blocked property depends on the asset and applicable regulations: blocked fiat funds and blocked virtual currency are subject to different holding requirements [23].

OFAC civil penalties may be imposed without proof of intent, but the penalty basis is statute-specific. As of the report date, the maximum civil penalty for violations of IEEPA-based sanc-

tions programs is the greater of $377,700 or twice the amount of the transaction underlying the violation; this amount has applied since January 15, 2025 [24]. Other statutes carry different maxima. Actual penalties are determined under OFAC's Economic Sanctions Enforcement Guidelines (31 C.F.R. part 501, appendix A).

3 Alternative Sovereign Rails, Participation Constraints, and Currency Accumulation

3.1 Sovereign Messaging and Settlement Infrastructure

Alternative national and cross-border systems operate at different layers and should not be treated as substitutes for one another.

CIPS (clearing and settlement). China's Cross-Border Interbank Payment System provides RMB payment clearing and settlement. China introduced it in 2015 to support international use of the renminbi. A 2024 Federal Reserve note puts CIPS's daily usage at about $60 billion, against about $1,800 billion a day for CHIPS, and reports that about 80 percent of CIPS payments still use Swift messaging even though CIPS has its own messaging capability [47]. CIPS is therefore an alternative channel for renminbi settlement, not a full replacement for either dollar clearing or Swift messaging.

SPFS (messaging). Russia's System for Transfer of Financial Messages, developed by the Bank of Russia, provides financial messaging. Messaging access does not itself supply a settlement asset, a correspondent account, or a legal exemption.

UPI international arrangements (retail). India's Unified Payments Interface supports retail payments, with specific cross-border acceptance and linkage arrangements. These should not be equated with wholesale trade-finance settlement.

Multi-CBDC platforms (wholesale). Projects such as mBridge explore cross-border transfers using central-bank digital money on shared infrastructure. Their participants, technical design, legal framework, liquidity arrangements, and maturity must be assessed separately.

3.2 Project mBridge: Architecture, Liquidity, and Reported Activity

The BIS reported on June 5, 2024 that mBridge had reached minimum viable product stage. The founding participants were the BIS Innovation Hub, the Bank of Thailand, the Central Bank of the United Arab Emirates, the People's Bank of China's Digital Currency Institute, and the Hong Kong Monetary Authority; the Saudi Central Bank joined as a full participant at that stage [25].

The BIS description identifies a shared mBridge Ledger supporting peer-to-peer cross-border payments and foreign-exchange transactions. The founding monetary authorities deployed validating nodes, the platform was compatible with the Ethereum Virtual Machine, and a bespoke governance and legal framework accompanied it [25]. This report does not characterize the consensus protocol further, because no public technical specification was identified.

Atomic payment-versus-payment (PvP) links two currency legs so that one settles only if the other settles under the relevant arrangement. This addresses principal settlement risk, the risk of paying away one currency without receiving the other. It does not eliminate foreign-exchange market risk, liquidity shortages, operational failure, replacement cost, or uncertainty about legal enforceability.

Reuters reported on January 16, 2026 that Atlantic Council analysis put cumulative mBridge activity at approximately $55.5 billion across more than 4,000 cross-border transactions, with the digital yuan estimated to account for approximately 95 percent of volume [26]. Other secondary

reporting dates the underlying figures to late 2025. These are reported estimates, not audited ledger statistics.

The estimated currency concentration indicates that observed activity depended heavily on digital-yuan use. It does not, by itself, establish that the platform had ceased to be technically multi-currency, or that equivalent liquidity was available in every participating currency.

3.3 BIS Graduation and Saudi Withdrawal

On October 31, 2024, at the Santander International Banking Conference in Madrid, BIS General Manager Agustín Carstens said the BIS was leaving mBridge because the project had matured to a stage where its central-bank partners could take it forward, and that the decision reflected neither failure nor political considerations. Asked whether mBridge could help BRICS countries avoid sanctions, he said that mBridge "is not the BRICS bridge" [27]. Analyses attributing the exit to geopolitical pressure are interpretations and should be attributed to their authors.

On September 20, 2026, the *Financial Times* reported that the Saudi Central Bank (SAMA) had withdrawn from mBridge [28]. In a statement to the newspaper, SAMA said it was no longer a participating member and that its participation ended on completion of a planned proof of concept on May 13, 2025, about eleven months after it joined as a full participant [29, 30]. No separate statement on SAMA's own website was identified. Commentators have linked the exit to U.S. policy concerns and the riyal's dollar peg; these are interpretations, not SAMA's stated reasons.

Changes in participation illustrate governance and continuity risks in cross-border platforms. Their causes should not be inferred solely from timing or broader geopolitical conditions.

3.4 BRICS Pay, the Proposed Unit, and CBDC Linkages

BRICS-related payment discussions encompass several distinct initiatives and proposals [1, 2, 8, 9]. Common branding does not establish common governance, official adoption, interoperability, reserve backing, or operational maturity.

- **BRICS Pay** should be described according to the specific organization, service, demonstration, or pilot under discussion. Claims that it connects CIPS, SPFS, UPI, and Pix require evidence of actual interfaces, participating institutions, transaction capability, and settlement arrangements; this report identified no such evidence.
- **The Unit** is a private proposal, not an adopted BRICS currency. Its white paper, dated May 9, 2023, names no authors or sponsoring institution and does not mention BRICS. It specifies a reserve basket of at least 40 percent gold, with no single other component above 30 percent, held by issuing nodes under an unnamed intergovernmental organization. Tokens cannot be redeemed for the basket, except when a node exits, and may be freely traded and used for payments [48]. The white paper therefore does not support describing the Unit as a non-recirculating, settlement-only instrument. Media reports linking the proposal to BRICS business bodies are secondary and do not establish official status.
- **CBDC linkages.** Reuters reported in August 2026 that the Reserve Bank of India had advocated linking BRICS members' CBDCs and fast-payment systems, and described associated technical, political, and liquidity hurdles [31]. This supports a description of a proposal under discussion, not operational deployment. Earlier reporting stated that the RBI had recommended placing the proposal on the agenda of the 2026 summit, which India chairs [59]; this report identified no record of formal adoption.

Claims that a circulating, asset-backed "BRICS Coin" would replace national currencies remain unsupported.

3.5 The Currency-Accumulation Constraint

Persistent bilateral trade imbalances can cause exporters to accumulate balances in the importing country's currency. These balances may be costly or difficult to deploy when conversion markets, banking access, investment options, hedging capacity, or demand for local goods are limited.

A bilateral trade imbalance should not be equated with a broader balance-of-payments imbalance. Nor does currency accumulation necessarily mean that balances are legally frozen or non-convertible. In India's Special Rupee Vostro Account (SRVA) framework, Reserve Bank of India guidance permits specified repatriation and investment uses, subject to the underlying transaction and applicable rules [32]. Practical constraints may nevertheless arise from banking risk appetite, sanctions exposure, market liquidity, and the available commercial uses of the currency.

An assessment should therefore identify:

- the account and the legal owner of the balance;
- permitted conversion, repatriation, investment, and hedging;
- actual banking and market access;
- the expected holding period and opportunity cost; and
- the currency and maturity of the exporter's liabilities.

The economic risk is not possession of local currency as such, but an inability to deploy or hedge it at acceptable cost within the exporter's working-capital horizon. Section 3.6 shows how the currency structure of Russian trade settlement has changed.

3.6 Currency Structure of Russia's Trade Settlement, 2021–2025

The Bank of Russia's annual reports publish the currency structure of Russia's settlements for exports and imports of goods and services with all partner countries, in three groups: rubles, currencies of "friendly" countries, and currencies of "unfriendly" countries. The last two labels are the Bank of Russia's own classification [68]. Table 2 gives the shares for 2021–2025.

Between 2021 and 2025 the ruble share of export settlements rose from 14.4% to 53.7%, and of import settlements from 28.2% to 54.4%. Over the same years the "unfriendly"-currency share fell from 84.6% to 14.4% for exports and from 67.6% to 15.0% for imports. "Friendly" currencies rose from 1.0% to 39.9% of exports by 2024 and then fell to 31.9% in 2025; for imports they peaked at 36.0% in 2023 and stood at 30.6% in 2025. The Bank of Russia separately reports that by the end of 2023 the RMB accounted for 35.8% of export revenue and 37.0% of import payments [68]. That figure uses a different base and is not added to the table.

These figures describe the currency in which settlement happens, not who bears the resulting risk. We argue that they are consistent with this report's central point: moving settlement into the ruble and into currencies of "friendly" countries changes which dependencies matter rather than removing them. A counterparty paid in rubles must be able to hold, convert or spend them (Section 3.5). The data here cannot measure that risk.

Table 2: Currency structure of Russia's trade settlements, percent of total (Bank of Russia [68]).

	Exports			Imports		
Year	Rubles	"Friendly"	"Unfriendly"	Rubles	"Friendly"	"Unfriendly"
2021	14.4	1.0	84.6	28.2	4.2	67.6
2022	27.8	8.6	63.6	28.1	15.2	56.6
2023	39.0	29.4	31.6	30.0	36.0	34.0
2024	41.5	39.9	18.5	43.6	34.5	21.9
2025	53.7	31.9	14.4	54.4	30.6	15.0

Note: Units: percent of settlements, all partner countries. 2021 is from the Annual Report 2023; 2022–2025 are from the latest report covering each year. Rows sum to 99.9–100.0 because of rounding. Source: Bank of Russia annual reports [68], transcribed; also in [69].

Limits. The series is annual with three groups, so it cannot show the RMB's share or isolate the effect of any dated measure. Each year's shares come from the latest report that covers it (2021 from the 2023 report); versions of the same year differ by 0.1 to 0.5 percentage points, so changes across 2021 and later years mix report versions. The Bank of Russia's definitions of "friendly" and "unfriendly" were not checked; they are Russian classifications, not OFAC or EU ones. The figures cover all partner countries, not Russia–China trade. Russian policy measures on settlement currency are not dated here. A monthly series is reported to exist but was not used. The shifts coincide with the sanctions period; this does not show that sanctions caused them.

4 Countertrade, Physical Netting, and Terms-of-Trade Costs

4.1 Forms of Non-Cash Settlement

Several distinct arrangements are often grouped under "barter":

- **Barter**: a direct exchange of goods for goods under a single contract.
- **Countertrade**: linked contracts in which a sale is conditioned on a reciprocal purchase.
- **Contractual set-off**: offsetting mutual obligations between the same parties under agreed terms.
- **Multilateral netting**: offsetting obligations among several parties through a netting agent or ledger.

Reporting since 2025 describes increased use of goods-for-goods trade involving Russia and its trading partners [4, 14].

Removing a cross-border cash payment does not remove sanctions, export-control, customs, tax, transport, or insurance obligations. Each delivery remains subject to the rules that apply to the goods, the parties, and the route.

4.2 Netting Mechanics

Countertrade arrangements may record reciprocal deliveries and offset contractual obligations over an agreed period. An illustrative cycle is:

1. An exporter delivers a commodity to a counterparty, and the agreed value is recorded as a credit.
2. Over the agreed period, importers in the exporter's country order goods from the counterparty's market, and their values are recorded as obligations.

3. At the end of the period, credits and obligations are offset. Residual balances are carried forward or settled under the contract.

The authority to net obligations, the treatment of residual balances, the length of any cycle, and the accounting consequences depend on the contracts, parties, and applicable law. Double-entry recording does not imply off-balance-sheet treatment; accounting treatment depends on the entity whose statements are prepared and the applicable standard.

4.3 Terms-of-Trade Costs

Countertrade may be priced on terms that differ from benchmark market prices. Two effects are commonly reported:

- **Commodity discounts.** Commodities affected by sanctions or shipping restrictions may be credited below benchmark prices. Discounts are commodity-specific and time-varying: a crude-oil discount is not evidence of a nickel discount.
- **Import premiums.** Suppliers bearing additional compliance, logistics, or payment risk may price goods above benchmark. The figures below are illustrative.

Illustrative calculation. Assume:

1. the commodity has an undistorted benchmark value of $100 million;
2. it is credited at a 25 percent discount;
3. equipment is priced 30 percent above its benchmark market price; and
4. quantity, quality, delivery terms, and timing are otherwise comparable, with freight, tax, financing, and insurance excluded.

The commodity credit is

$$\$100\text{m} \times (1 - 0.25) = \$75\text{m}. \tag{1}$$

The benchmark value of equipment this credit buys is

$$\frac{\$75\text{m}}{1.30} = \$57.69\text{m}. \tag{2}$$

Benchmark purchasing power therefore falls by

$$1 - \frac{0.75}{1.30} = 42.31\%. \tag{3}$$

Equivalently, obtaining $100 million of benchmark-priced equipment requires

$$\$100\text{m} \times \frac{1.30}{0.75} = \$173.33\text{m} \tag{4}$$

of benchmark-valued commodity, 73.33 percent more than under undistorted exchange.

Neither measure is an accounting loss or proof that sanctions caused the price difference. Those conclusions depend on carrying values, realizable alternatives, contract terms, and attribution.

5 Stablecoin Settlement, Issuer Controls, and Network Concentration

5.1 Corporate Use of Fiat-Backed Stablecoins

Some businesses in capital-controlled or correspondent-constrained markets use fiat-backed stablecoins, particularly USDT on TRON and Ethereum, to move value across borders. A typical

flow converts local currency into a stablecoin through an over-the-counter desk, transfers the token, and converts it into the destination currency through another intermediary. Some states have created formal channels for such settlement: since 2024, Russian law has permitted cryptocurrency settlement of foreign-trade contracts within an experimental legal regime approved by the Bank of Russia, with limited participants and duration [60].

Speed claims must specify the endpoint. Token confirmation on a blockchain is distinct from issuer redemption, from the recipient's access to fiat, and from completion of the commercial transaction. Each conversion step adds counterparty, custody, and legal dependencies.

5.2 Issuer Controls

Fiat-backed stablecoins combine a blockchain transfer mechanism with issuer-controlled contractual and administrative powers. Depending on the deployed contract and issuer policy, these powers may restrict transfers involving specified addresses and, in some contracts, remove balances held at them. Such controls are distinct from the underlying blockchain's consensus rules.

Issuer administrative functions differ by token, network, and contract version. Blacklisting stops the address from sending tokens, but it does not always stop it from receiving them. The verified source of the USDT contract on Ethereum checks only the sender against the blacklist, and a separate function, `destroyBlackFunds`, can remove a blacklisted address's balance; the USDC contract checks both sender and recipient. On TRON, a blacklisted address received USDT after its freeze: `TNwe3WoEX6XrQ5NPAeWPkvpTtdaf27XYxK`, frozen on 8 September 2026, received 1 USDT in a successful transfer on 9 September 2026 (transaction `89146d7875c198b7c1c23f26ce0e457a94108d56259ef0ae796f3cc1ae245843`).

Issuers may restrict addresses under their own terms and policies, in response to law-enforcement requests, or voluntarily. Tether announced in December 2023 that it would voluntarily freeze addresses added to OFAC's SDN List [33]. A formal warrant is therefore not a universal precondition for an issuer freeze.

Issuer controls are also not instantaneous. A freeze is itself a transaction that must be included in a block, so a holder who sees it coming can try to move funds first. An empirical study of USDT and USDC freezes from November 2017 to August 2025, covering more than $1.5 billion in frozen value, found that at least 7.3 percent of sanctioned USDT addresses and 18.7 percent of sanctioned USDC addresses were emptied before the freeze took effect [50]. That study reports that issuer control is imperfect, and its effectiveness depends on transaction ordering. Section 5.2.1 measures freeze timing on TRON.

5.2.1 Measured Freeze Timing on TRON

This subsection measures how Tether's freezes on TRON line up with OFAC listings. A "freeze" here means an `AddedBlackList` event: a log entry that Tether's USDT contract on TRON emits when an address is added to its blacklist, after which the address can no longer send USDT (incoming transfers are not blocked; see Section 5.2). We took every TRON-format address (a 34-character string beginning with "T") from OFAC's SDN_ADVANCED file, downloaded on 31 October 2026 [64]. It contains 346 such addresses (266 tagged TRX, 79 USDT and 1 XBT), held by 53 listed entities. We then retrieved all 9,124 `AddedBlackList` events from the contract (9,086 distinct addresses, 26 June 2020 to 30 October 2026) through the TronGrid interface [65]. All 346 addresses have a matching event. As a check on the event data, the 3,506 distinct addresses first blacklisted in 2025 equals the count BlockSec reports for TRON in that year [67].

To date the listings, we used the first day each address appeared in OFAC's daily list snapshots, kept in a public repository [66]. "Listing" below means this date. It is not the legal designation date. Resolution is about one day, and 345 of the 346 addresses have a date (the address tagged XBT does not). Of the 345, 242 (70.1%) were frozen on the listing day or the day before it. A further 97 (28.1%) were frozen two or more days before listing, 43 of them more

than 90 days before; none was frozen 31 to 90 days before. Six (1.7%) were frozen after listing, all of them listed on or before 4 December 2023, before Tether's December 2023 policy of freezing SDN-listed addresses [33] could apply. Among the 339 addresses listed after 4 December 2023, none was frozen after listing. The data are consistent with freezes that coincide with, or precede, listing for these addresses. They do not show who initiated a freeze or why.

We also rebuilt each address's USDT balance just before its freeze from TronGrid transfer histories. Of the 335 addresses with measurable activity, 173 (51.6%) held less than 1 USDT at the freeze and 234 (69.9%) held less than 1% of everything they had received. Of the 8.68 billion USDT received in total, 6.1% remained. The share holding less than 1 USDT was 65.8% (156 of 237) for freezes on the listing day or the day before, and 12.0% (11 of 92) for freezes two or more days before listing. These shares are not compared with the figures from [50] reported in Section 5.2, because that study's definition of an emptied address has not been checked against ours.

Table 3: Freeze timing and USDT held at freeze, OFAC-listed TRON addresses.

Panel A. All addresses, by freeze timing

Group	Addresses	Active	Held <1 USDT	Share
Frozen on listing day or day before	242	237	156	65.8%
Frozen 2+ days before listing	97	92	11	12.0%
Frozen after listing (listed on or before 4 Dec 2023)	6	6	6	100%
All	345	335	173	51.6%
Russia-program-tagged subset (included in the rows above)	11	8	4	50.0%

Panel B. Russia-program-tagged addresses (address-level)

Address	Entity	OFAC tags	Listed	Frozen	Lag	Received	At freeze
TX5GV4Dy...	Task Force Rusich	RU-EO14024	2023-05-19	2023-12-09	+204	106.85	0
TEFph7dZ...	Gambashidze	RU-EO14024	2024-03-21	2024-03-20	−1	9,841.00	9,841.00
TMGLqRQ4...	Gambashidze	RU-EO14024	2024-03-21	2024-03-20	−1	195,293.03	29,190.17
TFdTr9C3...	OKO Design Bureau	RU-EO14024	2024-05-02	2024-05-02	0	23.35	23.35
TLM3zA3E...	OOO KB Vostok	RU-EO14024	2024-08-24	2024-08-23	−1	38,003.03	1,285.03
TTUDyVhh...	Cryptex	CYBER2; RU-EO14024	2024-09-27	2024-09-26	−1	144,412,301.98	0
TDdbRFoB...	Chirkinyan	RU-EO14024	2024-12-05	2024-12-04	−1	146,071.75	0
TU4tDFRv...	Aeza Group LLC	CYBER4; CAATSA-RU	2025-07-02	2025-07-02	0	357,885.45	0
TFwjPSca...	Garantex Europe OU	CYBER4; RU-EO14024	2025-08-15	2025-08-14	−1	0	no activity
TJkBr9TZ...	Garantex Europe OU	CYBER4; RU-EO14024	2025-08-15	2025-08-14	−1	0	no activity
TNDjh6WG...	Garantex Europe OU	CYBER4; RU-EO14024	2025-08-15	2025-08-14	−1	0	no activity

Notes: Panel A: Active = with measurable USDT activity; Held <1 USDT = balance at freeze below 1 USDT. The 4 addresses with more than 30,000 transfers are excluded; all 4 are in the second row (93 valid of 97). Row checks: 237 + 92 + 6 = 335; 156 + 11 + 6 = 173. The final column is the share of addresses with measurable activity. The Russia-program row is a subset of the rows above, not an additional group: 10 of its addresses are in the first row and 1 in the third. Panel B: units are USDT (TRC-20), unconverted; dates UTC; lag in days. RU-EO14024 = RUSSIA-EO14024; CAATSA-RU = CAATSA - RUSSIA; OOO KB Vostok = Obshchestvo s Ogranichennoi Otvetstvennostyu Konstruktorskoe Byuro Vostok. "Listed" is the first-seen date in the list snapshots, not the legal designation date. Received counts gross pass-through flows. Small sample: 11 addresses, 8 entities; descriptive only. Sources: OFAC SDN_ADVANCED [64]; TronGrid [65]; list snapshots [66]; computed with [69] (version 1.0.0, accessed 2 November 2026); Panel B values are identical in the original run and the rerun.

Russia-program subset. The subset contains every address whose listed entity carries an OFAC program tag containing "RUSSIA" in the SDN_ADVANCED file (RUSSIA-EO14024 for 10 addresses, CAATSA - RUSSIA for 1; five also carry CYBER2 or CYBER4 tags). No address was added on any other basis. Among the 11 Russia-program-tagged TRON addresses, held by eight entities and first listed on eight distinct dates, all 11 have a dated listing and an observable `AddedBlackList` event, so all 11 are usable for the timing analysis. The window is the same as

Panel A of Table 3 (events to 30 October 2026); all 11 listings occur by 15 August 2025, so the result is unchanged under a window ending 31 August 2025.

Ten of the 11 were frozen on the listing day or the day before (lags of −1 or 0 days). The eleventh, listed on 19 May 2023 before Tether's December 2023 policy, was frozen 204 days after listing. The median lag is −1 day (minimum −1, maximum +204); no mean is reported because the single +204-day observation would dominate it. No address in the subset was frozen two or more days before listing, whereas 97 addresses in the full sample were. The split between before and after 1 December 2023 is degenerate (one address against ten), so the pre-policy case is reported individually rather than as a group estimate, and a split at 24 February 2022 is empty because all 11 were listed after that date.

Eight of the 11 addresses received USDT; three, all listed on 15 August 2025, never did and are excluded from the balance results rather than counted as drained. Of the eight, 4 (50.0%) held less than 1 USDT at the freeze, against 51.6% (173 of 335) in the full sample; the same 4 held exactly zero. The eight received 145.16 million USDT in total and held 0.04 million at the freeze (0.03%); received minus balance at freeze, a gross pass-through measure rather than distinct funds, was 145.12 million USDT. One address (TTUDyVhh. . . , Cryptex) accounts for 144.41 million of the amount received. Excluding it, the remaining seven received 0.75 million USDT and held 0.04 million (5.4%, against 6.1% in the full sample), and 3 of 7 (42.9%) held less than 1 USDT. Amounts are USDT on TRON, unconverted, at the time of each address's freeze. No comparison is made with the Ethereum figures of [50], for the reason given above.

The Russia-program subset is small, clustered across eight entities, and dominated by one high-value address; its results are descriptive and should not be read as representative of Russia-related stablecoin enforcement or of Tether's broader freeze performance. The pattern is consistent with freezes that coincide with listing for these addresses; it does not show who initiated them, why, or how the addresses were used.

Limits. Listing dates have about one-day resolution and come from a third-party archive; dates on or before 4 December 2023 are upper bounds on the true listing date. The 345 addresses are not independent events: they first appear on 34 distinct dates, and three dates account for 236 of them (68.4%). Four addresses with more than 30,000 transfers were excluded from the balance results, and 31 transfers of impossibly large value (about 2^{256} in size) in 30 addresses were ignored; their cause is unknown. A balance row is valid if the reconstructed balance lies between zero and total received, within a tolerance of max(1 USDT, 0.1% of total received). Gross USDT received counts pass-through flows, not distinct funds. A Tether freeze is an issuer-side contract action. The reason for a freeze is not public, and the cause of the 43 earliest freezes is untested. The sample covers all OFAC programs. A descriptive Russia-program subset of 11 OFAC-tagged TRON USDT addresses, held by eight entities, was analysed separately; given its small, clustered sample and concentration of value in one address, the results are reported as a bounded subset exhibit rather than a representative estimate of Russia-related stablecoin enforcement. Addresses removed from the SDN list before 31 October 2026 are not in the sample. None of the 346 addresses has a `RemovedBlackList` or `DestroyedBlackFunds` event up to 30 October 2026 (990 and 1,270 such events on the contract in total), so all 346 remained blacklisted, with their balances not destroyed, at the cutoff. For 25 entities that hold both a TRON address and an Ethereum-format address, the Ethereum side was not checked. We make no claim about intent, evasion or causation.

Replication. An independent rerun of the TRON pipeline from cached raw API responses reproduced 76 of 89 reported figures exactly. The 13 differences have a single cause. The original analysis was run in stages, and four high-volume addresses (34,101 to 71,568 USDT transfers each) were fetched beyond the 30,000-transfer cap applied to the rest of the sample, while four others were excluded at that cap. Applying the cap uniformly excludes all eight, reducing valid

addresses from 341 to 337 and received USDT from 8,678.8 million to 7,761.5 million. The headline shares move by at most 1.3 percentage points (held share 6.1 to 6.8 percent; held share for freezes two or more days before listing 6.9 to 8.2 percent; addresses holding less than 1 USDT 51.6 to 52.3 percent), and no conclusion changes. Separately, the OFAC list used in the rerun contains one TRON address added after the original snapshot (346 against 345), which affects only the listing-lag table. Reported figures are those of the original run. Rerun outputs and the difference report are included in the replication package [69].

Independent check. A sample of 10 freeze events was checked against on-chain records: for each, the transaction exists, it is an `AddedBlackList` event on the USDT contract, the blacklisted address matches, and the timestamp and transaction hash match the event data used here. All 10 matched.

5.3 Network Concentration on TRON

TRON block production is performed by 27 Super Representatives elected by votes from staked TRX [34]. Because the producer set is small, coordinated action by producers, or pressure on the hosting providers they use, could in principle delay or exclude particular transactions. This is an analytical risk, not a documented event.

Producers cannot freeze or confiscate a USDT balance. That requires the issuer's contract functions or a change to protocol rules adopted by the network. Delaying or excluding transactions (a consensus-layer action) is therefore distinct from blacklisting an address (an issuer action).

5.4 Risk Substitution

Replacing correspondent banking with stablecoin settlement does not eliminate counterparty risk; it substitutes one set of dependencies for another (Table 4).

Table 4: Risk substitution between correspondent banking and stablecoin settlement.

Dimension	Correspondent banking	Fiat-backed stablecoin settlement
Principal dependencies	Correspondent access, sanctions screening, intermediary decisions.	Issuer controls and reserves, network producers, on- and off-ramp intermediaries, custody.
Legal recourse	Account agreements, payment-system rules, and courts; deposit insurance applies only to eligible deposits, within limits and by jurisdiction.	Issuer terms, contract controls, and courts with often uncertain jurisdiction; no deposit insurance.
Restriction mechanisms	Screening, rejection, blocking, account termination.	Issuer blacklisting or freezing; producer-level exclusion of transactions; off-ramp refusal.
Time endpoint measured	Beneficiary funds availability in a given corridor; varies by corridor and start event.	Token confirmation on the network; fiat availability depends on the off-ramp.

6 Public Blockchain Security and On-Chain Analytics

6.1 Base-Layer Security and Censorship Resistance

Public, permissionless blockchains validate state changes across independent nodes using proof-of-work or proof-of-stake rules, propagate transactions through peer-to-peer networks, and au-

thorize transfers with digital signatures.

These properties make it difficult for any single party to rewrite history or permanently exclude a validly signed transaction. They do not guarantee prompt inclusion. Individual block producers can exclude transactions from their own blocks; the network-wide effect depends on the protocol, producer concentration, relay conditions, and duration. After the August 2022 Tornado Cash designation, at least 46 percent of post-merge Ethereum blocks were built by actors excluding Tornado Cash transactions, and the average inclusion delay for those transactions roughly doubled, from 15.8 to 29.3 seconds [51]. Exclusion delayed these transactions; it did not prevent them. A valid signature also does not guarantee that credentials have not been stolen or that the implementation is free of errors.

6.2 Protocol Incidents versus Custodial Failures

Assessments of Bitcoin's security should distinguish the base-layer protocol from custodial intermediaries. The protocol has a long operating history, but it is not incident-free: in March 2013, an incompatibility between software versions caused a chain split that required a coordinated response [35].

Major losses suffered by users of centralized platforms such as Mt. Gox, FTX, and Celsius arose in the custodial layer rather than from failures of the Bitcoin consensus rules. Their causes differed. Mt. Gox's former chief executive was convicted in Japan in 2019 of manipulating electronic records and acquitted of embezzlement [61]. FTX's founder was convicted in 2023 of fraud and conspiracy involving customer funds [62]. Celsius's former chief executive was sentenced in 2025 to 12 years in prison after pleading guilty to fraud [63].

6.3 On-Chain Analytics

Public blockchains are transparent ledgers. Blockchain analytics combines transaction-graph analysis with external information:

- **Co-spending and change-detection heuristics** infer common control from transaction structure. These apply specifically to UTXO-based systems such as Bitcoin; account-based networks require different methods.
- **Network-level data**, such as the observed origin of transaction broadcasts, may be correlated with addresses.
- **Off-ramp attribution** links address clusters to identified customers when they interact with regulated exchanges.

Attribution is probabilistic. Collaborative transactions, custodial pooling, and incomplete labels can undermine inferences. Cluster attribution should be presented with confidence limits rather than treated as proof of identity.

Empirical studies suggest sanctions change on-chain behavior without ending it. A study of sanctioned Bitcoin entities found sanctions effective for about half of them, while the others kept moving funds [54]. For Tornado Cash, sanctions cut deposit volume by about 71 percent, yet the service was still used in about 78 percent of Ethereum-related security incidents [52], and activity recovered only partially after the March 2025 delisting [53].

7 State-Issued CBDCs versus Permissionless Public Blockchains

7.1 Architectural Comparison

Retail CBDCs, wholesale CBDCs, and permissionless blockchains differ in governance, access, programmability, and data exposure. Table 5 compares them. Most entries are design-dependent rather than intrinsic to the category.

Table 5: Architectural comparison of retail CBDCs, wholesale CBDCs, and permissionless public blockchains.

Dimension	**Retail CBDC**	**Wholesale CBDC**	**Permissionless blockchain**
Governance	Issuer-specific; typically a national central bank.	Issuer- and platform-specific; may be single-issuer or multi-issuer.	Protocol rules and developer, validator, and user governance.
Access	Typically identity-linked through intermediaries.	Restricted to eligible institutions.	Open, pseudonymous addresses.
Transaction restriction	Depends on legal framework and design.	Depends on platform rules and participant controls.	Resistant to permanent exclusion; inclusion not guaranteed.
Monetary policy	Issuer policy.	Issuer policy for each currency.	Protocol rules; issuance schedules differ by network.
Programmability	Design-dependent; user-initiated payment logic is distinct from restrictions on money itself.	Settlement logic such as PvP.	Scripting and smart contracts; capability differs by network.
Financial privacy	Depends on access controls, data architecture, identity linkage, and lawful-access arrangements.	Depends on platform data-sharing rules.	Transparent ledger; pseudonymous but analyzable.

7.2 Programmability, Data Access, and Privacy Trade-offs

Depending on its design, a CBDC could technically support holding limits, conditional transfers, or time-limited units. Whether any such feature is used is a policy and legal choice, and some proposals exclude it expressly. The Bank of England and HM Treasury have committed that a digital pound would not be programmed by the state, and have distinguished user-authorized payment programmability from government programming of money; the digital pound remains a proposed design [36].

For any named project, each feature should be classified as implemented, proposed, technically possible, or hypothetical.

A transparent pseudonymous ledger is not necessarily private. Conversely, permissioned access does not by itself establish that a central bank sees all personal transaction data. Privacy outcomes depend on who holds which data, under what legal constraints.

8 Retail Settlement Example: Cross-Border Flower Delivery

[Observed service; inferred settlement mechanics.] This example is based on a real international flower-delivery service that accepts Apple Pay and delivers in Russia. The customer-facing steps were observed. The operator's internal settlement arrangements are not publicly disclosed, so steps 3 and 4 below are the author's inference of a plausible mechanism, not a documented one. The operator is not named.

A customer abroad orders flowers for delivery in Moscow. Customer funds are collected in one jurisdiction, and the local florist is paid from liquidity held in another. The example illustrates

settlement and liquidity mechanics only. It does not establish the availability or legality of any particular corridor, payment method, or service, and it does not imply that any operator conceals the nature of transactions.

1. **Collection** (observed). The customer pays the platform through Apple Pay. The wallet supplies an easy, familiar payment step, and funds reach the platform's corporate account outside Russia.
2. **Merchant of record.** The payment is accepted by a merchant of record, the entity that contracts with the customer, is identified to the acquirer, and is responsible for the sale. Merchant-of-record services are a common, lawful structure. Neither the merchant category code nor the place of incorporation resolves the sanctions, AML, or card-scheme obligations that apply to the transaction.
3. **Liquidity pools** (inferred). The operator holds cash in two places: an offshore pool, which increases when customer funds are received, and a local-currency pool, which decreases when suppliers are paid. In accounting terms, receipt of customer cash debits a cash asset and credits revenue or a customer liability.
4. **Payout** (inferred). The local florist is paid in rubles from the domestic pool under a standing fixed-price fulfilment contract, rather than through a cross-border transfer for each order.

No single payment crosses the border, but value is transferred across borders in economic terms, and the operator incurs obligations in both jurisdictions. A complete description must identify who owes the customer performance, who owes the florist payment, who owns each pool, and which entity holds which licenses. In the inferred model, the platform owes the customer delivery, the domestic entity or partner owes the florist payment under the fulfilment contract, and the corporate pool periodically funds the domestic pool. Whether these are one company or affiliated companies in different countries is not publicly known.

9 Operational, Legal, and FX Constraints in Dual-Pool Arrangements

9.1 Licensing and Criminal Exposure

Depending on jurisdiction and structure, an operator that accepts value in one jurisdiction and pays out in another may fall within money-transmission or payment-services licensing regimes. Supervisors sometimes describe such arrangements as informal value transfer systems.

United States. 18 U.S.C. § 1960 prohibits conducting an unlicensed money-transmitting business. The offense has three alternative limbs: operating without an appropriate state license where unlicensed operation is punishable under state law; failing to comply with federal registration requirements under 31 U.S.C. § 5330; and transmitting funds known to be derived from a criminal offense or intended to promote unlawful activity [37]. The maximum term of imprisonment is five years. On conviction, the court must order forfeiture of property involved in the offense or traceable to it (18 U.S.C. § 982(a)(1)); such property is also subject to civil forfeiture (18 U.S.C. § 981(a)(1)(A)) [38, 39]. Section 1960 is also a listed racketeering predicate [40].

European Union. Criminal-law measures on money laundering are set out in Directive (EU) 2018/1673, which also requires liability for legal persons. Under Article 10, a member state must establish jurisdiction where the offence is committed wholly or partly in its territory or the offender is its national, and may extend jurisdiction to other cases, including offenders habitually resident there or offences committed for the benefit of a legal person established there [41].

The nationality of a payer is not in itself a jurisdictional basis. Providing payment or money-remittance services without authorization is governed separately by member-state law implementing Directive (EU) 2015/2366, and penalties vary by member state [42]. Denmark does not take part in EU criminal-law measures of this kind.

Application. Whether these or other laws reach a particular offshore operator depends on its contacts with each jurisdiction, the conduct occurring there, its registration and licensing status, and the facts of each transaction. This report does not assess that question for any specific business, including the operator in Section 8.

9.2 Acquiring Constraints

Card schemes and acquirers monitor for transaction laundering, the processing of payments for one business through another business's merchant account. Where they detect it, acquirers may terminate the merchant account and withhold funds under the merchant agreement. A contractual reserve hold is not a seizure or forfeiture.

Onboarding a replacement merchant account requires underwriting, compliance review, and integration, which can take substantial time. If termination outpaces onboarding, a platform that depends on card acquiring can lose its ability to collect payments.

9.3 Domestic Capital Controls

Destination-country authorities may restrict or penalize cross-border netting that bypasses domestic foreign-exchange rules, including through action against domestic bank accounts. Russia, for example, permits cryptocurrency settlement of foreign trade only within an approved experimental regime [60], so netting outside authorized channels sits outside that framework. Applicable provisions and enforcement practice are jurisdiction-specific.

9.4 Rebalancing Delays and FX Exposure

When one pool is depleted and the other accumulates, rebalancing may take time, for example where it requires purchasing goods, shipping them, and selling them locally. During that period the operator has unhedged foreign-exchange and inventory exposure. The direction and size of any gain or loss depend on the operator's assets, liabilities, contractual payout amounts, pricing currency, and time to replenishment.

Illustrative exposure test. Assume a USD functional currency, an initial rate of RUB 100 per USD, and a move to RUB 125 per USD, a 20 percent fall in the dollar value of one ruble. (A rise from RUB 100 to RUB 120 per USD would be a 16.67 percent fall.) Fees, taxes, hedging, and changes in goods prices are ignored.

Table 6: Illustrative effect of ruble depreciation on different positions.

Position	Initial USD value	After move	FX effect
RUB 10,000 cash asset	$100	$80	$20 loss
RUB 10,000 fixed payable	$100 liability	$80 liability	$20 gain
RUB 10,000 cash matched to RUB 10,000 payable	$0 net	$0 net	none
$100 cash held for a RUB 10,000 payable	$0 net	$20 net	$20 gain

Holding dollars or dollar stablecoins against a fixed ruble obligation therefore benefits from ruble depreciation; a depleted ruble pool does not itself imply a loss. A loss arises in a different sequence: the operator pays $100 for imported inventory, expects to sell it for a fixed RUB 10,000,

and the ruble moves to RUB 125 per USD before collection, so the proceeds are worth $80. If the selling price can be raised to RUB 12,500, that loss does not arise.

A pricing markup is a buffer, not a hedge. If an operator charges $105 for a service with a $100 baseline cost, a $20 adverse cost movement leaves $105 - 100 - 20 = -\$15$ before other expenses.

10 Tokenization, the Oracle Problem, and Privacy-Preserving Compliance

10.1 Real-World Asset Tokenization

Tokenization creates on-chain representations of claims on off-chain assets [5, 10]. Major segments include:

- **Private credit.** Some platforms offer on-chain exposure to credit assets, such as trade receivables, through legal vehicles. Each product differs in legal vehicle, borrower structure, and investor eligibility. Reported yields depend on date and basis (gross or net, fees, defaults) and compensate for credit and liquidity risk.
- **U.S. Treasuries.** Tokenized short-duration Treasury products provide on-chain exposure to government securities, subject to eligibility and redemption terms.
- **Commodities.** On-chain records of vaulted gold and agricultural products may reduce some intermediation costs, subject to custody and audit arrangements [11, 12].

Performance claims for commodity-tokenization pilots, including claimed reductions in settlement time, were not supported by traceable methodology in the sources reviewed and are not relied on here.

10.2 The Oracle Problem and Enforceability

Several distinct risks separate a token from the asset it represents:

- **Data accuracy.** A smart contract can verify on-chain transfers but cannot independently verify that goods exist or meet specification. Sensors can be tampered with, and inspectors or custodians can issue false receipts.
- **Custody and fraud.** The asset may be lost, pledged twice, or misappropriated by the custodian.
- **Title and perfection.** Whether a token holder has an enforceable claim, and priority over other creditors, depends on the governing law and on any registration or perfection steps.
- **Insolvency.** The treatment of token holders on the insolvency of an issuer, vehicle, or custodian depends on the legal structure.
- **Cross-border enforcement.** On-chain code cannot seize off-chain assets. Recovery depends on the governing law, the forum, the debtor's and the asset's location, and the rules for recognizing foreign judgments.

High yields on tokenized credit may compensate for these legal and credit risks rather than reflect technological efficiency.

10.3 Zero-Knowledge Proofs and Compliance

Zero-knowledge proofs can demonstrate a specified property without disclosing the underlying data. Several components are often conflated:

- a **zero-knowledge proof**, which shows a statement is true;
- an **encrypted transaction record**;
- a **selective-disclosure credential** or identity attestation; and
- a **viewing-key system**, which grants designated parties access to transaction details.

Viewing keys are an optional system-level disclosure mechanism, not an inherent feature of zk-SNARKs. Research designs illustrate the separation: one proposed framework lets a privacy-preserving application de-anonymize linked illicit transactions by combining threshold encryption, which spreads the power to disclose across several parties, with zero-knowledge proofs [55].

Whether such a system satisfies a compliance obligation depends on the legal requirement, the statement proved, the reliability of its inputs, and the surrounding controls.

11 Comparative Settlement Matrix

Table 7 summarizes the arrangements discussed. Time endpoints differ across rows and are not directly comparable.

Table 7: Comparative evaluation of settlement arrangements.

Arrangement	Settlement asset and mechanism	Principal risk dependencies	Relevant time endpoint	Maturity
Central-bank swap lines	Central-bank credit in partner currencies.	Swap terms, political relationship, usage limits.	Drawdown availability.	Operational
Commercial local-currency settlement	Bank deposits in partner currencies.	Convertibility rules, banking access, hedging markets, sanctions exposure.	Funds availability; time to deploy accumulated balances.	Operational
Fiat-backed stablecoins	Issuer liabilities transferred on public networks.	Issuer controls and reserves, network producers, off-ramps, custody, applicable law.	Token confirmation; fiat availability at off-ramp.	Operational
Merchant-of-record collection	Card or wallet funds paid to the contracting merchant.	Acquirer and scheme rules, licensing, sanctions and AML obligations.	Merchant funding; onboarding time (separate).	Operational
Dual-pool liquidity	Prefunded balances in two jurisdictions.	Money-transmission licensing, FX and inventory exposure, capital controls.	Local payout; replenishment period.	Observed service; mechanics inferred
Countertrade and netting	Goods deliveries offset by contract.	Contract enforceability, sanctions and export controls, valuation, logistics.	Contractual offset period; shipping and customs.	Reported
Wholesale multi-CBDC	Central-bank digital money on a shared ledger.	Participation, liquidity by currency, governance, legal framework.	Ledger settlement.	MVP / pilot
RWA tokenization	Tokens representing off-chain claims.	Asset verification, title, custody, insolvency, cross-border enforcement, securities law.	On-chain transfer; underlying settlement (separate).	Pilot to operational

12 Implications for Stakeholders and Conclusions

12.1 Implications for Stakeholders

The following implications are conditional. Each presumes that the activity is lawful for the parties involved and is supported by legal advice and operational evidence.

12.1.1 Corporate Treasuries in High-Risk or Restricted Markets

- **Start with legal permissibility.** Confirm the applicable sanctions, export-control, and foreign-exchange rules and conduct counterparty due diligence before selecting payment routes or hubs.
- **Diversify routes where lawful.** Additional banking relationships and settlement routes can reduce single-point dependence, but they do not reduce exposure arising from ownership, control, or the underlying activity.
- **Treat entity segregation as limited.** Separating subsidiaries can isolate operations but does not by itself remove ownership, control, consolidated-risk, or sanctions exposure.
- **Evaluate stablecoin buffers case by case.** Any use requires assessment of issuer risk, custody, off-ramp access, accounting, and legal status; it is not a default.
- **Manage FX exposure explicitly.** Identify net currency positions and maturities. Pricing margins are buffers, not hedges.

12.1.2 Financial Institutions and Compliance Officers

- **Add ownership-graph analysis to name screening.** Graph-based tools can support analysis of multi-tier ownership under the 50 Percent Rule; they complement name and identifier screening rather than replace it.
- **Monitor E.O. 14114 exposure.** Identify activity that could constitute significant transactions or services involving Russia's military-industrial base, including transactions involving designated persons and specified items.
- **Screen on-chain exposure beyond exact matches.** Address screening should consider clusters, counterparties, and indirect exposure, not only exact matches to listed addresses.

12.1.3 Fintech Builders and System Architects

- **Use compliance controls, not compliance claims.** Allowlisting, identity attestation, and transfer restrictions can support compliance programs but do not by themselves establish legal compliance.
- **Design disclosure deliberately.** Where privacy-preserving systems are used, specify what is proved, who can access what data, and under what legal authority.
- **Harden asset verification.** Combine sensor data with independent physical audits, multiple custodians, and enforceable legal recourse.
- **Obtain the right authorizations.** Identify the registration and licensing requirements in each relevant jurisdiction; in the United States, federal registration and state licensing are separate requirements.

12.2 Conclusions

The global settlement system is becoming more plural. U.S. dollar clearing remains central to correspondent banking, while sanctions exposure, national policy, and new technology are encouraging the development of alternative arrangements.

None of these alternatives is frictionless. Sovereign platforms face participation and currency-concentration constraints. Countertrade can impose significant terms-of-trade costs. Stablecoins replace correspondent dependencies with issuer, network, and off-ramp dependencies. Public blockchains are analyzable. Dual-pool arrangements face licensing, acquiring, and FX constraints. Tokenization remains limited by asset verification and cross-border enforcement.

A hybrid settlement landscape is plausible, but no architecture examined here removes the need for reliable liquidity, enforceable rights, operational resilience, and compliance with applicable law. Permissionless infrastructure, sovereign systems, and privacy-preserving tools may coexist in different combinations rather than converge on a single dominant model.

AI Assistance Disclosure and Author Responsibility

Generative AI assisted with structural synthesis, outlining, language drafting, and revision. The author is responsible for the manuscript's analysis, source selection, revisions, and final content. Verification procedures and unresolved limitations are described in Section 1.1 and in the accompanying source record. The author checked a sample of 10 TRON freeze events against on-chain records (transaction, event type, address and timestamp); all 10 matched.

References

[1] Wikipedia. *BRICS Pay.* https://en.wikipedia.org/wiki/BRICS_Pay

[2] Aerapass. *BRICS Pay vs. Traditional FinTech: What Changes?* https://www.aerapass.io/blog/synergy-or-strife-brics-pay-fintech-and-the-path-forward/

[3] U.S. Department of the Treasury, OFAC. *FAQ 1147: How Does Executive Order 14114 Amend Executive Order 14024?* Updated June 12, 2024. https://ofac.treasury.gov/faqs/1147

[4] Euromaidan Press. *Frontline Report: Russia Revives Soviet-Era Barter Trade.* December 2, 2025. https://euromaidanpress.com/2025/12/02/frontline-report-2025-12-01-2/

[5] Allium. *What Is RWA Tokenization? A Definitive Guide.* https://www.allium.so/blog/what-is-rwa-tokenization-a-definitive-guide/

[6] Guidehouse. *How Executive Order 14114 Impacts Foreign Financial Institutions.* 2024. https://www.guidehouse.com/insights/financial-crimes/2024/executive-order-14114

[7] Cleary Gottlieb. *Impact of Recent US Secondary Sanctions Authority Targeting Foreign Financial Institutions.* 2024. https://www.clearygottlieb.com/news-and-insights/publication-listing/impact-of-recent-us-secondary-sanctions-authority-targeting-foreign-financial-institutions-supporting-russias-military-industrial-base

[8] BRICS Pay. *BRICS Pay News.* https://bricspayment.ru/en/news

[9] The Digital Banker. *BRICS Looks to Build New Corridors for Cross-Border Payments.* https://thedigitalbanker.com/brics-looks-to-build-new-corridors-for-cross-border-payments/

[10] Amplify ETFs. *A Primer on Tokenization and Real-World Assets.* https://blog.amplifyetfs.com/insights/a-primer-on-tokenization-and-real-world-assets-rwa

[11] Clapp. *RWA Gold Rush: 10 Platforms Tokenizing Real-World Assets in 2026.* https://clapp.finance/blog/rwa-gold-rush-10-platforms-tokenizing-real-world-assets-in-2026

[12] Spydra. *Tokenizing Agricultural Commodities.* https://www.spydra.app/blog/tokenized-agricultural-commodities

[13] U.S. Department of the Treasury, OFAC. *Russian Harmful Foreign Activities Sanctions.* https://ofac.treasury.gov/sanctions-programs-and-country-information/russian-harmful-foreign-activities-sanctions

[14] Business Standard. *From Oil to Pistachios: How Barter Trade Is Reshaping Global Commerce.* https://www.business-standard.com/world-news/barter-trade-russia-china-iran-pakistan-global-sanctions-impact-india-125100600722_1.html

[15] The Clearing House. *CHIPS Liquidity Algorithm.* April 2022. https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips_liquidity_algorithm_april_2022.pdf

[16] Hong Kong Monetary Authority. *Payment Systems.* https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/financial-market-infrastructure/payment-systems/

[17] Swift. *ISO 20022 for Corporates.* https://www.swift.com/corporates/iso-20022-corporates

[18] Swift. *ISO 20022: Removal of Unstructured Address.* https://www.swift.com/standards/iso-20022/removal-unstructured-address

[19] U.S. Department of the Treasury, OFAC. *CAPTA List.* https://www.treasury.gov/ofac/downloads/capta/captalist.txt

[20] U.S. Department of the Treasury. *Tornado Cash Delisting.* Press release SB0057, March 21, 2025. https://home.treasury.gov/news/press-releases/sb0057

[21] U.S. Department of the Treasury, OFAC. *FAQ 401: The 50 Percent Rule.* https://ofac.treasury.gov/faqs/401

[22] U.S. Department of the Treasury, OFAC. *FAQ 5: Blocking Reports.* https://ofac.treasury.gov/faqs/5

[23] U.S. Department of the Treasury, OFAC. *FAQ 646: Blocked Virtual Currency.* https://ofac.treasury.gov/faqs/646

[24] Office of Foreign Assets Control. *Inflation Adjustment of Civil Monetary Penalties.* 90 Fed. Reg., January 15, 2025. https://www.govinfo.gov/content/pkg/FR-2025-01-15/html/2025-00786.htm

[25] Bank for International Settlements. *Project mBridge Reaches Minimum Viable Product Stage and Welcomes Saudi Central Bank as Participant.* Press release, June 5, 2024. https://www.bis.org/press/p240605.htm

[26] Reuters. *China-Led Cross-Border Digital Currency Platform Sees Surge.* January 16, 2026. https://www.reuters.com/world/asia-pacific/china-led-cross-border-digital-currency-platform-sees-surge-2026-01-16/

[27] Reuters. *BIS to Leave Cross-Border Payments Platform Project mBridge*. October 31, 2024. Reproduced at https://www.globalbankingandfinance.com/bis-to-leave-cross-border-payments-platform-project-mbridge/

[28] *Financial Times*. Report on Saudi Arabia's withdrawal from mBridge. September 20, 2026. https://www.ft.com/content/ac104987-f43d-4e7d-97b6-057d98f7e422

[29] *Fortune. China Suffers Setback to Dedollarize Global Finance as Saudi Arabia Exits Beijing's Payment Scheme*. September 21, 2026. https://fortune.com/2026/09/21/china-dedollarization-mbridge-saudi-central-bank-sama-us-dollar-dominance-petrodollar/

[30] Trade Finance Global. *Saudi Arabia Has Withdrawn from China-Backed Payments Platform mBridge*. September 2026. https://www.tradefinanceglobal.com/posts/saudi-arabia-has-withdrawn-from-china-backed-payments-platform-mbridge

[31] Reuters. *BRICS Nations Discuss Linking Payment Systems, CBDCs, RBI Chief Says*. August 11, 2026. https://www.reuters.com/world/india/brics-nations-discuss-linking-payment-systems-cbdcs-rbi-chief-says-2026-08-11/

[32] Reserve Bank of India. *FAQs on International Trade Settlement in INR (SRVA)*. https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=3373

[33] Tether. *Tether Introduces New Policy to Strengthen Ecosystem Security*. December 2023. https://tether.io/news/tether-introduces-new-policy-to-strengthen-ecosystem-security/

[34] TRON Developer Hub. *Super Representatives*. https://developers.tron.network/docs/super-representatives

[35] Bitcoin. *BIP 50: March 2013 Chain Fork Post-Mortem*. https://bitcoin.org/bip/50/

[36] Bank of England and HM Treasury. *Response to the Digital Pound Consultation Paper*. January 2024. https://www.bankofengland.co.uk/paper/2024/responses-to-the-digital-pound-consultation-paper

[37] 18 U.S.C. § 1960. https://www.law.cornell.edu/uscode/text/18/1960

[38] 18 U.S.C. § 982. https://www.law.cornell.edu/uscode/text/18/982

[39] 18 U.S.C. § 981. https://www.law.cornell.edu/uscode/text/18/981

[40] 18 U.S.C. § 1961. https://www.law.cornell.edu/uscode/text/18/1961

[41] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02018L1673-20240519

[42] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. https://eur-lex.europa.eu/eli/dir/2015/2366/oj

[43] Federal Reserve Banks. *Operating Circular No. 6: Funds Transfers Through the Fedwire Funds Service*, § 8.2.6. Effective January 5, 2026. https://www.frbservices.org/wp-content/uploads/010526-operating-circular-6.pdf

[44] Bank of England. *Delay to the November 2026 RTGS Standards Release*. August 27, 2026. https://www.bankofengland.co.uk/news/2026/august/delay-to-the-november-2026-rtgs-standards-release

[45] Federal Reserve Financial Services. *Important Notice: Fedwire Funds Service's November 2026 Release Rescheduled to November 2027.* August 27, 2026. https://frbservices.org/news/communications/082726-fedwire-november-release-rescheduled

[46] U.S. Department of the Treasury, OFAC. *FAQ 970: Directive 2 under E.O. 14024.* https://ofac.treasury.gov/faqs/970

[47] Board of Governors of the Federal Reserve System. *Internationalization of the Chinese Renminbi: Progress and Outlook.* FEDS Notes, August 30, 2024. https://www.federalreserve.gov/econres/notes/feds-notes/internationalization-of-the-chinese-renminbi-progress-and-outlook-20240830.html

[48] *UNIT White Paper.* May 9, 2023. https://wp.unitfoundation.org/

[49] S. Aiyar et al. *Geoeconomic Fragmentation and the Future of Multilateralism.* IMF Staff Discussion Note SDN/2023/001, January 2023. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2023/01/11/Geo-Economic-Fragmentation-and-the-Future-of-Multilateralism-527266

[50] D. Wu, Y. Bai, S. Ren, et al. *Ordering Power is Sanctioning Power: Sanction Evasion-MEV and the Limits of On-Chain Enforcement.* arXiv:2603.27739, 2026. https://arxiv.org/abs/2603.27739

[51] A. Wahrstätter et al. *Blockchain Censorship.* arXiv:2305.18545, 2023. https://arxiv.org/abs/2305.18545

[52] E. Liu, M. Ryan, L. Zhou, and P. Berrang. *Evasion Under Blockchain Sanctions.* arXiv:2507.11721, 2025 (WWW '26). https://arxiv.org/abs/2507.11721

[53] R. Cristodaro, B. Kraner, and C. J. Tessone. *The Impact of Sanctions on Decentralised Privacy Tools: A Case Study of Tornado Cash.* arXiv:2510.09443, 2025. https://arxiv.org/abs/2510.09443

[54] F. Zola, J. A. Medina, and R. Orduna. *Assessing the Impact of Sanctions in the Crypto Ecosystem: Effective Measures or Ineffective Deterrents?* arXiv:2409.10031, 2024. https://arxiv.org/abs/2409.10031

[55] A. Chaudhary and H. Ivey-Law. *SeDe: Balancing Blockchain Privacy and Regulatory Compliance by Selective De-Anonymization.* arXiv:2311.08167, 2023. https://arxiv.org/abs/2311.08167

[56] A. Mahrous, M. Caprolu, and R. Di Pietro. *Stablecoins: Fundamentals, Emerging Issues, and Open Challenges.* arXiv:2507.13883, 2025. https://arxiv.org/abs/2507.13883

[57] Q. Tang and Y.-W. Si. *Central Bank Digital Currencies: A Survey.* arXiv:2507.08880, 2025. https://arxiv.org/abs/2507.08880

[58] H. Wen, S. Li, and J. Zhang. *Hybrid Monetary Ecosystems: Integrating Stablecoins and Fiat in the Future of Currency Systems.* arXiv:2505.10997, 2025. https://arxiv.org/abs/2505.10997

[59] Central Banking. *India Proposes Linking BRICS Countries' CBDCs.* January 19, 2026. https://www.centralbanking.com/fintech/cbdc/7974837/india-proposes-linking-brics-countries-cbdcs

[60] Bank of Russia. *Statement on the Law Permitting Cryptocurrency Use in Foreign Trade Settlements under an Experimental Legal Regime.* July 30, 2024. https://cbr.ru/eng/press/event/?id=18884

[61] Associated Press. *Mt. Gox Head Convicted of Manipulating Data, Cleared of Theft.* March 15, 2019. https://mynews13.com/fl/orlando/ap-top-news/2019/03/15/mt-gox-head-convicted-of-manipulating-data-cleared-of-theft

[62] U.S. Department of Justice. *Attorney General Merrick B. Garland Statement on Guilty Verdict in Jury Trial of Sam Bankman-Fried.* November 2, 2023. https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-statement-guilty-verdict-jury-trial-sam-bankman-fried

[63] NBC News. *Celsius CEO Alex Mashinsky Sentenced to 12 Years in Multibillion-Dollar Crypto Fraud Case.* May 2025. https://www.nbcnews.com/business/markets/celsius-ceo-alex-mashinsky-sentenced-12-years-multibillion-crypto-rcna205655

[64] U.S. Department of the Treasury, OFAC. *SDN_ADVANCED list file*, downloaded October 31, 2026. https://sanctionslistservice.ofac.treas.gov/api/PublicationPreview/exports/SDN_ADVANCED.ZIP

[65] TronGrid. *TronGrid API* (contract events and TRC-20 transfer endpoints), accessed October 2026. https://api.trongrid.io

[66] 0xB10C. *ofac-sanctioned-digital-currency-addresses* (daily list snapshots). https://github.com/0xB10C/ofac-sanctioned-digital-currency-addresses

[67] BlockSec. *1.26 Billion Frozen USDT: Blacklisting on Ethereum and Tron in 2025* (secondary source). https://blocksec.com/blog/1-26-billion-frozen-usdt-blacklisting-on-ethereum-and-tron-in-2025

[68] Bank of Russia. *Annual Report* 2023 (section 2.7), 2024 (Table 46) and 2025 (Table 42). Official publications page: https://www.cbr.ru/eng/about_br/publ/god/

[69] N. Jargalsaikhan. *Replication Package: Tether Freeze Timing for OFAC-Listed TRON Addresses and Bank of Russia Settlement-Currency Structure*, version 1.0.0 (software). Zenodo, 2026. https://doi.org/10.5281/zenodo.23833657