

Programmable Remittance Orchestration for Pakistan

A regulated architecture for giving global remittance providers one standardized digital-dollar settlement interface into Pakistan, while settling foreign currency through approved banking channels and delivering ordinary PKR through Raast.

Concept paper | Version 2.4 | 16 August 2026

The idea in one sentence

Give approved remittance providers around the world one standardized interface for regulator-approved digital-dollar settlement assets. Once compliant digital value reaches that interface, use a regulated orchestration layer to match it to the correct foreign-currency settlement, PKR payout and audit evidence.

Prepared for discussion with banks, money transfer operators, payment institutions and relevant Pakistani regulators.

This paper describes a proposed technical and operating model. It does not assume regulatory approval and is not legal advice.

Executive summary

Pakistan does not need to redesign how remittances are collected in every origin country. The narrower opportunity is to standardize what an approved foreign remittance provider sends into Pakistan. Today, each corridor can involve different banking connections, files, settlement arrangements and operational processes.

The proposal is to create a standardized inbound digital-dollar connector and a neutral orchestration layer behind it. The system begins when an approved foreign remittance provider submits a compliant remittance instruction and sends an approved dollar-denominated digital settlement asset to the inbound interface. How that provider collected the customer's fiat or acquired the digital asset is outside the core design and remains subject to the provider's own legal, treasury and compliance arrangements.

The permanent design is asset-neutral. Pakistan would standardize the interface, data model, controls and settlement rules rather than permanently select one private stablecoin. For a sandbox, this paper proposes USDC as a reference implementation. USDT or another regulator-approved dollar-denominated digital asset could occupy the same role through the same interface, subject to separate legal, reserve, operational, counterparty and technical assessment.

On the Pakistan side, the participating bank pays the beneficiary in ordinary PKR through Raast. A permissioned PKR settlement token can be added as a controlled settlement instrument, but it is not required for the basic remittance flow.

The key design principle is evidence. Blockchain events provide on-chain transaction references. Traditional banking events provide digitally signed institutional attestations. The orchestrator links these events into a single transaction record. A regulator can be given read-only access to the record and can independently verify the underlying evidence.

Important design choice

Across a blockchain, a bank account and Raast, the system should not promise literal atomic settlement. Those systems do not share one transaction engine. The practical goal is coordinated conditional settlement: the orchestrator only allows the next step when the regulator-defined evidence for the prior step has been verified.

The architecture is intentionally modular. SBP can require one-for-one settlement before every payout. If SBP later permits batching or net settlement, the same orchestration engine can support that policy without changing the customer experience.

The policy objective is simple. Formal remittance channels should become fast and inexpensive enough to compete on their own merits. A useful test of this architecture is whether a standardized inbound digital-dollar interface, Raast and tighter orchestration can reduce the underlying time, integration burden and operating cost of moving remittances into Pakistan, while preserving clear regulatory control and traceability.

1. What is being built, and where the system starts

The proposed product is best understood as a programmable remittance gateway and coordinator. Its system boundary starts at the standardized inbound digital-dollar interface. Foreign remittance providers remain responsible for collecting sender funds, performing the checks required in their jurisdiction and acquiring an approved settlement asset through whatever lawful route they choose. Pakistan standardizes the inbound handoff, not the provider's entire upstream business and not one vendor's token.

Participant	Role in the system
External remittance provider (outside the core system)	Collects value from the sender, performs required origin-side onboarding and compliance, acquires a regulator-approved digital-dollar settlement asset through its own lawful treasury or on-ramp arrangements, then submits a signed remittance instruction and sends the digital asset into the standardized Pakistani interface.
Standardized inbound digital-dollar connector	Provides one common handoff into the Pakistani system. It receives approved digital-dollar transfers and links them to signed remittance instructions. The interface is asset-neutral and may support one or more approved assets, networks and wallet structures behind the scenes.
Regulated USD conversion and settlement partner	Receives or controls the approved inbound digital-dollar asset, redeems or converts it into bank USD and routes the USD into the banking arrangement approved for the corridor.
Pakistani Authorized Dealer / payout bank	Receives or recognizes the foreign-currency settlement and pays the beneficiary in ordinary PKR through Raast.
Orchestrator	Matches the signed remittance instruction to the inbound digital-dollar transfer, tracks the transaction, verifies evidence, applies settlement rules, coordinates steps, handles exceptions and exposes the audit record.
Regulators	Set the permitted participants, licensing, reporting, settlement timing, data and control requirements. They can be given independent audit access.

What the orchestrator is not

It is not a new bank. It is not a public PKR currency. It is not a mechanism for bypassing foreign-exchange controls. It is the coordination and evidence layer that makes several regulated parties behave like one reliable end-to-end service.

2. A simple \$100 remittance

Assume Ahmed is in New York and wants to send \$100 to his mother in Lahore. For illustration only, assume the sandbox uses USDC as its approved digital-dollar asset and \$1 equals PKR 280. The same flow could use another approved asset without changing the orchestration model.

1	Outside the proposed system, Ahmed funds his chosen remittance provider. The provider performs the sender checks required in its market and acquires 100 USDC, the reference sandbox asset in this example, through its own lawful treasury or on-ramp process. Pakistan does not prescribe this step.
2	The provider connects to Pakistan. It submits a signed remittance instruction containing the required transaction, beneficiary and compliance information, then sends 100 USDC to the standardized inbound digital-dollar connector.
3	The orchestrator matches value and instruction. It detects the on-chain USDC transfer, verifies the provider's signed instruction and links both to Ahmed's remittance record.
4	The sandbox asset is converted back into USD. A regulated conversion partner redeems or off-ramps the 100 USDC and sends \$100 into the foreign-currency banking route agreed for the Pakistani partner.
5	The USD credit is confirmed. The relevant institution sends a signed confirmation that the required USD settlement has reached the designated banking channel.
6	PKR is released. Once the regulator-defined settlement condition is satisfied, the Pakistani payout bank sends PKR 28,000 to Ahmed's mother through Raast.
7	The payout is confirmed. The bank returns a signed payout event and payment reference. The orchestrator marks the remittance complete.

Note: The exact account path, settlement timing and reporting treatment must be agreed with SBP and participating banks. This paper does not assume that every remittance directly increases SBP's own foreign-exchange reserves. The objective is to settle the incoming foreign currency through the approved Pakistani banking channel and account for it correctly.

3. The standardized inbound digital-dollar connector

The core proposal begins here. Pakistan does not need to prescribe how every foreign provider turns local fiat into a particular stablecoin. A provider may use its own balance sheet, a bank, a licensed on-ramp, a stablecoin

issuer or another lawful arrangement available in its jurisdiction to acquire an asset that the Pakistani gateway has approved.

What Pakistan can standardize is the handoff. An approved provider sends a regulator-approved digital-dollar settlement asset into one common interface and submits the remittance information in one common machine-readable format. From that point onward, the Pakistani system handles matching, foreign-currency settlement, PKR payout and evidence.

- One standardized interface and transaction format can serve many origin markets and providers.
- The foreign provider can source the approved digital-dollar asset through its own lawful treasury process without Pakistan integrating to that upstream stack.
- The orchestrator can detect the approved inbound digital-dollar transfer programmatically and match it to the provider's signed remittance instruction.
- The conversion partner can specialize in redeeming or converting the approved digital-dollar asset into bank USD and routing that USD into the approved banking channel.

The digital asset is not being used because crypto must be part of remittances. It is being used because a widely supported dollar-denominated digital asset can create a simple common handoff into Pakistan. The permanent standard is the interface, not the token.

3.1 Asset neutrality and the sandbox reference asset

Asset neutrality is not asset indifference. Different stablecoins can have different issuers, reserve arrangements, redemption mechanics, network support and regulatory treatment. Each asset must therefore be approved separately even if it plugs into the same technical interface. The architecture should make switching or adding an approved asset straightforward without treating all assets as economically or legally identical.

For the initial sandbox, USDC can be used as the reference implementation because it gives the pilot one concrete asset to design, integrate and test against. That is an implementation choice, not an endorsement, exclusivity arrangement or permanent national standard. A later pilot or production network could support USDT or another approved dollar-denominated digital asset using the same remittance instruction, orchestration and audit model.

3.2 One connector does not have to mean one literal wallet address

The policy and product concept is one standardized connector. The implementation does not have to force every provider, asset, network and transaction through one physical blockchain address. A production design may use asset-specific or chain-specific wallets, partner-specific deposit addresses or other controlled routing for security, compliance and reconciliation. To the foreign provider, the interface can still feel like one connection to Pakistan.

This distinction matters because the standard being proposed is the interface and rulebook, not a single private key, single blockchain or single stablecoin issuer.

3.3 The connector receives value plus a remittance instruction

A digital-dollar transfer by itself does not say who should receive PKR in Pakistan, why the payment is being made or which sender information must travel with it. The inbound connector therefore needs two linked inputs: the digital value and a signed remittance instruction from the approved foreign provider.

The remittance instruction should contain the fields required under the approved operating model. At minimum, the design should support a unique remittance ID, origin-provider identity and reference, asset identifier,

amount and network, beneficiary and payout details, required sender and compliance information or references, purpose information where required, timestamp and the provider's digital signature.

The orchestrator should only accept an inbound remittance as matched when the signed instruction and the observed approved digital-dollar transfer agree on the required identifiers, asset and amount. Unmatched value or unmatched instructions should enter an exception queue rather than trigger a PKR payout.

A useful test

If the standardized digital-dollar handoff does not reduce integration complexity, settlement time or operational friction for the actual corridor, it should be simplified or removed. The architecture should never keep a blockchain step merely for appearance.

4. The orchestration layer

The orchestrator is the system that knows the whole story. Each institution still performs its own regulated function. The orchestrator makes sure those functions belong to the same remittance and happen under the correct rules.

4.1 A transaction as a state machine

A remittance moves through a small set of states. For example:

- Inbound instruction received
- Digital-dollar asset received
- Inbound value and instruction matched
- USD conversion confirmed
- USD settlement confirmed
- PKR payout authorized
- PKR paid
- Complete

A transaction cannot jump forward simply because an internal database flag was changed. Each important state change should require evidence from the party that actually performed the action.

4.2 Evidence, not blind trust

The evidence comes in two basic forms.

Type of event	Evidence	Example
Blockchain event	On-chain transaction reference	Digital-dollar asset received. Optional PKR settlement token burned.
Banking or API event	Clear message plus digital signature	Signed inbound remittance instruction accepted. USD credited to the agreed account. PKR paid through Raast.

4.3 Do not force the system into exactly four proofs

The early design used a simple mental model of two blockchain transaction references and two signed institutional attestations. That is useful for explanation, but production software should not assume there are exactly four events.

For example, these may be separate facts:

- A signed inbound remittance instruction was received and accepted.
- The approved digital-dollar asset was received at the inbound connector and matched to the remittance instruction.
- The conversion partner accepted and redeemed or converted the approved digital-dollar asset.
- USD was actually credited into the designated banking channel.
- A PKR settlement token was burned, if that feature is enabled.
- The recipient was paid through Raast.

The orchestrator should use an append-only event model. If a new regulator-required checkpoint is added later, it becomes another event rather than requiring a redesign of the whole system.

5. What a signed institutional attestation actually is

A signed attestation is not an encrypted message and it is not a scanned signature from a CEO. It is a normal, readable machine message with a cryptographic signature attached to it.

Simple analogy

Think of a clear envelope with a tamper-proof wax seal. Anyone allowed to see the envelope can read the message. The seal proves who sent it and whether the message was changed after it was sealed.

A payout bank might send a message like this:

```
{
  "event": "pkr_payout_completed",
  "remittance_id": "PKR-8421",
  "amount_pkr": 28000,
  "payment_rail": "Raast",
  "payment_reference": "R-981273",
  "timestamp": "2026-08-11T12:01:04+05:00"
}
```

The bank keeps its private signing key secret. It signs the exact message above. The orchestrator already has the bank's registered public key or certificate. It uses that public key to check the signature. The result is simply valid or invalid.

If somebody changes PKR 28,000 to PKR 29,000 after the bank signed the message, verification fails. If a random third party creates a new message and signs it with a different private key, verification also fails because it does not match the bank's registered public key.

5.1 Who creates the keys

Each institution should generate and protect its own private signing key. The orchestrator should never generate a partner's production private key and email it to them. The partner provides only its public key or certificate during onboarding. In a production bank environment, the private key would normally be protected using appropriate enterprise key-management controls such as an HSM or managed KMS.

5.2 What the orchestrator stores

- The original readable event message.
- The digital signature received with the message.
- The identity and public-key identifier of the signing institution.
- The time the event was received and the result of signature verification.
- Any bank payment reference, blockchain transaction reference or settlement reference linked to the event.

Digital signatures provide evidence of origin and message integrity. They do not make the underlying business fact true by magic. The system still depends on regulated institutions honestly attesting to events inside systems they control. The benefit is accountability: a valid signature makes it much harder for an institution or the orchestrator to rewrite the record later without detection.

6. PostgreSQL, blockchain and the source of truth

The operational database can still be PostgreSQL. Redis can still be used for queues, locks or short-lived state. Familiar infrastructure is not a weakness.

The important distinction is this: the database is the index and operating record. It should not be the only evidence.

- For an on-chain event, the database stores the transaction reference and relevant decoded details. An auditor can check the blockchain independently.
- For an off-chain event, the database stores the readable message and institutional digital signature. An auditor can verify the signature independently using the institution's registered public key.
- For the complete remittance, the database links all events to one remittance ID and shows whether the settlement rules were satisfied.

6.1 A regulator view

SBP or another authorized supervisor could receive a read-only API or dashboard. A reviewer could open any remittance and see the signed inbound instruction, the matching digital-dollar transfer and the subsequent settlement and payout timeline.

Time	Event	Evidence	Status
11:59:58	Inbound instruction	Signed provider instruction	Verified
12:00:01	Digital-dollar asset received	Base transaction 0x...	Verified
12:00:08	USD redemption	Signed converter event	Verified
12:00:21	USD credited	Signed bank / settlement event	Verified
12:00:25	PKR token burned	Stellar transaction ...	Verified, if enabled
12:00:31	Raast payout	Signed bank event + reference	Verified

Illustrative only. Times are shown to explain the event sequence, not to promise a specific settlement speed.

6.2 Should the audit record itself be on a blockchain?

It can be, but it does not have to be.

A sensible first version is hybrid. Keep sensitive transaction details in controlled systems. Keep blockchain transaction references where blockchain is actually used. Keep signed institutional attestations for banking events. Optionally anchor a cryptographic summary of the event log to a blockchain or other tamper-evident storage at regular intervals.

A later version could move more of the settlement state machine onto a shared blockchain. That would let several institutions see the same settlement status without relying on one company's database. However, a blockchain still cannot directly observe a bank account or Raast. Someone must submit the bank event. Requiring the bank itself to sign that event reduces the trust placed in the connector.

7. What if the digital-dollar asset and the PKR token use different blockchains?

That is not a fatal problem. It does mean the system should avoid pretending that one blockchain automatically knows what happened on another blockchain.

For example, the sandbox might use USDC on Base while an optional PKR settlement token exists on Stellar. A future approved asset could use another supported chain. The orchestrator can watch the relevant networks and link the transactions to the same remittance ID. For stronger independence, more than one approved watcher can observe each chain, or the institutions themselves can provide signed references to the relevant transactions.

Cross-chain messaging systems also exist, but using them adds another security and governance layer. For a regulated pilot, the simpler design is usually better: independently verify each chain, obtain signed evidence for off-chain events, then join the evidence at the orchestration layer.

The trust model

The goal is not to remove every trusted party. A bank must still be trusted to report what happened inside its own bank ledger. The goal is to stop any single orchestrator from being able to invent or silently rewrite the entire transaction history.

8. The optional PKR settlement token

The basic remittance model works without a PKR token. The payout bank can simply send ordinary PKR through Raast and return a signed attestation. That is enough to prove the local payout leg.

The PKR settlement token becomes interesting for a different reason. It creates a controlled environment in which regulated institutions can learn how tokenized PKR might behave without putting a retail stablecoin into public circulation.

8.1 How it could work

- A participating bank or approved structure holds PKR in a supervised account under rules agreed with regulators.
- A matching amount of PKR settlement tokens exists in whitelisted institutional wallets.

- The token cannot be freely transferred to the public. It is a controlled settlement instrument.
- When PKR is paid out, the corresponding settlement tokens can be burned or otherwise retired under the agreed model.
- The token transaction creates an additional on-chain control and audit point.

8.2 What it adds on day one

Its immediate operational value may be limited if the bank payout attestation already proves the same economic event. That should be stated plainly.

Its strategic value is optionality. Regulators and banks gain experience with issuance controls, whitelisted wallets, reserve matching, mint and burn rules, monitoring, incident handling and reconciliation. If Pakistan later chooses to support a broader tokenized PKR instrument, the ecosystem will have learned from a narrow institutional use case first.

There is no assumption that such a pilot should lead to a retail PKR stablecoin. Its value is partly that it gives policymakers real operational evidence before they decide whether broader tokenized PKR is desirable at all.

Positioning

The PKR settlement token should be presented as an optional, permissioned settlement instrument and regulatory learning environment. It should not be presented as a retail PKR stablecoin unless and until the relevant authorities expressly approve such a model.

9. Settlement timing and the meaning of atomicity

The policy question is simple: how closely must the foreign-currency settlement and the PKR payout be linked?

The strictest version could require proof that the incoming USD has reached the designated banking channel before PKR is released. A more flexible version could allow a participating bank to pay immediately against a controlled prefunded PKR pool and settle the incoming USD in approved batches later.

The system should be built to support both. The rule should be a configuration set by the approved operating model, not a hard-coded assumption.

Mode	How it works	Trade-off
Strict linked settlement	PKR payout waits until the required USD settlement confirmation is verified.	Strong one-for-one linkage. Potentially slower and more dependent on banking hours or bank finality.
Controlled prefunding	Bank pays from approved PKR liquidity once defined inbound conditions are met. USD is settled under an approved later cycle.	Faster payout and better batching. Requires regulator-approved exposure, limits and reconciliation.

Why not call this fully atomic? True atomicity is straightforward when all actions occur inside one transaction system. Here, the flow crosses a blockchain, traditional bank ledgers and Raast. The orchestrator can enforce conditional release and all-or-nothing business rules, but it cannot make independent external systems share one physical transaction boundary unless those systems themselves expose such a mechanism.

9.1 Batch settlement and the transaction manifest

Batching should reduce banking traffic without weakening transaction-level traceability. If SBP permits a conversion partner to settle several remittances through one USD bank payment, the orchestrator should treat that payment as a settlement batch. It should never treat the batch as one remittance.

Example. One hundred \$100 remittances may be settled as one \$10,000 USD credit. The receiving bank confirms one \$10,000 credit. Each of the 100 remittance records still points to that batch and retains its own sender, beneficiary, inbound digital-dollar transaction reference, allocated USD amount, expected or actual PKR amount, and payout evidence.

Each batch should have a unique batch ID and a signed transaction manifest. The batch record should identify the conversion partner, receiving bank and designated account, total USD amount, value date and time, banking payment reference such as a UETR or equivalent reference, number of underlying remittances, and a reference to the signed manifest.

Each manifest line should link the individual remittance ID, origin-partner reference, sender and beneficiary information required under the approved AML/CFT model, original amount and currency, inbound digital-asset identifier and transaction reference, USD amount allocated to that remittance, relevant purpose or compliance references, and the PKR payout obligation and status. The exact mandatory fields, and which fields must travel in the bank payment instruction versus a secure API or file, should be agreed with SBP and participating banks.

Accounting rule. Every unit of USD in a batch should be allocated once and only once. Fees, rounding, shortages and excesses should be explicit. The sum of individual allocations must reconcile to the approved gross or net settlement amount. Any mismatch should pause the affected items for exception handling.

Two events should remain separate. The conversion partner can attest that it redeemed or converted the approved digital-dollar asset and instructed the USD payment. The receiving institution should separately attest that the USD was actually credited into the designated banking channel. The second event is stronger evidence that foreign-currency settlement occurred.

Sensitive customer data should stay off public blockchains. The manifest can move through an encrypted API or file channel between approved parties. If a shared ledger is used, the system can anchor a hash of the manifest without publishing its contents.

Current SBP rules provide useful design precedent, but not automatic approval for this exact structure. SBP AML/CFT/CPF rules require traceable originator and beneficiary data in specified batch wire-transfer cases. Separate SBP foreign-exchange reporting guidance requires intermediary banks in Pakistan to pass complete details of underlying transactions to beneficiary banks. A pilot should therefore ask SBP expressly whether one institutional USD settlement may represent multiple individual remittances from multiple originators, and under what controls.

10. Compliance and data handling

Compliance should be part of the transaction model, not a separate spreadsheet after the payment is complete.

- The external remittance provider remains responsible for the sender checks required in its jurisdiction and for lawfully acquiring the approved digital-dollar asset it sends into the interface. It passes the required sender information, references and compliance attestations through the standardized remittance instruction.
- The payout institution performs the recipient checks required in Pakistan.

- Travel Rule or equivalent originator and beneficiary fields can be carried when required by the applicable regulatory framework.
- Sensitive personal data should remain off public blockchains. Public or shared ledgers should contain only the minimum identifiers and cryptographic references needed for verification.
- Every material compliance decision can be attached to the remittance event log with timestamps and responsible institution identifiers.

The system should be designed so regulators can inspect the full authorized record, while the public cannot reconstruct a remittance customer's identity or financial history from a blockchain explorer.

11. Regulatory context for discussion

This architecture touches two regulated domains in Pakistan: foreign exchange and payment systems on one side, and virtual assets on the other.

- SBP operates Raast as Pakistan's national instant payment system and is already pursuing cross-border connectivity, including the Raast-Buna initiative.
- SBP's Foreign Exchange Manual separately covers Authorized Dealers, Nostro accounts, inward and outward remittances, and foreign-exchange reporting. The exact foreign-currency settlement structure for this proposal should therefore be agreed with SBP and the participating Authorized Dealer.
- Pakistan now has a dedicated virtual-asset regulator. PVARA states that virtual-asset services, stablecoins and allied blockchain solutions fall within its regulatory ambit under the Virtual Assets Act, 2026. PVARA has also advised firms to seek prior authorization for pilots involving such services.

The practical implication is not that the model is prohibited. It means the pilot should be designed jointly with the relevant authorities rather than launched first and explained later.

Regulatory framing

The proposal should be presented as regulated payment infrastructure that standardizes the inbound handoff into Pakistan and uses digital assets only where they solve a specific settlement or interoperability problem. The permanent architecture is asset-neutral. USDC is only the proposed reference sandbox asset. Any alternative, including USDT, would require its own regulatory and risk approval. The consumer receives ordinary PKR. Banks remain responsible for bank money. Regulators retain control over who can connect, which assets are approved, what data must accompany each remittance, when PKR can be released and how the transaction is reported.

12. Core controls for a pilot

Control	Purpose
Whitelisted institutions and wallets	Only approved participants and settlement addresses can interact with the system.
Signed institutional events	Off-chain settlement events are accepted only when signed by a registered institution key.

Key management	Partners generate and protect their own private keys. Public keys or certificates are registered, versioned and rotated under a formal process.
Replay protection	Every signed event includes a unique event ID, remittance ID and timestamp so an old valid message cannot be replayed as a new payment.
Idempotency	Duplicate blockchain notifications or webhooks cannot create duplicate payouts.
Append-only audit log	Material events are not silently overwritten. Corrections are recorded as new events.
Reconciliation	Foreign-currency settlement, PKR payout and optional token balances are reconciled continuously and at defined closing periods.
Exception queue	Any mismatch pauses the affected remittance for review rather than forcing the system to complete.
Regulator access	Authorized supervisors can receive read-only transaction and evidence access at the granularity agreed for the pilot.

13. A practical implementation path

The architecture does not need to start with every feature. A staged approach keeps the first pilot understandable and lowers regulatory and operational risk.

Phase 1. Prove the remittance orchestration

One standardized inbound digital-dollar connector. One approved external remittance provider for the pilot. Use USDC as the reference sandbox asset while keeping the interface asset-neutral. One conversion partner. One Pakistani payout bank. No PKR token required. Signed inbound instructions, signed evidence for the banking legs and a regulator-readable event log.

Phase 2. Add redundancy and scale

Add more approved foreign remittance providers, more than one conversion partner and more than one Pakistani bank. The inbound interface stays consistent while the orchestrator routes transactions based on approved rules, corridor permissions, service availability and operational capacity.

Phase 3. Test permissioned tokenized PKR

If regulators see value, add a whitelisted PKR settlement token backed by an agreed supervised PKR structure. Keep it institutional and restricted.

Phase 4. Shared settlement substrate

If multiple institutions want a common tamper-evident state machine, move selected settlement state and evidence anchors to a shared ledger while keeping personal data and bank-confidential data off-chain.

13.1 What the pilot should measure

The pilot should be judged on economics and operating performance, not on whether it successfully uses blockchain. It should compare the proposed flow with an equivalent conventional remittance flow and measure:

- End-to-end time from sender funding to final PKR receipt.
- The all-in cost to the sender where origin-partner data is available, with origin-side collection and digital-dollar asset sourcing shown separately from the cost of the Pakistani gateway, banking settlement and payout.
- The cost and time from arrival of the approved digital-dollar asset at the standardized connector through USD settlement and final PKR payout. Origin-side asset acquisition can be measured separately where partners choose to provide that data.
- Operational effort for reconciliation, exception handling and transaction investigation.
- Failure, retry, reversal and exception rates.
- The amount and duration of liquidity or prefunding required under the approved settlement model.
- How quickly an authorized reviewer can trace a remittance from inbound value to foreign-currency settlement and final PKR payout.

If the proposed rails do not produce a meaningful improvement in cost, speed or operating simplicity, the architecture should be simplified. Blockchain is a means to an outcome, not the outcome itself.

14. Why this may be useful

The strongest case for the model is not that it uses crypto. The strongest case is that it could make a fragmented cross-border process behave like one inspectable system.

- Global remittance providers can connect to one standardized inbound digital-dollar interface and remittance-instruction format, without Pakistan prescribing how each provider collects local fiat, manages its upstream treasury or which approved asset it must use forever.
- Banks can continue using ordinary regulated bank money and Raast for the customer-facing PKR leg.
- The conversion partner can specialize in digital-dollar redemption and banking settlement without needing to operate a Pakistani retail payout network.
- The payout bank can specialize in local PKR settlement without directly handling the foreign digital asset if the approved structure isolates that role.
- The regulator can see the full chain of evidence rather than receiving fragmented reports from several systems after the fact.
- The architecture can start conservatively and later support additional banks, settlement assets, batch rules or tokenized money without rebuilding the remittance product from scratch.

15. Questions the pilot should answer with regulators

1. What exact event should count as final receipt of the foreign-currency leg for an inward remittance?
2. Which bank account, Nostro, correspondent or other settlement structure should receive the USD?
3. Must the USD credit be final before PKR is paid, or can regulated prefunding and later batch settlement be permitted under limits?
4. Which entities may legally receive, hold, transfer, redeem or convert each digital-dollar settlement asset approved for the corridor?

5. What licenses, NOCs or sandbox approvals are required from PVARA for the digital-asset portions of the architecture?
6. Can a permissioned PKR settlement token be tested as an institutional instrument, and how should the backing and legal claim be structured?
7. What sender, beneficiary, purpose-of-remittance and Travel Rule data must an approved foreign provider submit with each inbound remittance instruction, and which parties must be able to access each field?
8. What transaction-level evidence and reporting should be exposed to regulators in real time, near real time or periodically?
9. What reconciliation, tolerance and correction rules should apply to fees, rounding, short or excess USD settlements, failed PKR payouts, reversals, later amendments, and cases where one external leg fails after another has completed?
10. If batching is permitted, may one institutional USD settlement represent multiple individual remittances from multiple originators, provided every underlying transaction remains individually identified and reconcilable?
11. Which transaction fields must accompany the banking payment itself, and which may be carried through a secure signed manifest or API?
12. What receiving-bank event and evidence should constitute final confirmation that a batch USD settlement has arrived in the designated banking channel?
13. Which foreign remittance providers are eligible to connect to the standardized inbound interface, and what licensing, contractual or technical onboarding conditions should apply?
14. Should the standardized connector be implemented as one custody wallet, multiple chain-specific wallets, partner-specific deposit addresses or another controlled structure while preserving one common external interface?
15. What objective criteria should SBP and participating institutions use to approve a digital-dollar settlement asset, including issuer and reserve risk, redemption access, liquidity, supported networks, compliance controls and operational resilience?
16. What matching rules should apply between the signed remittance instruction and the observed digital-dollar transfer, and how should unmatched funds, duplicate instructions or incorrect assets or amounts be handled?

Conclusion

The proposal is not to replace Pakistan's banking system with crypto, and it is not to standardize how remittance companies collect money around the world. It is to standardize the point at which compliant digital-dollar value enters the Pakistani remittance system, then connect the regulated institutions behind that interface through a programmable coordination layer. The standard belongs to Pakistan's interface and rulebook, not to any one stablecoin issuer.

A regulator-approved digital-dollar asset can provide a simple common inbound value format for remittance providers around the world. For the sandbox, USDC can serve as the reference implementation. The foreign provider remains free to acquire the approved asset through its own lawful arrangements. It submits a signed remittance instruction and sends the matching digital value into the standardized connector. A regulated conversion partner can turn that value back into bank USD and route it into the approved Pakistani foreign-currency channel. A Pakistani bank can then deliver ordinary PKR to the recipient through Raast. USDT or another approved asset could later use the same architecture without redesigning the remittance product.

Where an event occurs on a blockchain, the system records the on-chain transaction reference. Where an event occurs inside a bank or conversion platform, the institution sends a clear digitally signed attestation. The orchestrator verifies the evidence, enforces the settlement rule and exposes a regulator-readable record.

A PKR settlement token is optional. It is not needed to prove that a Raast payout happened. Its potential value is as a narrow, permissioned test of tokenized PKR settlement that could create useful institutional experience if regulators choose to explore that path.

The measure of success is practical: can the system make formal remittances faster and less costly while preserving clear regulatory control and evidence? Blockchain components should remain only where they help achieve that result.

The core proposition

One standardized asset-neutral digital-dollar interface. One signed remittance-instruction format. One programmable transaction record. Clear responsibility for every leg. Evidence that can be independently verified. Ordinary PKR to the recipient.

Appendix A. A simple technical view

A conventional web stack is sufficient for the first implementation. The important part is how the inbound connector, signed remittance instruction, settlement responsibilities and evidence are structured.

Component	Possible role
Inbound instruction API	Receives the approved foreign provider's signed remittance instruction, validates schema, partner identity, timestamp and signature, and creates the remittance record before or alongside the matching digital-dollar transfer.
Digital-dollar connector / wallet layer	Exposes the standardized inbound digital-dollar interface. It can support approved asset and network adapters and may map one logical connector to multiple approved wallets or deposit addresses for security, partner segregation and reconciliation.
PostgreSQL	Remittance records, append-only event records, evidence metadata, participant configuration, reconciliation state.
Redis / queue	Short-lived jobs, locks, retries, webhook processing and chain event processing. Not a system of record.
Blockchain watchers	Observe approved wallets and token contracts, wait for the required finality and submit verified chain events.
Partner API / webhooks	Receive institution events. Require authenticated transport plus message-level signatures.
Signature verifier	Checks the partner signature against the registered public key, validates timestamp and event ID, then stores the evidence.

Rules engine	Determines whether the next step is allowed under the regulator-approved settlement policy.
Regulator API / dashboard	Read-only access to transaction timeline, evidence references, verification results, exceptions and reconciliation.
Optional shared ledger	Anchors event-log summaries or later hosts parts of the settlement state machine. Does not contain customer PII.

Example verification logic

```

receive signed_remittance_instruction
  -> verify provider identity and active public key
  -> verify digital signature over the exact instruction bytes
  -> validate required transaction, beneficiary and compliance fields
  -> verify requested asset and network are approved
  -> create remittance record in waiting_for_digital_asset state
observe inbound_digital_asset
  -> verify asset, network, approved destination and required confirmations
  -> match asset, amount and identifiers to the signed instruction
  -> if unmatched, route to exception review
  -> if matched, append verified inbound event
receive later signed_event
  -> verify partner identity and signature
  -> verify timestamp, unique event ID and remittance ID
  -> reject replay or duplicate event
  -> store original message + signature + verification result
  -> append event to remittance timeline
  -> evaluate settlement rule
  -> if rule is satisfied, authorize next action
  -> otherwise wait or route to exception review

```

Appendix B. Selected current references

Current public sources used to validate the regulatory and technical context in this discussion paper. Vendor-specific technical sources are illustrative only. The architecture does not recommend or require a particular private stablecoin issuer.

[State Bank of Pakistan, Raast](#). Pakistan's national instant payment system.

[State Bank of Pakistan, Raast cross-border payments](#). Current material on cross-border connectivity, including the Raast-Buna initiative.

[State Bank of Pakistan, Foreign Exchange Manual](#). Relevant chapters include Authorized Dealers, Nostro accounts, inward and outward remittances, and foreign-exchange returns.

[PVARA, Virtual Asset-Related Announcements and Activities Advisory, 26 April 2026](#). States that virtual-asset services, stablecoins and allied blockchain-based solutions fall within PVARA's regulatory ambit and that relevant pilots should seek prior authorization.

[Pakistan Virtual Assets Regulatory Authority](#). Current official licensing and regulatory framework pages for virtual-asset service providers.

[NIST FIPS 186-5, Digital Signature Standard](#). Public-key digital signatures for verifying message origin and detecting unauthorized modification.

[State Bank of Pakistan, AML/CFT/CPF Regulations, Regulation 11](#). Current wire-transfer rules include originator and beneficiary information requirements and specific traceability requirements for certain cross-border batch files.

[State Bank of Pakistan, Changes in Monthly Reporting of Foreign Exchange Returns \(ITRS\), 14 January 2022.](#)

Includes guidance that intermediary banks pass complete details of underlying transactions to beneficiary banks in the specified remittance context.

Sources checked 16 August 2026.