

Tokenized Roshan Access for Pakistan

A regulated architecture for presenting existing foreign-currency deposits and Pakistani investment products through a controlled digital-asset interface.

Concept paper | Version 1.1 | 16 August 2026

The idea in one sentence

Let eligible investors fund an approved RDA-linked USD position through a modern digital-asset interface, represent recognized backing with restricted digital units, and route investment into existing products such as Naya Pakistan Certificates while preserving bank custody, regulatory control and ordinary USD redemption.

Prepared for discussion with RDA participating banks, investment administrators, digital-asset infrastructure providers and relevant Pakistani regulators.

This paper describes a proposed technical and operating model. It does not assume regulatory approval, does not determine the legal classification of the proposed digital unit and is not legal, tax or investment advice.

Executive summary

Pakistan already has much of the financial infrastructure needed to attract foreign-currency investment from overseas customers. Roshan Digital Accounts provide remote access to Pakistani bank accounts, foreign-currency balances, repatriation and investment products. Naya Pakistan Certificates provide government-issued investment instruments in foreign currencies including USD, GBP and Euro. The question is whether a new distribution interface can bring additional investors and additional foreign currency into that existing regulated system.

The proposal is to build a controlled digital-asset interface above the RDA and NPC ecosystem. For the first pilot, an eligible investor in the UAE would send ordinary USD to local funding instructions provided through a regulated UAE collection partner. That partner would settle the USD to the participating Pakistani bank through an approved banking arrangement. Once the Pakistani bank confirms that the USD has been credited to the approved RDA-linked structure, the platform would create a matching number of restricted digital USD units in a managed wallet. One recognized dollar of backing would support one digital unit.

The investor could then select an approved investment term. Underneath the interface, the corresponding USD would be placed into the approved product, initially an NPC or another instrument expressly approved for the pilot. The investor could see principal, expected return, maturity information and redemption terms in a digital-

native interface. The economic return would come from the underlying regulated investment, not from the token itself.

The first version should be deliberately narrow. The digital units should not be freely transferable, listed on an exchange or usable in unrelated decentralized-finance applications. The customer should be able to deposit, hold, invest, receive recognized investment proceeds and redeem. The blockchain, if used, is a controlled record and programmable asset layer. It is not the source of the yield and it does not replace the bank account or the investment instrument.

The key technical design principle is evidence. The platform should not mint or burn merely because a bank balance changed. Participating institutions should provide clear transaction events such as USD deposit settled, investment subscribed, profit credited, redemption paid or prior event reversed. Important events should carry unique identifiers and, where practical, digital signatures. The platform verifies the event, applies the regulator-approved rules and then changes the digital state.

Important design choice

The proposal should not pretend that cash remains sitting in an RDA after it has been invested. Once USD is used to acquire an NPC, the backing has changed form. The legal and accounting model must define exactly what asset supports the digital units at each stage, who owns that asset and what claim the investor has against it.

The policy objective is straightforward. The pilot should test whether a digital-native interface can attract incremental foreign currency into Pakistan from investors who would otherwise keep that capital abroad. If the interface does not improve distribution, customer acquisition or operating transparency, it should not be expanded.

The strategic value is optionality. A narrow pilot can give banks and regulators practical experience with tokenized assets, managed wallets, mint and burn controls, signed institutional events, reconciliation and real-time supervision. If the model works, the same infrastructure could later support other regulated Pakistani financial assets. If it does not, the pilot can remain contained.

1. What is being built

The proposed product is best understood as a tokenized access layer for existing regulated financial products. It does not need to recreate RDA, NPCs, bank custody or customer due diligence. It connects those systems to a digital-native customer interface and keeps a clear record of why each digital unit exists.

Participant	Role in the system
Investor	Completes required onboarding, sends USD through an approved channel, chooses an investment and later redeems according to the approved rules.
UAE collection partner	Provides customer-specific USD receiving details in the UAE, maps funds to the verified investor, confirms local receipt and settles USD to the participating Pakistani bank through the approved corridor arrangement.
RDA participating bank	Opens or links the eligible account, receives foreign currency, performs required banking controls and executes permitted USD payments and redemptions.
Investment administrator / agent bank	Subscribes the approved underlying product, tracks the position, confirms maturity, profit and premature encashment events.

Participant	Role in the system
Digital-asset platform	Provides the application, managed wallet, token interface, orchestration, event verification, customer position ledger and reconciliation.
Token contract / ledger	Maintains restricted digital units and approved lock, mint and burn actions. It should not contain sensitive customer information.
Regulators	Set eligibility, asset structure, licensing, disclosure, custody, minting, redemption, reporting, privacy and supervisory requirements.
What the platform is not It is not a new offshore bank, a substitute for RDA, an algorithmic stablecoin or a mechanism for bypassing Pakistan's foreign-exchange rules. It is a controlled distribution and record layer above assets that remain inside an approved regulated structure.	

2. The pilot funding corridor: UAE to Pakistan

Phase 1 should avoid trying to solve global collection at once. The proposed pilot should use one origin market, the United Arab Emirates, one funding currency, USD, and one or a small number of participating Pakistani banks. The investor experience should begin with a local regulated funding endpoint in the UAE rather than asking the investor to initiate an international wire directly to Pakistan.

2.1 Give each investor local USD funding instructions

After the investor completes onboarding and an eligible RDA is opened or linked, a regulated UAE banking or payment partner can provide USD receiving details that map uniquely to that investor. Depending on the partner's capabilities and the approved legal structure, this could be an individual or virtual account, a virtual IBAN, or another customer-specific funding reference under a supervised collection arrangement.

The investor sends USD to those UAE funding instructions. If the investor holds AED, any AED-to-USD conversion should happen through existing regulated FX services before this step and remain outside the Phase 1 product. The token platform therefore accepts only USD funding.

2.2 The customer avoids the international wire, but the system does not

The cross-border banking leg still exists. The difference is that it happens between regulated institutions instead of being recreated by every customer. The UAE collection partner can settle the received USD to the participating Pakistani bank through an approved correspondent, partner-bank or other regulator-permitted arrangement. That settlement may occur transaction by transaction or, if regulators permit, in an institutional batch.

Each customer deposit should keep a unique funding ID and RDA mapping from the moment it is received in the UAE through final credit in Pakistan. If settlement is batched, a signed manifest should allocate every dollar in the institutional transfer to the correct underlying investor and RDA. The customer therefore gets a simple local funding experience while the institutions handle the cross-border settlement behind the platform.

2.3 Mint only after Pakistan-side credit is confirmed

Receipt by the UAE collection partner is not sufficient backing for the digital unit. The event that authorizes minting should be the regulator-defined confirmation that the investor's USD has been credited to the RDA or other approved Pakistan-side custody structure.

A simple sequence is: investor USD received by UAE partner; local receipt confirmed; USD settled to Pakistani bank; RDA credit confirmed; digital units issued. This keeps the one-unit-to-one-recognized-dollar rule attached to assets inside the approved RDA structure rather than to money that is still in transit.

Pilot simplification

Phase 1 is USD in and USD out. It does not need to solve AED conversion, multi-currency collection or a global network of origin banks. Those can be added only after the UAE-to-Pakistan USD flow works reliably.

3. A simple USD 10,000 investor journey

Assume Sana is an eligible overseas investor and wants to place USD 10,000 into a six-month USD investment. The return below is not specified because the applicable NPC or other approved product rate should always come from the current official schedule.

1	Sana completes onboarding. The platform collects the information required by the participating bank and any digital-asset regulator. An eligible RDA or other approved legal account structure is opened or linked, and customer-specific UAE USD funding details are assigned.
2	Sana sends USD 10,000 in the UAE. She sends USD to the customer-specific funding details provided through the regulated UAE collection partner. The partner confirms local receipt. This does not yet create digital units.
3	The Pakistan-side USD credit is confirmed. The UAE collection partner settles the USD through the approved banking arrangement. The participating Pakistani bank confirms that USD 10,000 has been credited to Sana's RDA or other approved structure.
4	The platform creates 10,000 digital units. After verifying the event and checking that it has not been processed before, the platform mints or records 10,000 restricted digital USD units in Sana's managed wallet.
5	Sana selects a six-month investment. The digital interface may use familiar language such as invest or stake, but underneath it is an instruction to purchase the approved regulated instrument.
6	The underlying investment is confirmed. The agent bank or administrator confirms that the USD 10,000 position has been subscribed. Sana's digital units are marked as committed to that position.
7	The application tracks the position. Sana can see principal, maturity date, current product terms and estimated return. Estimated return is not automatically treated as newly backed digital money.
8	Profit or redemption value becomes recognized. When the administrator confirms a payable profit, maturity amount or approved early-encashment amount, the platform applies the agreed rules. Additional digital units are created only when the legal and accounting model says corresponding recognized backing exists.
9	Sana redeems. The bank pays ordinary USD through the approved banking channel. Once the required settlement evidence is received, the corresponding digital units are burned or retired.

Illustrative only. The legal account path, asset ownership, exact timing of minting and the meaning of recognized backing must be agreed with SBP, PVARA, participating banks and the relevant investment administrator.

4. Why use a tokenized interface

The strongest argument is not that tokenization changes the economics of an NPC. It does not. The argument is that distribution, interface and financial language affect which investors discover and use a product.

A digital-asset investor already understands a flow that looks like: deposit dollars, receive a digital balance, commit that balance to a term, earn a stated return and redeem. The same investor may never research an RDA, navigate a Pakistani bank portal and then subscribe to an NPC even when the underlying economics are attractive.

At the time of this paper, SBP's July 2026 schedule lists gross annual USD NPC returns from 6.75 percent to 7.75 percent across the available tenors. Those rates can change and should never be hard-coded into the product. They do, however, illustrate why the underlying instrument may be commercially interesting to eligible investors.

The platform therefore tests a customer-acquisition hypothesis: can the regulated Pakistani product reach investors who are comfortable with digital assets but are not currently active RDA users?

A useful test

If the tokenized interface does not attract meaningful incremental foreign currency, lower customer-acquisition friction or improve transparency enough to justify its cost, it should be simplified or removed. Tokenization is a means to reach an investor and operate the product, not the policy objective.

5. The backing model

The backing model is the most important piece of the architecture because the asset underneath changes during the life of the investment.

5.1 One digital unit should map to one recognized dollar of value

The intuitive rule is simple: one digital USD unit should correspond to one US dollar of recognized backing under the approved legal and accounting model. The difficult part is defining recognized backing precisely.

Before investment, the backing may be settled USD cash in the participating bank. After the investor subscribes to an NPC, the cash has been exchanged for an investment position. At that point, the backing is no longer simply the bank-account cash balance. It is the legally recognized USD value or redemption entitlement of the underlying investment, plus any approved cash balances associated with the position.

5.2 Do not use a bank balance as the only source of truth

A bank balance can rise because of a new deposit, profit payment, correction, mistaken transfer or a previously pending settlement. It can fall because of a redemption, investment subscription, fee, reversal or other approved movement. The platform therefore needs transaction-level reasons, not just before-and-after balances.

A participating institution should send clear events such as deposit settled, NPC subscription confirmed, profit credited, redemption paid or prior event reversed. The platform processes the event only when the business rule for that event has been satisfied.

5.3 Individual and pooled structures

There are two broad legal models. In an individual model, each investor holds the relevant bank account and investment position directly, and the digital platform mirrors that individual position. In a pooled model, an approved bank, trustee, custodian or vehicle holds assets for multiple investors while the platform maintains a precise sub-ledger of each investor's entitlement.

The individual model is conceptually cleaner for an early pilot because it is closer to the existing RDA structure. A pooled model may improve operating efficiency later, but it should be used only if the relevant authorities expressly approve the ownership, insolvency, tax, custody and repatriation treatment.

6. The transaction and event model

The platform should know the full history of each investor position. A digital balance should never change because an administrator manually edited a number in a database.

6.1 A position as a state machine

A simple USD investment could move through states such as:

- Created
- Customer cleared
- USD deposit pending
- USD settled
- Digital units issued
- Investment instructed
- Investment confirmed
- Position active
- Maturity or early-exit amount confirmed
- USD redemption paid
- Digital units burned
- Complete

Some messages only describe what may happen next. Deposit initiated or redemption requested can be useful operational events without being financial finality events. The rules engine decides which confirmed event is strong enough to authorize the next state.

6.2 Signed institutional events

Important off-chain events should ideally arrive as readable machine messages carrying a digital signature from the institution that controls the underlying system. The signature proves which registered institution sent the message and whether the message was altered after signing. It does not make an incorrect banking fact true by magic. The institution remains accountable for what it attests to.

Event	Possible evidence	Typical digital action
USD deposit settled	Signed bank event with amount, account or pool reference, value date and unique event ID	Mint or authorize issuance of matching digital units.
Investment subscribed	Signed agent-bank or administrator event identifying product, tenor, amount and position reference	Mark the corresponding units as committed to the investment.

Event	Possible evidence	Typical digital action
Profit payable / credited	Signed administrator or bank event identifying the investor entitlement and value date	Create additional units only if the approved backing rule permits it.
USD redemption paid	Signed bank payment event and payment reference	Burn or retire the corresponding redeemed units.
Correction / reversal	Signed event referencing the original event ID and reason	Apply the approved compensating action. Do not erase history.

6.3 Duplicate messages and reversals

Every event should have a unique identity. If a bank webhook is retried, the same event must not mint twice. The platform checks whether it has already processed that event before changing financial state. Corrections should be recorded as new events that point back to the original event, rather than silently overwriting the record.

7. How the yield works

The yield comes from the underlying approved investment. The digital unit itself does not manufacture a return.

7.1 Estimated earnings and recognized backing are different things

Suppose Sana has invested USD 10,000 and the application estimates that she has economically earned USD 120 so far. The application may display that estimate. It does not follow that 120 new digital units should immediately be created.

Current NPC terms pay shorter-tenor profit at maturity and longer-tenor profit on specified periodic dates. For an early pilot, the safer rule is to mint additional units only when the administrator confirms that the profit or redemption entitlement has become a recognized asset under the approved accounting model. This keeps the visible estimated return separate from the actual token supply.

7.2 Early encashment should mirror the underlying economics

Current NPC rules permit premature encashment, including partial encashment, subject to the applicable return treatment. The digital interface should therefore not promise unlimited instant liquidity, but it also should not impose an artificial lock if the underlying product allows a regulated early exit. The approved early-exit rule should be reproduced faithfully.

7.3 Allocation must happen at the investor-position level

If several investors use the same digital unit but choose different tenors, the platform needs a separate position ledger. It must know who committed how many units to which product, on what date and under what terms. Profit is allocated to those positions, not simply spread across every token holder.

8. Managed wallets, the token contract and the blockchain

The customer should not need to manage seed phrases or understand blockchain mechanics. A managed wallet can be created as part of onboarding. From the customer's perspective, the product can feel like a modern financial application with a digital balance and a small set of permitted actions.

8.1 Restrict transferability in Phase 1

The first digital unit should be deliberately limited. It should not be freely sent to external wallets, listed on exchanges or used as collateral in unrelated applications. The allowed actions can initially be limited to mint, hold, commit to an approved investment, unlock when permitted, receive recognized proceeds, redeem and burn.

This restriction makes the pilot easier to supervise and avoids creating a public circulating dollar instrument before regulators have decided whether such a product is desirable.

8.2 The blockchain should remain an implementation choice

A public network such as Base could support the restricted token and managed wallets, and infrastructure providers such as Bridge or Privy could be evaluated for relevant components. Those choices should not be hard-coded into the policy architecture. The participating institutions should be able to change wallet provider or blockchain if security, regulation, privacy or economics require it.

If the blockchain does not create enough practical value to justify its complexity, the system can keep more of the state in conventional regulated infrastructure. The pilot should prove why the blockchain layer deserves to remain.

8.3 Minting authority is a high-risk privilege

The credentials that can create digital units should be protected with institutional key-management controls. Large administrative actions may require more than one approval. The contract should support pause controls, explicit roles and an audit trail. No developer or technology vendor should be able to create unexplained supply.

9. Reconciliation and the source of truth

The platform has to reconcile three related records. None should be allowed to drift silently away from the others.

Record	What it answers
Regulated asset record	What USD cash, NPC positions and recognized redemption or profit entitlements actually exist under the approved custody structure?
Customer position ledger	What does each investor legally and operationally own, including free balance, committed principal, estimated earnings, recognized proceeds and pending redemptions?
Digital-unit ledger	How many restricted digital units exist, which approved wallets hold them and which units are locked or being redeemed?

A mismatch is not an instruction to mint or burn until the numbers happen to match. A mismatch is evidence that something is wrong. The affected workflow should pause, the authoritative financial state should be determined, and then an approved corrective event should be recorded.

9.1 A regulator view

SBP, PVARA or another authorized supervisor could receive a read-only dashboard showing total recognized backing, total digital supply, outstanding investment positions, pending deposits and redemptions, reconciliation status, exceptions and the evidence supporting material state changes.

The trust model

The goal is not to remove banks, investment administrators or regulators from the trust model. The goal is to make responsibility explicit and to stop a technology operator from being able to invent, duplicate or silently rewrite the complete financial history of a position.

10. Liquidity, redemption and investment terms

The digital interface should never create the illusion of liquidity that the underlying investment does not have. Redemption rules should be driven by the actual product terms, settlement timing, bank availability and regulator-approved controls.

A customer request may move through requested, validated, investment encashment instructed, proceeds received, USD payment instructed, USD payment confirmed and token burn completed. The digital units can be frozen or marked as pending during that process so the same value cannot be used twice.

If an underlying product later supports same-day or near-instant encashment, the digital experience can become faster without changing the core architecture. If the instrument requires a waiting period, the interface should say so plainly.

11. Compliance and data handling

Compliance should be part of the transaction model from the start.

- The participating bank performs the account-opening, source-of-funds and customer checks required under the approved RDA structure.
- The digital-asset operator performs any additional onboarding, wallet and transaction controls required by PVARA or another relevant authority.
- Investment eligibility and disclosures should be checked before a position can be created.
- Sensitive customer data should remain in controlled systems. Passport details, bank account numbers, tax records and full transaction histories should not be placed on a public blockchain.
- Every material compliance decision should be linked to the relevant customer or position record with a timestamp and responsible institution identifier.
- Sanctions or compliance holds must be able to stop a deposit, investment instruction or redemption without corrupting the backing reconciliation.

If individual wallet balances on a public blockchain would reveal more financial information than regulators and customers consider appropriate, the pilot can use a more privacy-preserving structure, including pooled on-chain balances with a controlled off-chain customer ledger. That design choice should be deliberate.

12. Regulatory context for discussion

This proposal touches at least two regulated domains. RDA, foreign-currency accounts, repatriation and NPCs sit within Pakistan's banking, foreign-exchange and government-investment framework. Token issuance, custody, wallet services and digital-asset investment interfaces may also fall within PVARA's virtual-asset framework.

SBP currently describes RDA as a remotely opened, fully repatriable platform available to eligible non-resident Pakistanis and, under current eligibility material, certain foreign individuals and companies. Current SBP material also confirms that USD, GBP and Euro NPCs can be purchased from the corresponding foreign-currency RDA balance.

PVARA states that issuance, transfer, custody, exchange or arrangement of virtual assets, stablecoins and allied blockchain solutions fall within its regulatory ambit, and that pilots enabling such services require prior authorization. PVARA also currently states that sandbox applications for asset-referenced token issuance are open.

Regulatory framing

The proposal should be presented as a regulated access and distribution layer for existing financial assets. The pilot should not rely on the label stablecoin to make its case. The legal classification of the digital unit, the identity of the issuer, the customer claim, custody, backing and redemption rights should be settled with the relevant authorities before launch.

13. Core controls for a pilot

Control	Purpose
Eligible and identified customers	Only investors permitted under the approved RDA and digital-asset framework can participate.
Approved funding routes	Phase 1 accepts USD only through approved UAE collection arrangements. Local receipt alone does not authorize token issuance. The Pakistan-side RDA credit must be confirmed first.
Signed institutional events	Important off-chain financial events are accepted only from registered institutions using approved authentication and message-level signing.
Unique event IDs and replay protection	A retried webhook or duplicated file cannot mint, unlock or redeem the same value twice.
Restricted wallets and transfers	Phase 1 units remain inside the approved environment and cannot circulate publicly.
Controlled mint and burn roles	Only authorized services and approvers can alter supply. Privileged actions are logged and subject to limits.
Position-level investment ledger	Each investor's tenor, principal, dates, expected return and recognized proceeds remain separately attributable.
Continuous reconciliation	Regulated assets, customer positions and digital supply are compared continuously and at defined closing periods.
Exception queue	Any unexplained mismatch pauses the affected workflow instead of forcing completion.
Regulator access	Authorized supervisors can inspect backing, supply, positions, exceptions and supporting evidence at the granularity agreed for the pilot.

14. A practical implementation path

The system does not need to begin as a broadly transferable digital dollar. A staged approach keeps the policy experiment understandable.

Phase 1. Prove tokenized RDA access

One corridor, UAE to Pakistan. One funding currency, USD. One regulated UAE collection partner. One participating Pakistani bank, or at most a small number. One approved underlying investment category. Customer-specific funding instructions. Managed wallets. Restricted transferability. Individual RDA-linked

ownership or another structure expressly approved for the pilot. Signed evidence for local receipt, Pakistan-side credit, investment and redemption events. Regulator-readable reconciliation.

Phase 2. Add product depth and distribution

Add additional NPC tenors, participating banks and approved distribution partners. Improve the customer interface and compare acquisition performance across diaspora markets. After the UAE corridor is proven, add one origin market at a time using the same local collection pattern. Evaluate additional funding currencies only after the USD model works.

Phase 3. Add other regulated Pakistani assets

If the first product attracts incremental capital and operates safely, the same interface can be studied for government securities, sukuk, approved funds, equities, green instruments or other assets. Each product should retain its own suitability, liquidity and disclosure rules.

Phase 4. Consider broader digital-asset functionality

Only after real operating evidence exists should policymakers consider controlled wallet-to-wallet transfer, institutional settlement, approved exchange access, collateral use or links to trade and remittance infrastructure. These are options, not assumptions.

14.1 What the pilot should measure

The pilot should be judged on capital formation, customer acquisition, operating safety and regulatory usefulness. It should measure:

- Incremental foreign currency attracted that participants report would otherwise have remained outside Pakistan.
- Percentage of customers who were new to RDA or inactive RDA users before the pilot.
- Average deposit and investment size by corridor and customer segment.
- Customer-acquisition cost compared with ordinary RDA and NPC distribution.
- Time from local UAE USD receipt to confirmed RDA credit, from RDA credit to confirmed digital balance, and from investment instruction to confirmed position.
- Redemption and early-encashment time.
- Reinvestment and retention rates.
- Unmatched or misallocated funding events, reconciliation mismatches, failed events, retries, reversals and compliance holds.
- Cost of wallet, blockchain, custody, banking integration and support infrastructure.
- How quickly an authorized reviewer can trace a digital unit from funding through investment and redemption.

If the new interface does not materially improve distribution or attract incremental capital, the architecture should be simplified. A successful blockchain pilot that does not improve the economic outcome is not a successful policy pilot.

15. Why this may be useful

RDA is already a meaningful platform rather than a theoretical program. SBP's July 2026 statistics report 956,790 accounts and cumulative funds received of approximately USD 13.647 billion. Of that amount,

approximately USD 8.603 billion had been utilized locally and USD 2.118 billion repatriated, leaving a net repatriable liability of approximately USD 2.926 billion.

That scale changes the nature of the proposal. Pakistan is not being asked to trust an entirely new investment system. It is being asked whether a new interface can expand the addressable market of an existing one.

- Eligible investors gain a digital-native path into regulated Pakistani products without needing to manage cryptographic keys themselves.
- Participating banks retain custody, account controls and the existing relationship with the underlying financial products.
- Pakistan can test whether attractive regulated USD returns reach new pools of diaspora and digital-native capital when presented through a familiar interface.
- Regulators receive a system designed around traceable backing events, reconciliation and read-only supervision rather than a public token launched first and explained later.
- The architecture creates reusable capability for tokenized capital-market distribution without requiring Pakistan to commit today to a public circulating stablecoin.

16. Questions the pilot should answer with regulators

1. What exact legal claim does one digital USD unit represent?
2. Must each investor hold the underlying position directly through an individual RDA, or may an approved pooled or omnibus structure be used?
3. What assets count as recognized backing before investment, during an NPC position, at maturity and during early encashment?
4. Which entity is legally the token issuer, and which entity is legally responsible for USD redemption?
5. How should the digital unit be classified under the Virtual Assets Act and PVARA framework?
6. What PVARA license, NOC or sandbox authorization is required for token issuance, managed wallets, custody and the investment interface?
7. What SBP and Finance Division approvals are required to connect the digital interface to RDA and NPC subscriptions?
8. Can the platform display accrued or estimated earnings before the underlying profit is payable, and when may those earnings become additional digital units?
9. How exactly should current NPC premature-encashment rules be represented in the digital interface?
10. What customer information may appear on a public blockchain, and should individual balances be public at all?
11. What controls should govern minting keys, administrative actions, contract upgrades and emergency pauses?
12. What evidence should constitute final confirmation of a USD deposit, investment subscription, profit entitlement, encashment and USD payout?
13. What reconciliation frequency, tolerance and exception procedures should apply?
14. How should insolvency of the technology provider, bank, custodian or other participant affect customer rights and token redemption?
15. What disclosures should explain sovereign, banking, liquidity, technology and digital-asset risks without misrepresenting the product as equivalent to cash held at a foreign bank?
16. For a UAE-to-Pakistan USD pilot, which UAE-regulated entity may provide local collection or virtual-account infrastructure, and what safeguarding, client-money or account-structure requirements should apply?
17. Can the UAE collection partner settle multiple investor deposits to the Pakistani bank in one institutional USD transfer, and what signed manifest or customer-level data would SBP require to map each amount to the correct RDA?

18. What Pakistan-side bank event should constitute final USD credit and authorize token minting?
19. Should Phase 1 require one-to-one cross-border settlement from the UAE to Pakistan, or permit controlled batching once transaction-level traceability is proven?
20. Which eligible customer segments in the UAE should be included in the first pilot, and how should incremental capital be measured?

17. Strategic optionality

The first product should stand on its own. If it attracts incremental USD and operates safely, it has succeeded even if no broader token ever emerges.

Success would nevertheless leave Pakistan with new choices. The same operating capability could support tokenized access to other government or capital-market instruments. The local collection pattern could be replicated one corridor at a time in markets such as Saudi Arabia, the United Kingdom or the United States without changing the core Pakistan-side token and investment logic. It could also support institutional investors and provide a controlled laboratory for transferability, collateral or settlement rules. It could later connect with trade or remittance infrastructure if regulators see a clear economic case.

One future question may be whether a proven Pakistan-linked digital USD instrument should remain a closed investment representation or eventually become usable for a wider set of approved settlement purposes. That decision should be made after operating evidence exists. Phase 1 should not prejudge it.

Positioning

The strategic case is optionality, not inevitability. Pakistan does not need to decide today whether it wants a broadly circulating digital dollar instrument. It can first learn how to issue, back, restrict, reconcile and redeem a narrow regulated digital asset tied to financial products it already understands.

Conclusion

The proposal is not to replace Roshan Digital Accounts with crypto. It is to create a new controlled interface into the RDA ecosystem.

For the first pilot, an eligible investor funds USD through customer-specific instructions provided by a regulated UAE collection partner. The partner settles the USD to the participating Pakistani bank. A confirmed Pakistan-side RDA credit authorizes the matching digital balance. The investor can commit that balance to an approved investment such as a Naya Pakistan Certificate. The underlying banks and investment systems continue to perform the regulated financial work. The digital layer provides a managed wallet, restricted asset representation, programmable controls and a clear event history.

The design should be conservative about backing. Cash, investment positions, profit entitlements and redemption proceeds are different financial states. The system should know which state exists and should change digital supply only when the approved evidence and accounting rules justify it.

The measure of success is practical: can this interface bring meaningful incremental foreign currency into Pakistan from investors who would otherwise keep that capital abroad, while preserving clear custody, redemption, compliance and regulatory supervision?

If the answer is yes, Pakistan gains both capital and capability. If the answer is no, the digital layer can remain narrow or be removed. That is why the proposal is suitable for a controlled pilot rather than a large irreversible policy commitment.

The core proposition

Keep the financial substance regulated. Modernize the interface. Let every digital unit have an explainable backing event. Measure whether new foreign capital actually arrives. Preserve the option to build more only after the first product proves itself.

Appendix A. A simple technical view

A conventional web stack is sufficient for most of the first implementation. The important part is how responsibilities, financial state and evidence are structured.

Component	Possible role
Customer application	Onboarding flow, funding instructions, balance display, investment selection, disclosures and redemption requests.
UAE collection partner API	Provides customer-specific USD funding details, confirms local receipt, supplies unique funding references and settles USD to the participating Pakistani bank through the approved corridor arrangement.
PostgreSQL	Customer position ledger, event records, evidence metadata, product configuration, reconciliation state and exceptions.
Queue / job system	Webhook processing, retries, chain transaction submission, periodic reconciliation and long-running settlement workflows. Not the source of financial truth.
Pakistani bank / administrator API	Confirms final RDA credit and sends confirmed investment, profit, redemption and reversal events. Prefer authenticated transport plus message-level signatures for material events.
Signature verifier	Checks institution identity, public key, exact message signature, timestamp and unique event ID before accepting an event.
Rules engine	Determines whether the next action is allowed under the approved product and regulatory rules.
Managed-wallet provider	Creates controlled customer wallets and manages signing under an approved custody model.
Token contract	Implements restricted mint, burn, lock, unlock, pause and role controls on the approved blockchain if an on-chain token is used.
Blockchain observer	Confirms token transactions and finality, then links them to the platform event record.
Reconciliation service	Compares regulated assets, customer positions and digital supply. Opens an exception rather than auto-correcting unexplained differences.
Regulator dashboard / API	Read-only view of backing, supply, positions, evidence, exceptions and reconciliation status at the level approved for supervision.

Example event-processing logic

```

receive signed_event
  -> verify institution identity and active public key
  -> verify digital signature over the exact message
  -> verify timestamp and unique event ID

```

- > reject duplicate or replayed event
- > store original event + signature + verification result
- > append event to customer / position timeline
- > evaluate regulator-approved rule
- > if rule is satisfied, authorize the matching token or investment action
- > otherwise wait or route to exception review

Appendix B. Selected current references

Current public sources and discussion material used to validate the regulatory, product and market context in this paper.

- State Bank of Pakistan, Roshan Digital Accounts. Current eligibility, foreign-currency account, repatriation and investment-access material.
- State Bank of Pakistan, Roshan Digital Account - Key Statistics. July 2026 position reports 956,790 accounts, USD 13.647 billion cumulative funds received, USD 2.118 billion repatriated, USD 8.603 billion utilized locally and USD 2.926 billion net repatriable liability.
- State Bank of Pakistan, Naya Pakistan Certificate. Current product information on eligible RDA accounts, currencies, tenors, electronic subscription and premature encashment.
- State Bank of Pakistan, FD Circular Letter No. 04 of 2026, 1 July 2026. Current conventional NPC minimum investment and gross annual return schedule, including USD rates of 6.75 percent to 7.75 percent across listed tenors.
- State Bank of Pakistan, FD Circular No. 03 of 2020 and subsequent NPC instructions. Includes premature-encashment treatment and related operating rules, subject to later amendments.
- Pakistan Virtual Assets Regulatory Authority, Advisory on Virtual Asset-Related Announcements and Activities, 26 April 2026. States that issuance, transfer, custody, exchange or arrangement of virtual assets, stablecoins and allied blockchain-based solutions fall within PVARA's regulatory ambit and relevant pilots require prior authorization.
- Pakistan Virtual Assets Regulatory Authority, current licensing and sandbox pages. Includes licensing requirements for token issuers, custodians, wallet operators and investment platforms and current sandbox intake for asset-referenced token issuance.
- Bank of Punjab, Low Cost Remittance Corridors for South Asia, 2026 presentation. Discusses RDA expansion, stablecoin and multi-rail infrastructure, digital settlement, freelancer RDA corridors and regulated payout rails. Used as sector context, not as regulatory authority.

Sources checked 16 August 2026. Product rates, eligibility and regulatory requirements can change and should be revalidated before any external circulation or pilot launch.