HaRBInger 2025 - Reserve Bank of India's Fourth Global Hackathon

Introductions

A hackathon is an event organised to bring together people and entities for the development of innovative solutions for the existing challenges in specified areas through identified problem statements. The problem statements are worked upon by the participants who include, but not limited to, individuals, teams, entities from the hardware/ software and coding community during the limited time-period of the hackathon. In this competitive event, the participants submit ideas, create solutions, exhibit the prototypes, and the solutions are judged by an independent panel to arrive at the winner/s of the hackathon. The solutions thus achieved are primarily technology-driven innovative solutions which are feasible for implementation.

About HaRBInger 2025

The financial landscape is undergoing a transformative shift, driven by the convergence of fintech innovations and the rapid adoption of emerging technologies. This shift is reshaping traditional banking models, placing emphasis on secure, inclusive and identity-driven solutions. From customer onboarding to grievance redressal, financial services are evolving to become not only more efficient and personalised but also more transparent and trustworthy.

HaRBInger 2025 is centred around the theme **"Secure Banking: Powered by Identity, Integrity, and Inclusivity"**. The objective of this hackathon is to leverage emerging technologies to build innovative, secure, and user-centric financial solutions that protect customer identity, foster trust, enhance customer safety, improve system-wide efficiency and promote financial inclusion. Participants are encouraged to develop solutions that enhance customer safety and experience, simplify complex banking processes, and bridge access gaps, thus ensuring that the future of banking is not only connected and convenient, but also secure and equitable for all. Participants are invited to ideate, prototype, and build creative technology-driven solutions to address three critical areas of the financial landscape.

Problem Statements:

HaRBInger 2025 invites innovative ideas for the problem statements as detailed below:

Problem Statement 1: Tokenised KYC

In today's rapidly evolving digital financial ecosystem, ensuring a seamless, secure and user-centric Know Your Customer (KYC) experience is critical for fostering financial inclusion, trust, maintaining integrity and meeting customer expectations. The current KYC processes (onboarding and periodic updation) can be further refined to make them more frictionless and accessible, while addressing integrity and threats like identity fraud.

Tokenised KYC presents a transformative opportunity to reimagine identity management that could be easily shared with financial institutions and instantly verified. By enabling users to securely store, control, and share their verified identity as reusable digital tokens, it can reduce duplication, safeguard sensitive information, promote privacy, ensure compliance and streamline delivery of financial services. Tokenised KYC models ensure that once a user's identity is verified, it can be securely reused across financial service providers via consent-driven mechanisms. This problem statement invites participants to design and develop a tokenised KYC model and focus on the following features:

a. Creating token-based user-held KYC models where credentials are digitally signed by trusted issuers and shared securely across institutions.
b. The digital identity tokens should be tamper-proof, machine-readable and issued by trusted authorities and reusable across multiple onboarding processes.
c. Users should have full control over their KYC data. Sharing of data must be explicitly consent-driven and auditable.
d. Identity credentials should be tamper-resistant, traceable and support selective disclosure of information based on the requirement.
e. Cross-platform and inter-institutional interoperability using open standards, standardised APIs, and common data exchange protocols.
f. Adhere to applicable privacy guidelines.
g. Real-time KYC revocation, renewal, and audit tracking mechanisms for improved lifecycle management.

h. Integrate with/ make it interoperable with existing infrastructure such as Aadhaar, DigiLocker, and the Central KYC Registry (CKYCR), and work across institutions via common standard APIs.
i. Secure delegation of tokenised KYC access to legal heirs, guardians, or nominees when required.
j. Address updation, periodic KYC updation and how the KYC platform can be leveraged by other sectors such as insurance, mutual funds.

The solutions may leverage emerging technologies such as blockchain, zero-knowledge proofs (ZKPs), smart contracts, and biometric authentication to enable trust, reduce fraud, and improve operational efficiency. Tokenised KYC has the potential to revolutionise digital identity and customer onboarding in India. The objective is to build a scalable, standards-driven identity verification framework that enhances collaboration between institutions, reduces redundancy, and empowers users with greater control over their digital identity. By placing users at the centre and ensuring regulatory alignment, tokenised KYC can reshape India's digital identity landscape and accelerate secure and convenient financial access at scale.

Problem statement 2: Offline CBDC (e₹)

Digital Rupee is envisaged as a digital form of physical cash. The offline functionality forms one of the foundational considerations for the design of e₹. In addition to ensuring widespread usage, offline transactions would be beneficial in remote locations and would offer resiliency in places where mobile network is not available. Participants are invited to design a secure, user-friendly, tamper-resistant, and scalable solution for enabling offline Central Bank Digital Currency (CBDC) transactions. The solution should allow retail CBDC transactions without requiring real-time internet or telecom connectivity, ensuring double-spend prevention and reliability in low-resource environments. The goal is to build a functional offline CBDC solution that allows individuals and merchants to transact CBDCs without internet or mobile network. The solution should:

a. Prevent double-spending without requiring real-time server validation.
b. Allow for consecutive offline payments i.e, funds received in offline mode shall be spendable in offline mode also.

c. Work on low-cost devices i.e., not necessarily rely only on NFC/ mobile secure element. Solution should be agnostic to all types of devices/OEM and communication protocols and can be enabled on different form factor.
d. Shall be interoperable across OEM hardware and software across all form factors, wallets and on various available acceptance devices in India.
e. Enable secure P2P authentication and transaction integrity, including mutual authentication between sender and receiver.
f. Maintain auditability for regulatory compliance and customer dispute resolution/ grievance redressal (while preserving privacy).
g. Incorporate all the dependencies for e.g., permission/ partnership with OEMs/ chipmakers, if required.
h. Include an approach plan for implementation at scale across India, including an estimate of the costs and timelines.
i. Provide the reconciliation framework for such transactions at the system, individual/ merchant, and bank level.
j. Be modular i.e., the offline elements can be easily integrated within the existing CBDC system/ architecture without/ with minimal system-level changes.
k. Should be largely based on open-source software and be willing to share the source code in case the solution is selected for implementation.
l. Revocation mechanisms in the event of lost/stolen devices.
m. Secure and tamper-proof method for device binding during registration.
n. Offer multi-protocol support for the solution (NFC, Bluetooth, sound, etc.)
o. Provide high level of security to ensure that the payment credentials should not be accessible by any malicious actor on device, reference of same need to be shared as a proof.
p. Ensure high level of device integrity, data integrity and risk protection, reference of same need to be shared as a proof.
q. Provide random fingerprint technique to determine tampered device and provide technique to do device-based blacklisting and
r. Suggested solution features should be managed and owned by the solution provider only and must not include any third-party solution.

Problem Statement 3: Enhancing trust

As the financial ecosystem becomes increasingly digital, use of technology serves both as a driver of innovation in transforming financial services and a critical line of defence against emerging risks. Customers are now exposed to a growing array of cyber threats, including phishing, identity theft, data breaches, and unauthorised transactions. Financial institutions also face the challenge of keeping the system safe and avoid fraudulent activities. This necessitates the need to implement technology-driven solutions that can effectively enhance customer safety without compromising convenience, privacy, or financial inclusion. The key challenges for financial institutions include:

- **Identity fraud and impersonation** - Using deepfakes, fraudsters mimic faces, voices, or even live video calls, making traditional verification systems vulnerable and inadequate. Other threats include biometric spoofing and executive/ c-suite impersonation.
- **Fake banking and digital lending apps** – There are instances of fake banking and digital lending apps that trick users into revealing sensitive information, steal funds, or coerce vulnerable customers into predatory debt traps. These incidents significantly erode trust in digital financial services.
- **Customer grievance redressal** - There is tremendous potential to use technology to automate, streamline, and improve the complaint resolution journey. Also, special attention is needed to improve accessibility for vulnerable groups such as senior citizens, people with disabilities (Divyang), and those with limited digital literacy, using appropriate technology.

Participants are invited to design innovative, technology-based solutions that enhance customer safety, strengthen digital financial infrastructure, improve user experience, and enhance systemic security. Solution may address any or all of the following areas:

a. Develop systems that can detect impersonation attempts using deepfakes in videos/ images, voice manipulation, or forged identities. It should also flag tampered documents during customer onboarding and detect c-suite impersonation frauds.
b. Design and develop a solution that identifies and blocks unauthorised banking/ digital lending apps before they defraud customers. It should be capable of generating real-time alerts to enable swift and proactive response to fraud

attempts. It should be designed to preserve customer privacy while strengthening detection capabilities. It may also include features that allow customers to verify the authenticity of apps before installation, thereby reducing the risk of falling victim to unauthorised applications.

c. Design and develop an intelligent and inclusive technology-driven grievance redressal system. It should automate processes and reduce turnaround time across various stages of complaint handling and empower regulated entities with data-driven intelligence to resolve complaints. It should automatically categorise, prioritise, and route complaints to the appropriate channels. It should detect recurring issues and automate standardised responses where applicable.

Participant or team may submit maximum up to three distinct solutions, one each for the challenges related to impersonation fraud, fake apps, and grievance redressal. Each solution should be clearly aligned to the specific challenge it addresses and must demonstrate the use of technology to enhance customer safety and improve system-wide efficiency. Best solution(s) across these sub-themes would be considered for rewards.

Who Can Apply?

All entities, teams or individuals (eighteen years and above) who are eligible to enter into a contractual agreement are eligible to apply. Further, the product/ solution should have an element of innovation or novel application of technology serving the common good. Participants from all backgrounds and geographies are welcome, albeit knowledge about the Indian financial services market and consumers is preferred. Employees of the Reserve Bank of India (RBI) and its subsidiary institutions are not eligible to participate.

How to Apply?

HaRBInger 2025 is owned and operationalised by RBI and is hosted on the Application Programming Interface Exchange (APIX) platform. A participant may click on the following link to register for the hackathon and submit the proposal after the registration:

https://app.apixplatform.com/h1/harbinger2025

Applications will be received only through the given link. Once registered, select the problem statement, and submit your proposal on the platform. Please fill in the responses for all the proposal questions.

You may apply for more than one problem statement if you fulfil all the criteria set out in each category. Your solution can aim to address the needs covered by more than one problem statement. We are looking at the uniqueness and innovation of the proposition as well as the feasibility of the business model to achieve the desired goal.

HaRBInger 2025 shall run in three phases with Screening of entries (Phase I), Shortlisting of entries for Solution Development (Phase II), and Final evaluation and selection of winners/ runner-ups (Phase III). In Phase I, screening of the most promising solutions will be done. The selected entities will have to present their proposal before an independent panel of judges in phase II. The shortlisted entities will work on developing a working model or prototype solution during the solution development stage. During the final evaluation in Phase III, the solutions will be evaluated by an independent jury to decide the winners/ runner-ups. The winners/ runner-ups will be selected based on certain evaluation criteria, which, inter alia, include understanding of the problem statement, innovation, solution comprehensiveness, ease of implementation, demonstration/user experience, feasibility, scalability and compliance etc.

Important Dates:

Stage	Start Date	End Date
Registration & submission of the proposal	October 23, 2025	November 23, 2025

Other details:

- Each of the three problem statements will have one winner and one runner-up.
- Winners will get prize money of ₹ 40 lakh. Runner-ups will get prize money of ₹ 20 lakh.
- Special prize of ₹ 20 lakh to the best ‘all woman team’ (a team comprising of only woman members’), across all the three problem statements.
- Stipend of ₹ 5 lakh to teams shortlisted for solution development for meeting the cost of development of prototype.

- The judges reserve the right to disqualify any entry that, in their sole opinion, violates the spirit of the Hackathon, the rules, or any applicable laws.
- The decision of the judges with respect to the selection of winners/ runner-ups and all other matters related to the HaRBInger will be final, binding, and non-negotiable.
- Participants are responsible for ensuring that their submissions do not infringe on any third-party intellectual property rights, including patents, copyright, trademark etc. and would have to provide an undertaking on the same. The RBI will not be responsible for any dispute or liabilities arising on account of such infringements.

Contact information:

- For HaRBInger 2025 related queries, please send mail to harbinger2025@rbi.org.in
- For technical queries during registration or proposal submission process, please reach out to support@apixplatform.com

****