



• • • • •  
• • • • •

# Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

• •  
• •  
• • • • • • • • • • • • • •  
• • • • • • • • • • • • • •



# About Us - Swinburne Blockchain Innovation Lab

**Our research has been supported by Australian Research Council (ARC), Data61, and various key industry partners.**

## Focus areas and capabilities

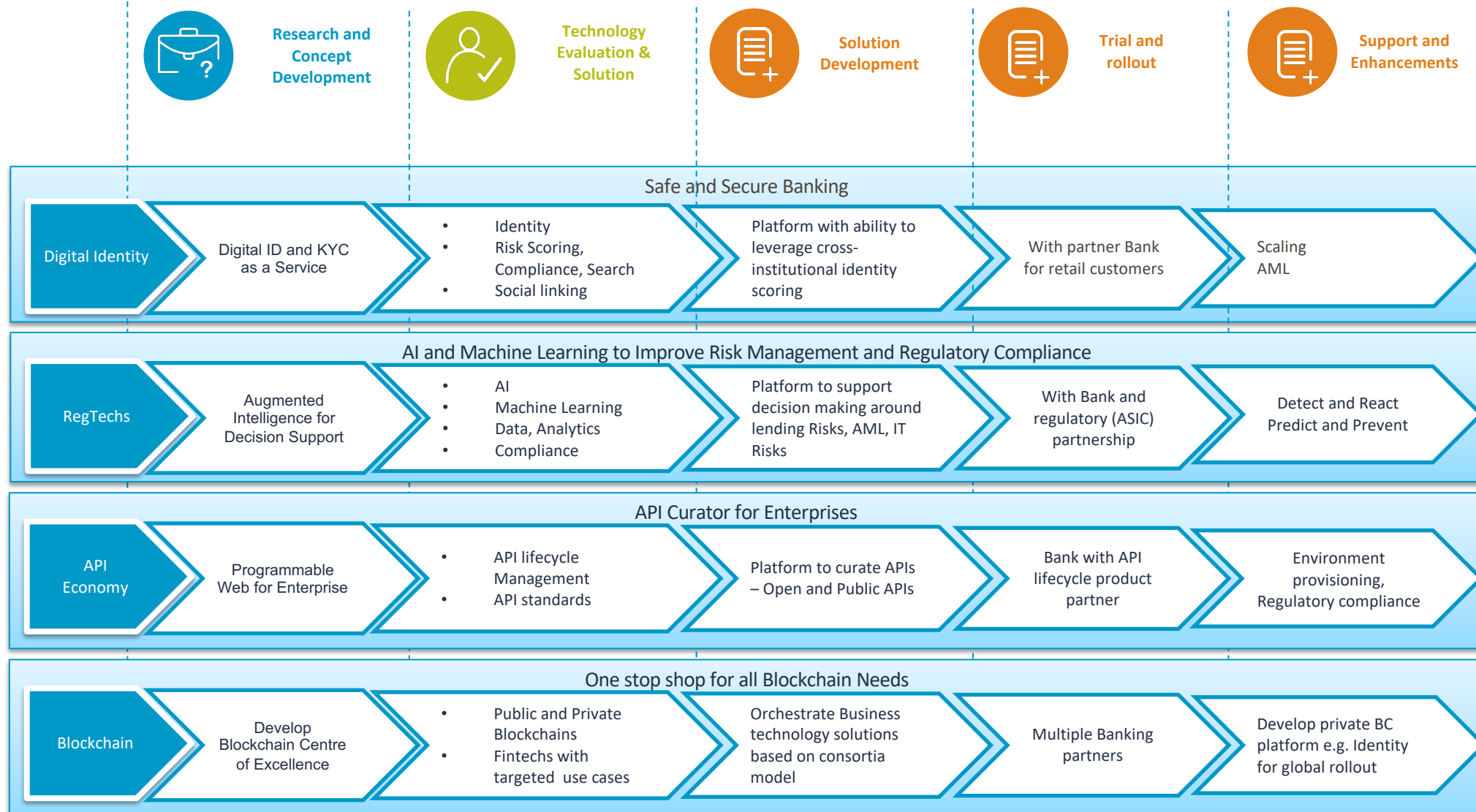
Our application and impact-driven research is focused on the development and evaluation of new generation blockchain systems in different application areas. Much of it is experimental and is focused on validating proposed new concepts by means of implementation and deployment in prototypes that are used in the real world.

Our capabilities:

- Blockchain architecture
- Performance and efficiency of blockchain
- Blockchain applications and proof-of-concept
- Smart contracts
- Security and privacy in blockchain

**Contact:** Prof. Yang Xiang, [yxiang@swin.edu.au](mailto:yxiang@swin.edu.au) and A/Prof. Vincent S. Wen [swen@swin.edu.au](mailto:swen@swin.edu.au) .

# From Research to Commercial deployments at Scale



# Building Trust with Distributed Ledgers for Digital Platforms

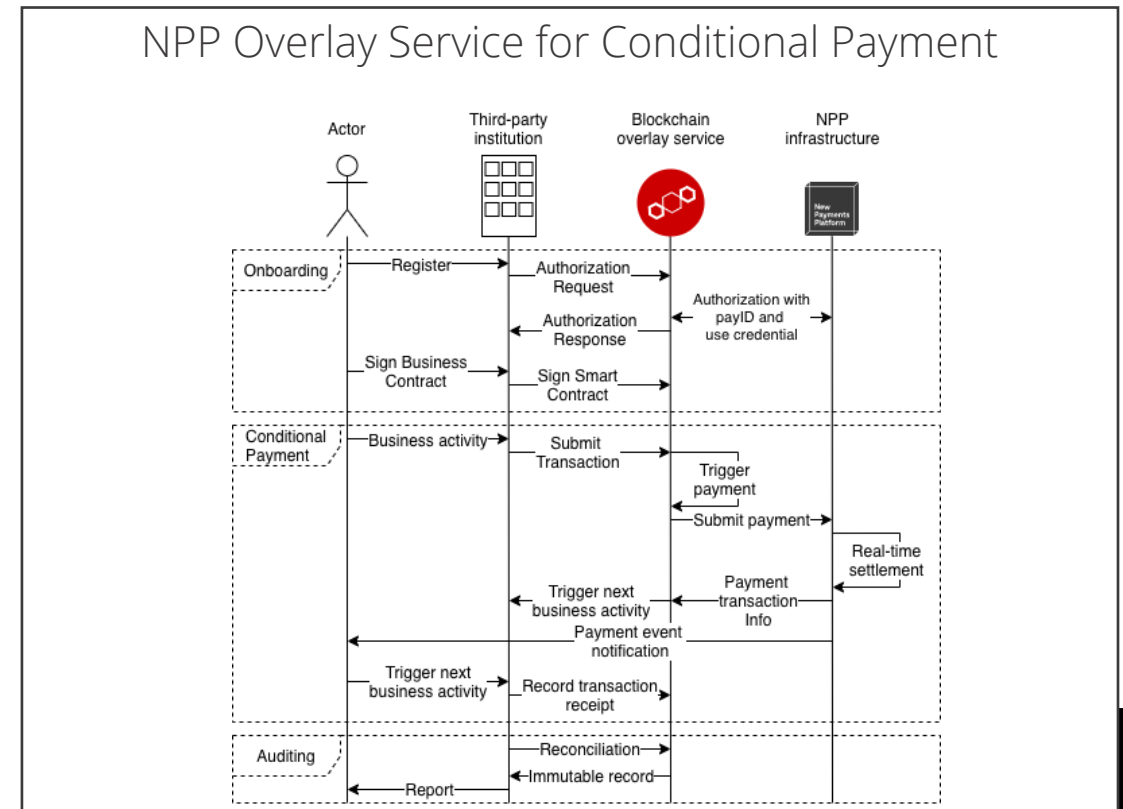
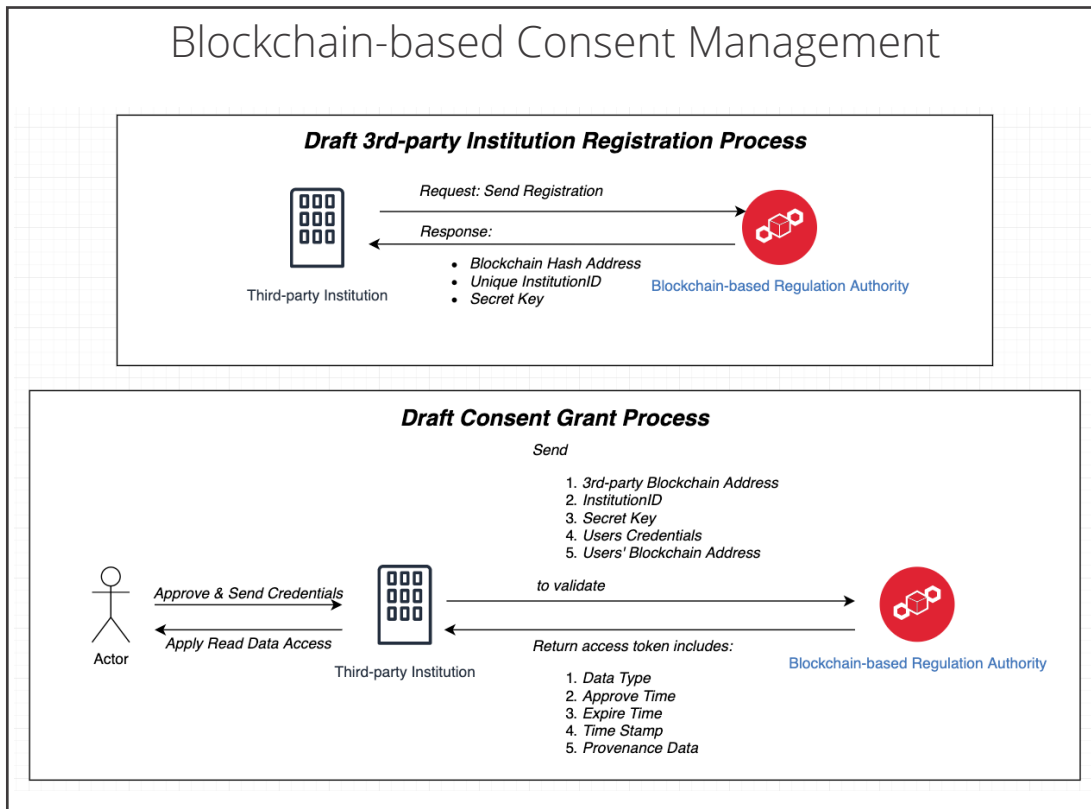


Provide framework and guidance for the application of building trusted consumer consent in open banking and other sectors.

Explore technical feasibility, risks, and potential benefits of using a blockchain-based extension of New Payments Platform (NPP) to allow smart contracts to decide on conditional payments, where those smart contracts can also use Consumer Data Rights (CDR) authorisations to access data through CDR APIs.

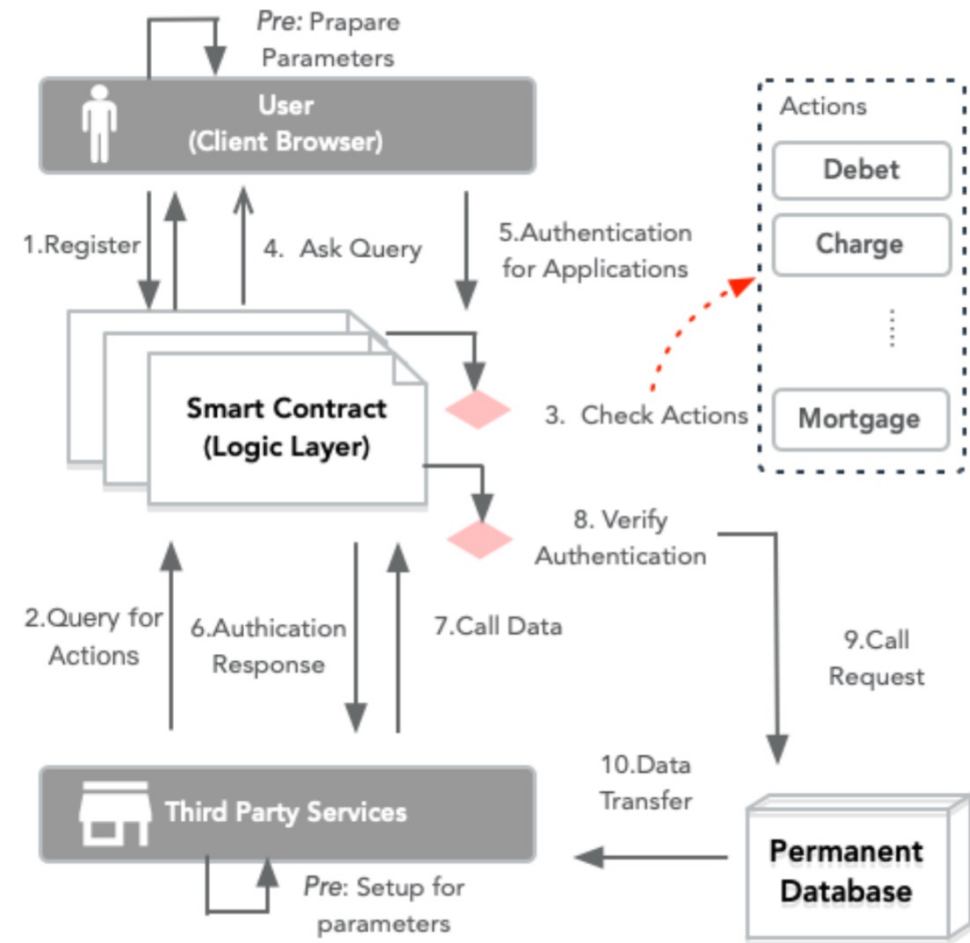
Centralized approaches suffer from lack of transparency on data access and use, data breaches (e.g., Facebook-Cambridge Analytica incident), and inefficient business processes. We design and develop blockchain-based solutions for:

- Consent management for data sharing
- NPP overlay service for conditional payment



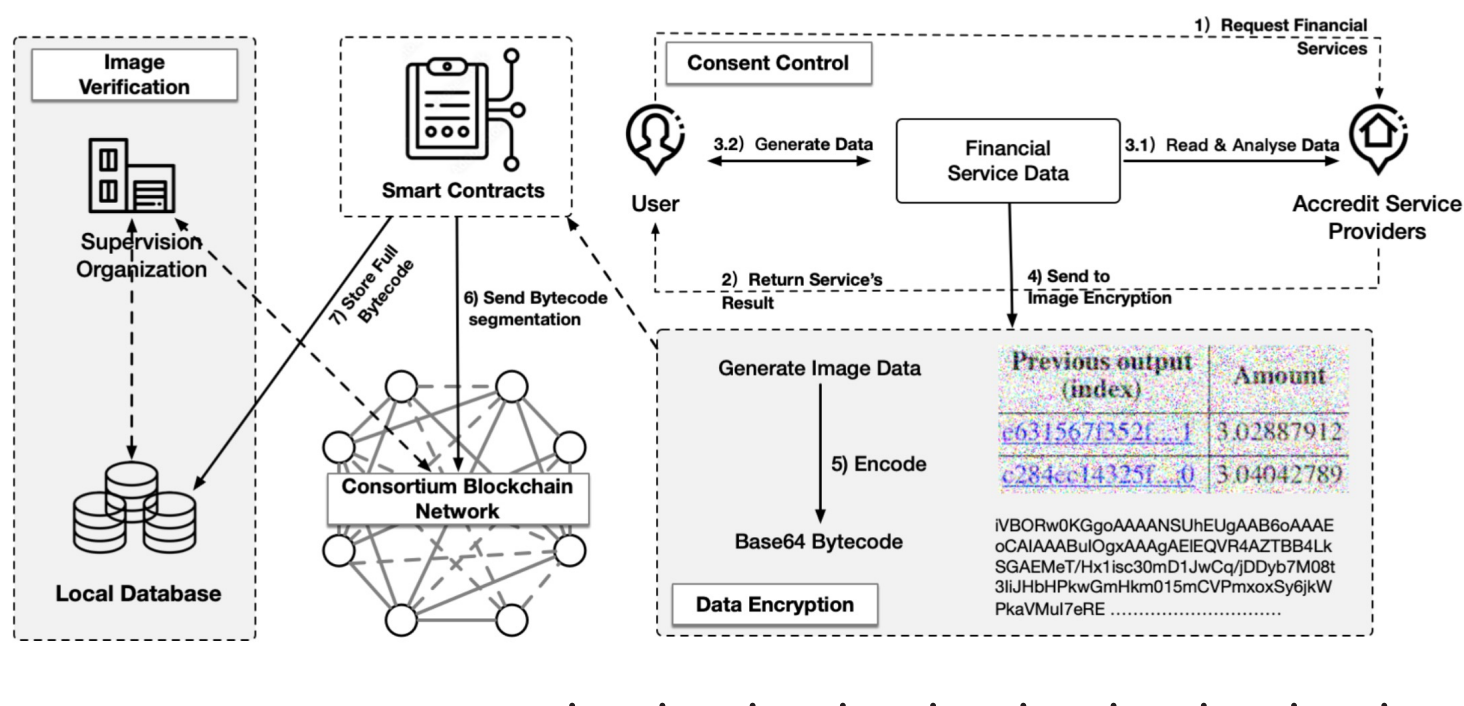
# PPM: A Provenance-Provided Data Sharing Model for Open Banking via Blockchain

- ❑ The authentication of our model is transparent and public on a distributed ledger. The transparency means users and third-party services can freely obtain the records
- ❑ The customized access control enables users to control and share personal data with other parties with their willingness. The public key encryption system protects the authentication of actions' control with the users' identities.
- ❑ The authentication is publicly recorded on the chain, where both user and the third party can get the whole history of their actions. Whenever the powerful authority does evil, the activity will be traced with accountability.



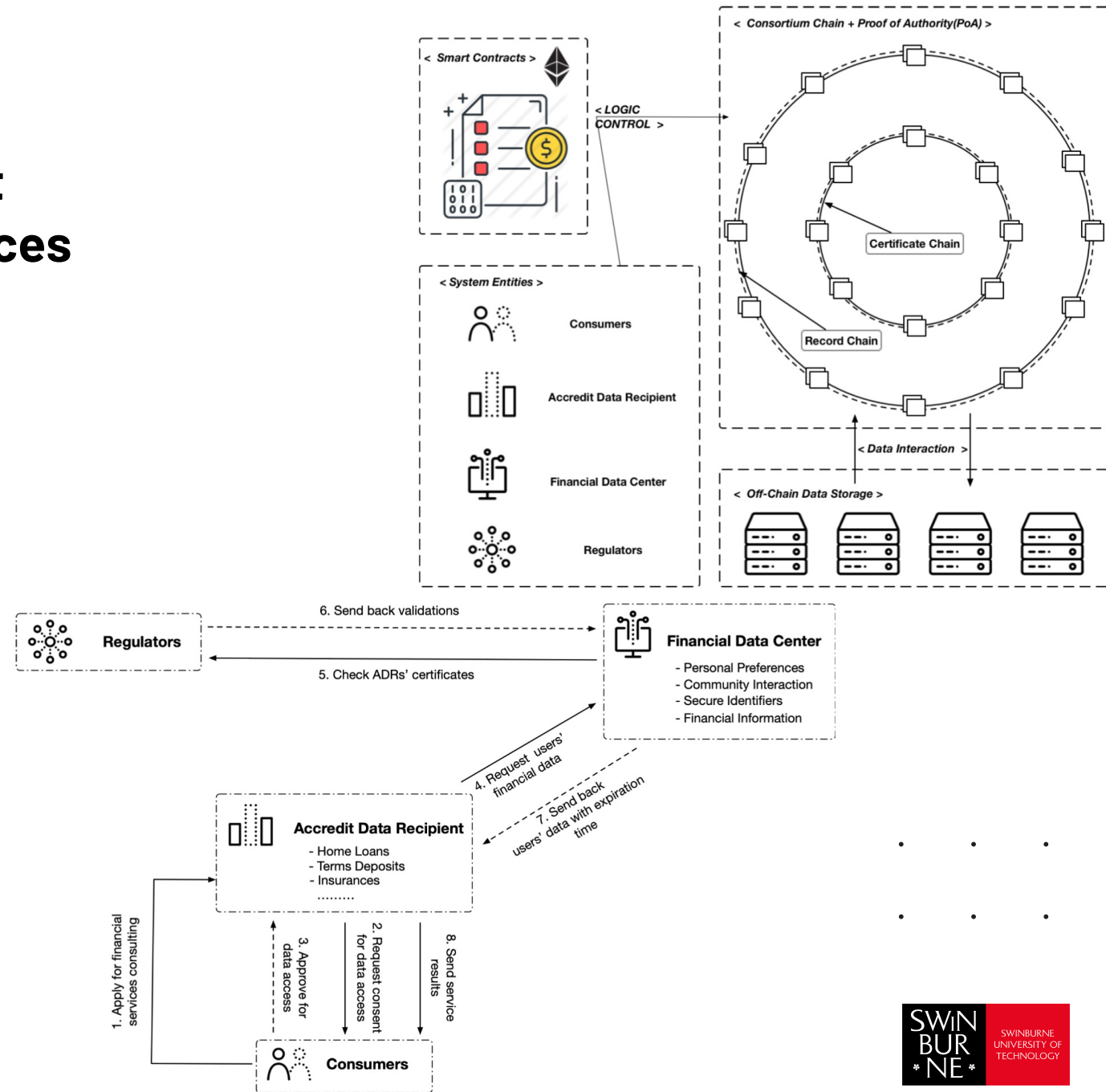
# An Image-based Privacy-preserving Blockchain Model for Financial Services

- ❑ With image-based encryption, numerical data are present as images, protecting user privacy and providing transparent records. Users can read all numerical data as in the image way.
- ❑ We treat the CAPTCHA algorithm as a microservice. When new records are generated, the algorithm will convert data into images first. Then images would transfer to bytecode and push on the blockchain.
- ❑ Our system adopts image encryption to enhance user privacy and reduce the risk of managing keys.



# An Automated Consent Management Model for Blockchain Financial Services Platform

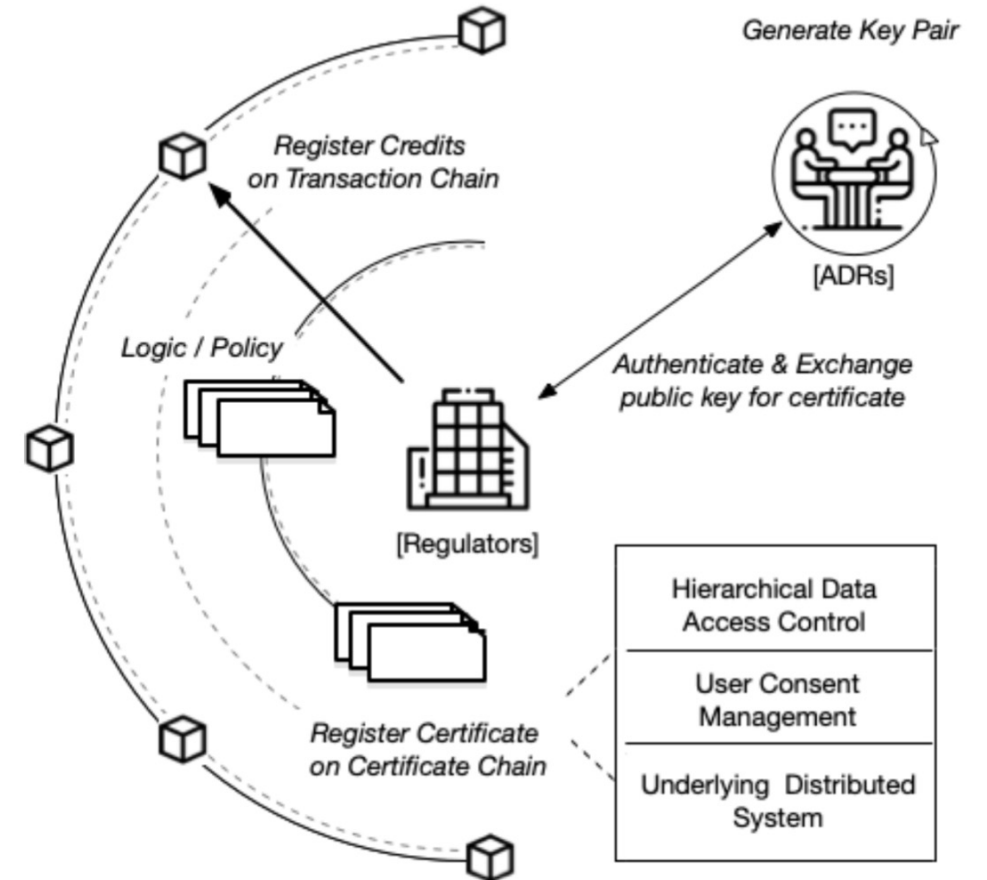
- ❑ A novel consent management workflow, and the user, regulators, and ADRs jointly and automatically manage the data sharing. Data sharing between different parties need to verify certificates and request are controlled by smart contracts around different parties.
- ❑ Due to the ADRs being responsible for providing various financial services, we record ADRs' registration data on the public ledger. Participants can examine and ensure the validity of companies' identities before granting them to provide services.





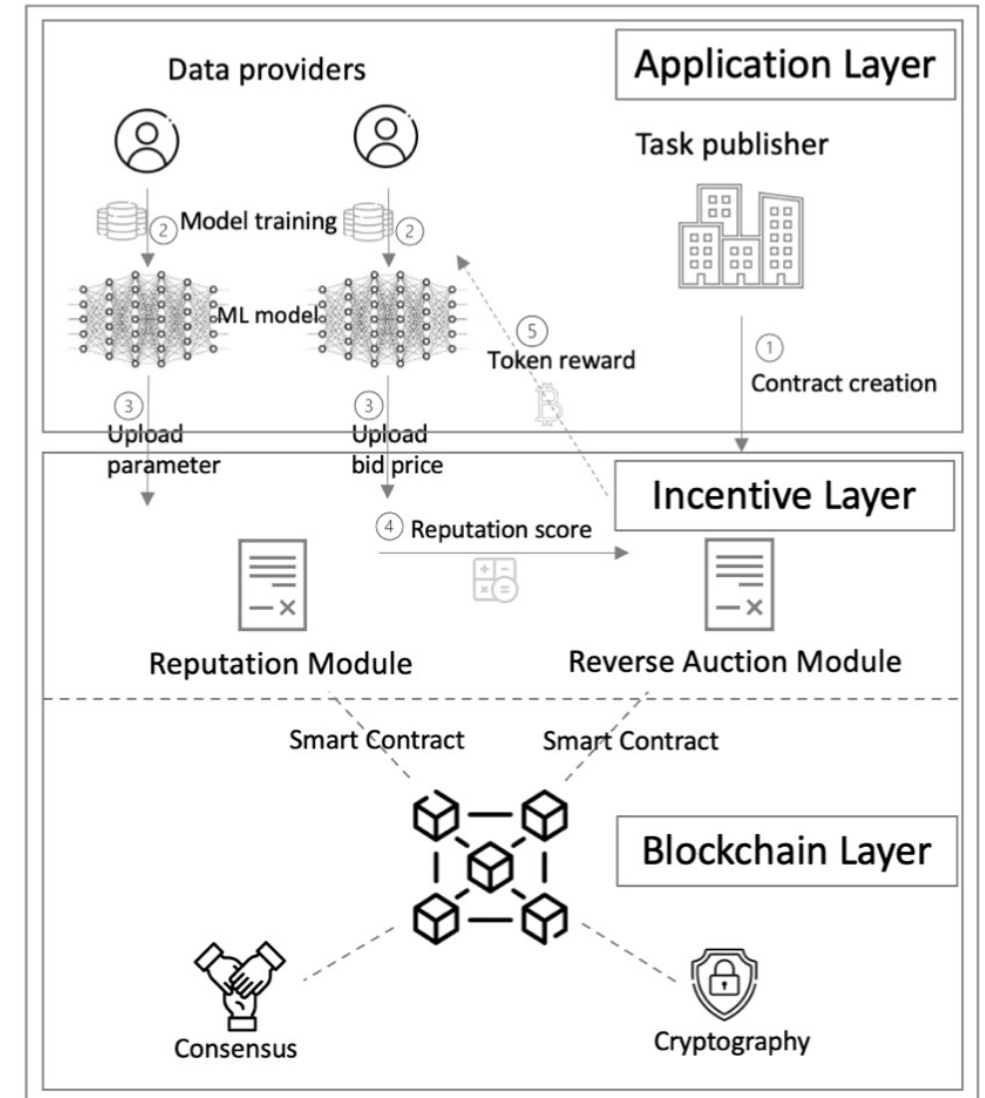
# BHDA - A Blockchain-Based Hierarchical Data Access Model for Financial Services

- ❑ Based on consortium blockchain, the system's proposed model needs to register on the blockchain to record their certificate data.
- ❑ The hierarchical data access control is based on transactions completed by ADRs. As more and more blocks are created along the transaction chain, the ADR's score is dynamically updated.
- ❑ In order to improve the approval efficiency between different parties, we write logic into smart contracts for automated management.



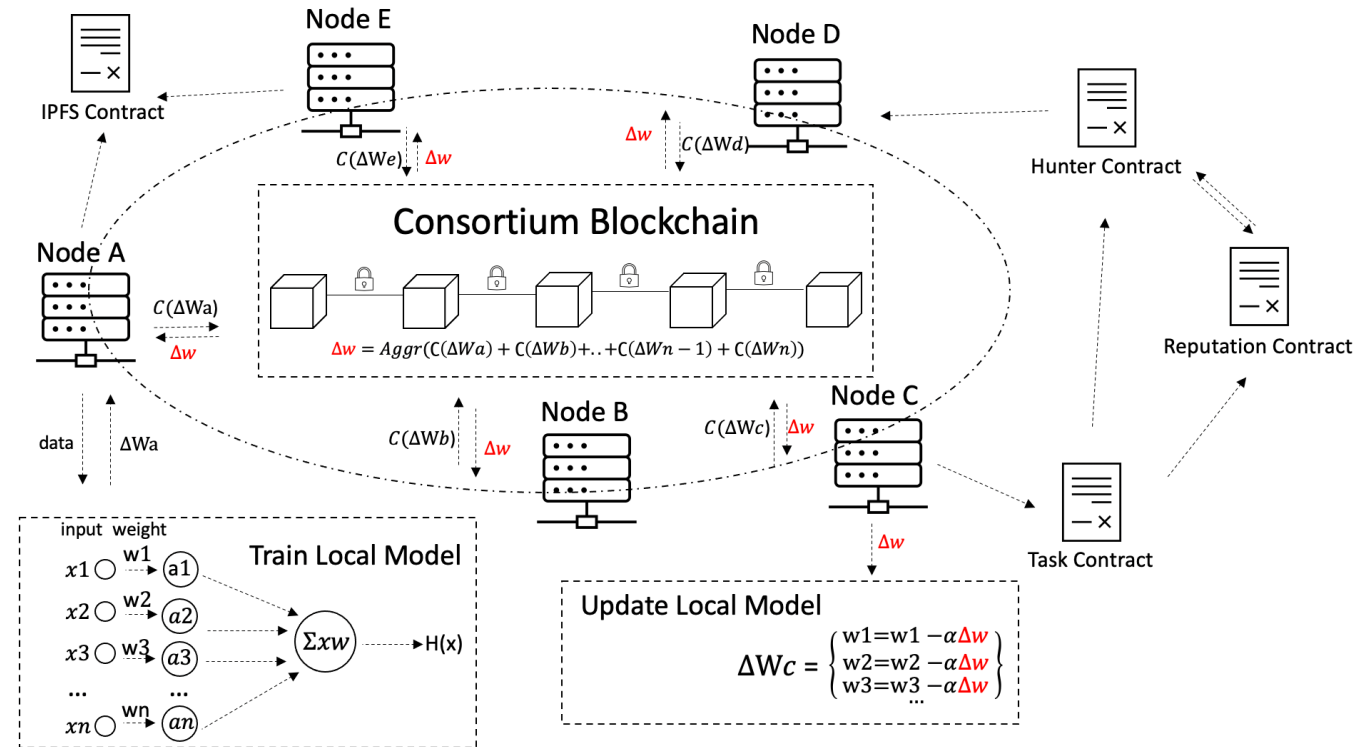
# A Hybrid Incentive Mechanism for Decentralized Federated Learning

- ❑ A dynamical participant reputation scheme consisting of parameter quality evaluation and bid price trust value calculation.
- ❑ A smart contract-based reverse auction approach to stimulate data owners to participate in FL model training while minimizing monetary incentive costs.
- ❑ Experiments on the proposed mechanism and perform quantitative model analysis in terms of the effectiveness against three typical threats and the utility of smart contracts.



# A Blockchain-enabled Federated Learning Model for Privacy Preservation: System Design

- ❑ A novel Homomorphic-integrated and blockchain-based FL model is proposed for data sharing, in which privacy can be effectively protected.
- ❑ A smart-contract-based reputation scheme and an on/off-chain storage strategy are introduced respectively, to solve the trust issue and large-gradients storage problem.
- ❑ Experiments are conducted to evaluate the practicability and effectiveness of the proposed model in terms of model accuracy, time cost, and smart contract testing.

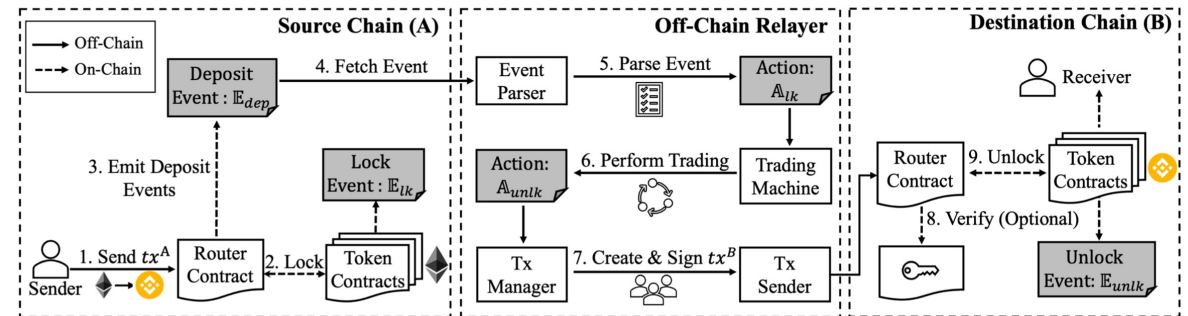




# Ethereum Foundation Project S-CCSC: Security of Cross-chain Smart Contract

## Cross-chain Smart Contract (CCSC)

- ❑ Cross-chain smart contracts are decentralized applications that consist of separate smart contracts on different blockchain networks that intercommunicate to create a single unified application.
- ❑ Different smart contracts on different chains perform different tasks yet all stay in sync and work towards supporting a single use case.



## Why secure CCSC?

- ❑ **Blockchain bridges** have so far largely focused on the transfer of tokens between networks.
- ❑ Cross-chain smart contracts require more **generalized bridges** to support the transfer of arbitrary data packets, tokens, and commands.
- ❑ Lots of **attacks** happened on blockchain bridges.



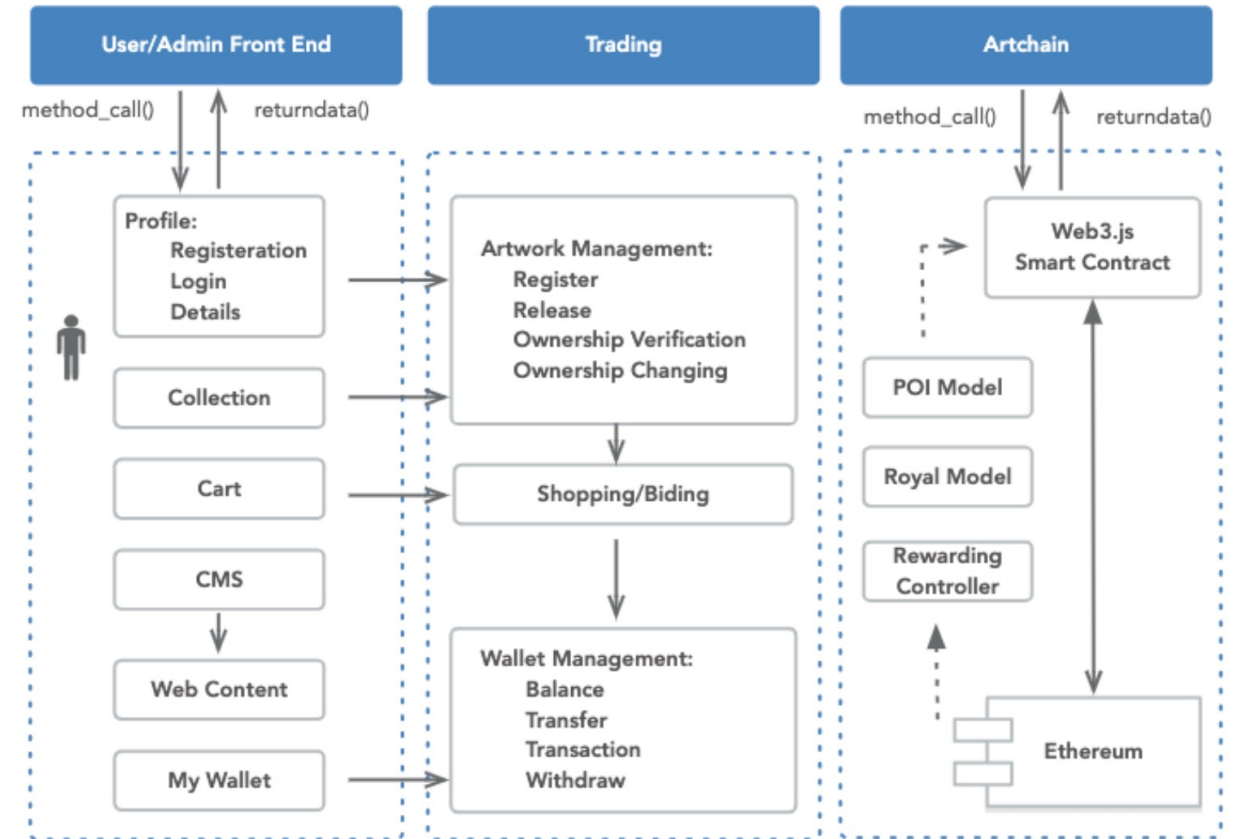
## BACKGROUND & UNDERSTANDING

---

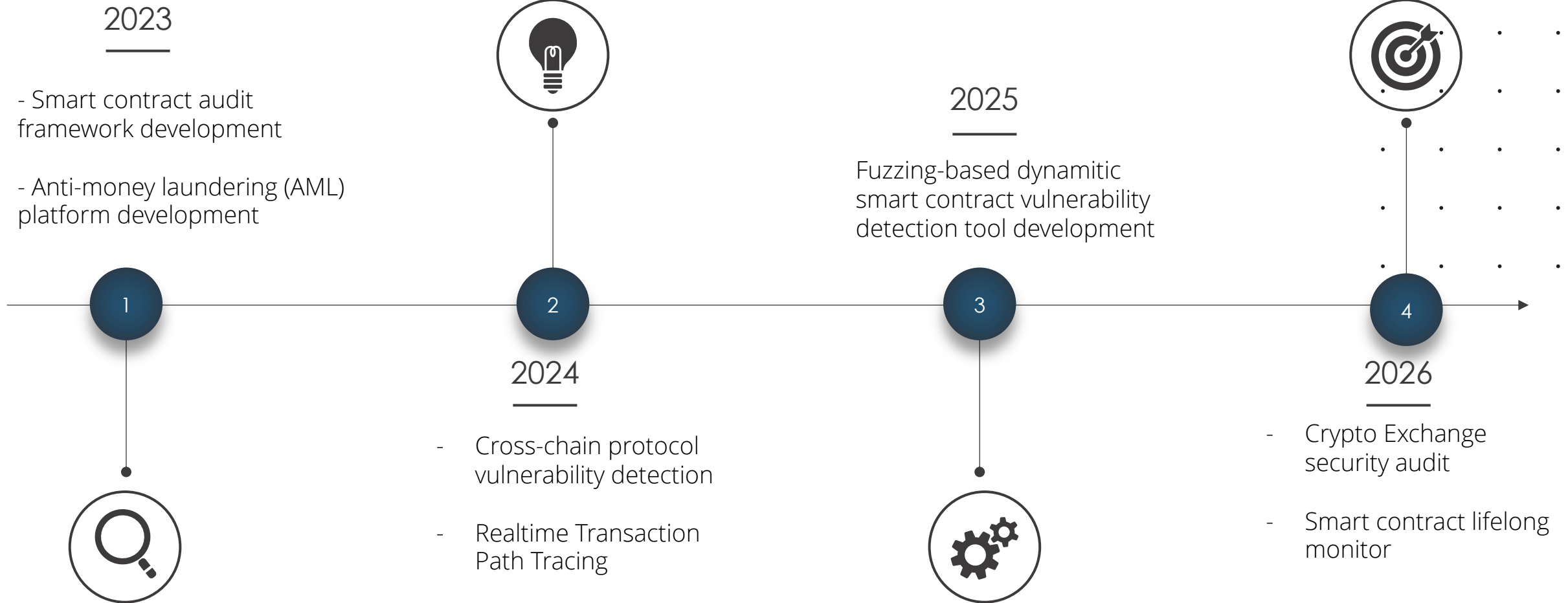
*ArtChain Global intends to establish an art trading/exchange platform using the ACG blockchain through a modern, user-friendly website in line with current design trends and functionality. This will create a unique and extraordinary experience for the different users.*

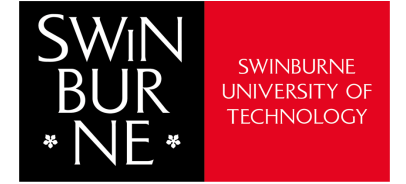
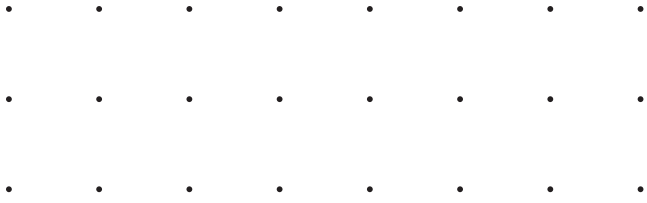
# ArtChain: Blockchain-enabled Platform for Art Marketplace

- ❑ Shared ledger along with permissioned control ensures the transparency of each transaction which guarantees the privacy protection in art trading and provenance.
- ❑ Real-time tracking of individual artworks combined with the blockchain ledger assists in the fight against counterfeit artworks
- ❑ The on-chain registration of collectors offline assets provides an immutable digital record of the artwork, which guarantees the true ownership, the provenance and the value of the artwork
- ❑ Publicly displaying artworks to a wider range of professional investors, leveraging the openness of art ecosystem.



# Future Work





Thank You

