



► Project Aurum Phase 2

Privacy-enhancing technologies for digital cash

October 2026



HONG KONG MONETARY AUTHORITY
香港金融管理局

© Bank for International Settlements 2026.

All rights reserved.

Limited extracts may be reproduced or translated provided the source is stated.

ISBN 978-92-9259-986-7

Executive summary

A. Objectives of Project Aurum Phase 2

Improve privacy and confidence for digital cash

For digital cash to be widely accepted, people may require assurances that at least some of their spending is not tracked. At the same time, authorities must still be able to prevent crime, protect consumers and intervene when the law requires it.

Project Aurum Phase 2 looks at whether these two goals can be met in one design, rather than being treated as an either-or choice. Indeed, the project explores how digital cash could offer everyday privacy similar to physical cash, while still supporting public policy objectives such as anti-money laundering (AML), countering the financing of terrorism (CFT), fraud prevention and financial stability.

It asks a simple question: *can people make routine payments without exposing unnecessary personal information, while authorities retain appropriate tools to manage risks?*

B. Policy context

The project explores the technical solutions to address the following policy questions:

How can central banks ensure privacy in digital cash systems without compromising compliance with AML/CFT regulations?

The Aurum Phase 2 design enables compliance through targeted and proportionate access. Indeed, in line with the current two-tier financial system, commercial banks obtain and retain account identity information. This information is not visible to central banks. Instead, the system includes mechanisms that allow verification, investigation and intervention only when legally required, in line with standing laws and regulations. While enabling privacy in line with existing statutes, this design supports core public policy goals such as combating money laundering, terrorism financing and fraud.

What role should central banks play in the design and governance of privacy-preserving digital cash systems?

A core central bank mandate is to maintain the robustness and integrity of the digital cash system. This, however, does not require central banks to have access to or keep payment details. Aurum Phase 2 starts from the standpoint that privacy should be technologically enforced rather than institutionally promised. This means that privacy should not rely on central banks saying, "we won't look", but rather be embedded through privacy-enhancing technologies (PETs), allowing personally identifiable information (PII) to be protected while enabling compliance with AML/CFT regulations.

How can privacy-enhancing technologies (PETs) support the dual goals of privacy and regulatory oversight?

The Aurum Phase 2 prototype combines different PETs, including encryption, the Boneh-Boyen-Shacham signature plus (BBS+) scheme, pseudonym-based ownership and zero-knowledge proofs (ZKPs). BBS+ signatures protect users' real identities from third parties while preserving verifiability for compliance purposes. ZKPs add a further layer of privacy-preserving payment integrity, allowing transactions to be validated without revealing sensitive payment details.

What trade-offs does combining different PETs in the design of digital cash create as compared to simply limiting access rights?

Stronger privacy through the use of PETs is not free of trade-offs. Additional privacy protections can slow transaction processing times or make the system harder to adapt for complex financial products. Wallets that maximise privacy may also be harder to recover if access is lost, much like losing physical cash. These are policy-relevant choices, not purely technical ones, illustrating strategic decisions and design trade-offs to be made by central banks during the design phase.

C. Main lessons

The project has the following lessons learned:

Exploratory prototype

For central banks, the policy relevance of Project Aurum Phase 2 lies in showing how privacy choices can be explored at the technology design stage of digital cash, rather than treated only as legal or operational safeguards after launch. While not a production-ready technology stack, the prototype demonstrates that digital cash can achieve cash-like privacy while meeting regulatory requirements. The prototype thereby explores ways for central banks to adopt privacy-focused designs.

A practical middle ground on privacy

Project Aurum Phase 2 builds on earlier work that was shared with the central banking community for learning purposes.¹ It illustrates a balanced approach between complete anonymity on the one hand and full transaction transparency on the other. Users would still join the system through regulated banks, which carry out identity checks and meet existing legal obligations. This preserves accountability at the system's edge and aligns with current financial regulation.

Once onboarded, however, ordinary payments would not automatically reveal a person's name, account number or spending history to everyone involved in processing the payment. Instead, through the use of PETs, payments can be validated and settled without exposing who paid whom, or how much, to parties that do not need that information. In other words, banks remain able to meet their obligations, but sensitive personal data is not routinely shared across the system.

1. The code of Phase 1 was shared with the central banking community on BIS Open Tech at www.bis.org/innovation/bis_open_tech.htm

Policy flexibility rather than one fixed model

A key feature is the flexibility of the prototype to adapt to different national policy environments. Indeed, privacy and control can be adjusted to reflect local policy choices. The prototype includes options such as:

- greater privacy for low-value, everyday transactions, similar to cash;
- stronger checks or traceability for higher-risk uses;
- configurable onboarding rules depending on legal requirements; and
- safeguards that protect consumers while still allowing recovery or intervention in defined cases.

These features allow different jurisdictions to calibrate the balance between privacy, inclusion, financial crime controls and consumer protection according to their own laws and risk appetite.

D. Key takeaways

Privacy and compliance can coexist. Privacy-enhancing approaches can help digital cash meet public expectations without undermining regulatory objectives.

Privacy is a design choice that can be reinforced through technology, institutional arrangements and regulatory safeguards. Together, these elements can provide stronger privacy assurances than reliance on organisational constraints alone.

Payment integrity does not require full transaction transparency. ZKPs enable validation of transactions and compliance rules without disclosing sensitive payment information.

The design requires careful consideration of trade-offs with other policy and operational objectives. Stronger privacy protections may affect programmability, system performance and complexity. Appropriate design and operational arrangements are therefore needed to balance the desired system attributes.

Privacy-enhancing technologies can support a degree of payment anonymity while maintaining regulatory safeguards. Cryptographic mechanisms enable users to conduct transactions without routinely revealing their identities to intermediaries and counterparties, while preserving the ability to identify illicit activities.

Central banks can benefit from further studies of PETs across a range of use cases. Beyond supporting payment privacy, these technologies can facilitate secure data sharing and collaboration among institutions, enabling the detection of money laundering, fraud and other illicit activities while protecting sensitive information.

Given the still early stage of PETs in the context of central bank money, the Aurum Phase 2 prototype is the result of extensive collaboration between the BIS Innovation Hub, the Hong Kong Monetary Authority, the Hong Kong Polytechnic University and the Hong Kong Applied Science and Technology Research Institute.

Contents

Executive Summary	3
Acronyms, abbreviations and definitions	8
1. Goals and objectives	9
2. Core guiding principles	9
2.1. Privacy by design	9
2.2. Public policy objectives	11
3. Related work on privacy in digital cash	11
3.1. e-HKD	11
3.2. BIS Project Tourbillon	12
3.3. Digital Euro	12
4. High-level system architecture	13
5. PETs used in Aurum Phase 2	15
6. Balancing privacy and controls	16
6.1. Selective disclosure	16
6.2. Anonymous wallets	17
6.3. Fractional locking of funds	18
6.4. Configurable onboarding process	19
7. Privacy improvements in Aurum Phase 2	20
8. Analysis of trade-offs in the Aurum Phase 2 design	21
8.1. Performance	21
8.2. Limited programmability	22
8.3. Backup and recovery	22
9. Other learnings	23
9.1. Collaborative compliance	23
9.2. Continuity of access across intermediaries	24
9.3. Auditability using pseudonyms	25
9.4. Custody and ownership proofs for tokenised digital assets	26
9.5. Quantum resilience	27
10. Conclusion	28

Acknowledgements	29
Bibliography	30
Annex A Data access matrix	32
Annex B Technical details on PETs adopted	34
1. BBS+ signatures	34
2. Pseudonyms	35
3. Zero-knowledge proofs	37
4. Privacy-preserving coin structure	40
5. Unique double-spending prevention tag & signature proof of knowledge mechanism	41
6. Two-step ZKP generation to enhance usability	42
Annex C. Transaction flow	44
1. Overall transaction flow	44
2. Encrypted remarks message for bank communication	45
3. New coin scheme	46
4. Coinbase transaction	47
5. Regular transaction for payment	48
6. Redemption transaction	49
7. Decree transaction	50
8. Batch transaction	51
Annex D Performance	52
1. Pseudonym Size	52
2. Cryptographic performance	52
3. Batch processing	53
Annex E Resilience to privacy risks	55

Acronyms, abbreviations and definitions

AML	Anti-money laundering.
Bank	Commercial banks who have access to the wholesale and retail layers to distribute digital cash to their customers.
BBS+ signature	BBS+ signature refers to an improved variant of the Boneh–Boyen–Shacham (BBS) signature scheme, originally named after its creators.
CFT	Countering the financing of terrorism.
Digital cash	A form of money that exists in digital form which is equivalent to physical cash, and which represents the liabilities of the central bank.
DLT	Distributed ledger technology.
ECC	Elliptic curve cryptography.
End user	A bank's customer or retail user, acting as payee or payer using digital cash. They are also consumers from the perspective of consumer protection.
Input coin	An existing coin from the payer to be specified in a payment transaction, the value of which will be transferred to the payee.
MPC	Multi-party computation.
Output coin	A new coin generated in a payment transaction, to be received by the payee.
Payee	An end user who receives digital cash from a payer.
Payer	An end user who transfers digital cash to a third party.
PII	Personally identifiable information.
PETs	Privacy-enhancing technologies.
PQC	Post-quantum cryptography.
Prover	A party that generates a ZKP to demonstrate knowledge of a secret to a third party.
PSD	Abbreviation of pseudonym.
RSA	Rivest–Shamir–Adleman is a widely used asymmetric public-key cryptographic algorithm for secure data transmission.
SPK	Signature proof of knowledge is a signature that proves ownership of a coin, by associating the coin and the corresponding tag.
Tag	Double-spending prevention tag is a unique proof associated with each coin. It is presented to the validator to decide whether the coin has been spent before.
TEE	Trusted execution environment.
Transaction proposal	Constructed jointly by the payer and the payer's bank to initiate a payment, including the input coin(s) and output coin. The proposal needs to be endorsed by the validator to complete the payment.
UTXO	Unspent transaction output, the representation for the digital cash token and the digital cash-backed stablecoin. Each Aurum 2.0 transaction contains input and output UTXOs.
Validator	A trusted entity that validates transactions executed by the banks. There are two types of validators: (i) for the digital cash system, a dedicated validator which is an independent trusted entity; and (ii) for the wholesale central bank money, a DLT validator, which is a role performed by an issuing bank which is also a member of the interbank DLT system, as shown in Graph 6.
VCs	Verifiable credentials.
Verifier	A party that verifies the ZKP presented by a prover.
ZKP	Zero-knowledge proof.
zk-SNARK	Zero-knowledge succinct non-interactive argument of knowledge.

1. Goals and objectives

According to publications by the Bank for International Settlements (BIS) on digital cash,² privacy is a design goal that should balance user confidentiality with law enforcement and public policy needs. A digital cash system should not be so opaque that it hinders financial crime compliance, nor so transparent that it violates user privacy. In practical terms, this means limiting unnecessary access to payment data while preserving lawful access where legally justified.

Rather than the absence of data altogether, privacy is the ability to limit who can access payment data, what they can see and under which conditions.³ Every digital cash design sits somewhere between hard anonymity (like physical cash) and transparency (like many account-based payment systems). Viable digital cash must occupy a middle ground, namely “privacy with auditability”: ordinary payment data are shielded by default, while legally justified access remains possible to prevent crime, protect consumers and intervene when the law requires it.

Using cryptographic techniques including BBS+ signature scheme and ZKPs, Project Aurum Phase 2 explores privacy options that can provide increased protection compared with certain existing private sector digital payment solutions, while balancing public policy objectives such as anti-money laundering, fraud prevention and financial stability. We end with an evaluation of the limitations of the design, offering ideas for future improvements.

Why is pseudonymisation alone not enough to address privacy threats?

It is because the underlying data in the payment ledger often carry enough unique features to enable re-identification, especially when combined with other data sets. Pseudonymisation typically replaces the direct identifiers (eg name), while quasi-identifiers, including payment linkages, transaction patterns, timestamps or geolocation, can enable inferences as to the real identity (eg name) behind a pseudonym.

2. Core guiding principles

This section lays out the principles of privacy by design balanced with public policy objectives such as anti money laundering, fraud prevention and financial stability that guide the Aurum Phase 2 investigation into payment privacy in digital cash. Together, they frame the policy question for central banks: *can people make routine payments without exposing unnecessary personal information, while authorities retain appropriate tools to manage risks?*

2.1. Privacy by design

Privacy by design provides a holistic approach whereby privacy protections are built into the technical architecture from the outset, limiting data collection, exposure and access by default, while still allowing proportionate and legally bounded auditability.

2. Bank of Canada et al (2020).

3. Auer et al (2025).

Any PETs should be embedded into the architecture of the digital cash system, not bolted on as an extra layer, and privacy by design requires a clear designation of the roles of central banks and intermediaries, which can directly affect the privacy landscape in the digital cash system (Jiang (2023)). Overlaying privacy at a stage later than at the initial design may introduce risk and may make it challenging to uphold the end-to-end security principle.⁴

Against this backdrop, Aurum Phase 2 adopts the privacy by default and privacy by design principles as follows:⁵

- **Proactive, preventive.** Privacy by design requires anticipating and preventing privacy risks before they occur, rather than responding after harm has happened. As noted above, the key design principle is to build systems to avoid privacy breaches, not just to respond to them. In the case of Aurum Phase 2, this entails privacy risk assessment during system design, threat and misuse cases modelling upfront and not relying on ex post controls alone.
- **Privacy by default.** Personal data should be automatically protected without requiring any action by the user. The key idea is that if a user does nothing then their privacy remains intact. The Aurum Phase 2 prototype provides for maximum privacy settings and minimum data-sharing by default, unless legally required or requested by end users.
- **Positive-sum functionality.** Privacy by design rejects the idea that privacy must be traded off against other objectives (eg security, efficiency, compliance). The key design principle is to achieve both privacy and system functionality. In the case of the Aurum Phase 2 prototype, we seek solutions that satisfy multiple goals simultaneously and that support PETs like ZKPs, which enable compliance without disclosure.
- **Embedded into the design.** As noted above, privacy must be integrated into the architecture and core functionality of systems, not bolted on as an add on. This helps align privacy protections with the way payment data move through the system.
- **End-to-end security.** Privacy applies across the entire data lifecycle: from collection to use, retention and deletion. This principle closely links privacy by design to security engineering and requires implementation of strong personal data protection from beginning to end across the complete data processing cycle. Payment transactions may propagate via different parties, creating the risk of misuse of transaction records, including re-identifying users through complex data analytics. The Aurum Phase 2 prototype prevents this through different ledgers and access controls.
- **Visibility and transparency.** Privacy by design requires that systems be open to inspection, verification and accountability. The key design principle is that there should be no secrets about how the system works. This means clear

4. Bank of Canada et al (2024).

5. Cavoukian and , A., & Rossos , P. G. (2009). Personal health information a practical tool for physicians transitioning from paper-based records to electronic health records.

documentation of data practices, auditability of privacy controls and independent verification where appropriate. For the Aurum Phase 2 prototype, this report serves to explain the architecture. It is backed up by clear documentation and code that is available to central banks on BIS Open Tech.

- **User-centricity.** End users should be properly informed and give their consent before their data are shared. In the Aurum Phase 2 prototype end users have the option to select transaction data to be shared with the counterparty, or not to share at all.

2.2. Public policy objectives

Privacy design should not harm or degrade the effectiveness of public policy objectives such as anti money laundering (AML), countering the financing of terrorism (CFT), fraud prevention and financial stability. It should not prevent lawful access by authorities where legally justified and should not hinder law enforcement's ability to conduct legitimate investigations of financial crime offences.

3. Related work on privacy in digital cash

This section highlights selected digital cash initiatives that have explored approaches to payment privacy. They provide useful context for Aurum Phase 2.

3.1. e-HKD

Project Aurum Phases 1 and 2 contribute to the research of the e-HKD's potential extension into retail scenarios in Hong Kong SAR. Privacy has been placed at the forefront of the e-HKD's design, responding directly to public and industry feedback. It was identified as the most significant concern among all potential impediments to adoption – ahead of cyber security, performance, scalability and operational resilience. Most respondents to the consultation believed privacy should take precedence over efficiency, with many emphasising that safeguards must be built into the central bank digital currency itself rather than relying solely on regulation. There was also a strong call for transparency about which data would be collected and held by the central bank, banks and other intermediaries, so that users could fully understand how their personal information would be handled.

To address these priorities, the Hong Kong Monetary Authority (HKMA) has adopted a privacy by design framework for the e-HKD. The model is built on Hong Kong SAR's well established two-tier banking system, in which licensed banks remain the primary customer interface. These banks undertake identity verification, financial crime compliance checks and transaction processing, while sensitive personal data stay with the customer's chosen bank. Such information is not automatically shared with the HKMA or other actors. Only the minimum data required for payment

6. BISIH (2023).

7. Deutsche Bundesbank (2026).

processing and financial crime compliance are exchanged and unlike public blockchain systems, transaction details are not openly visible to all participants.

This approach seeks to strike a careful balance between privacy, financial crime compliance requirements and performance. For users, it means digital cash that addresses their top concern by ensuring confidentiality in every transaction, while still delivering the convenience and speed of modern payments. With privacy protections embedded into its architecture from the outset, the e-HKD is designed to foster trust, encourage adoption and meet some of the highest standards for security and personal data protection.

3.2. BIS Project Tourbillon

Project Aurum Phase 2 builds on the learnings of Project Tourbillon⁶, carried out by the BIS Innovation Hub Swiss Centre. Project Tourbillon focused on privacy in digital cash, specifically testing the notion of payer anonymity. In other words, individuals making payments using digital cash do not reveal their identity, such that they remain anonymous to merchants, banks and central banks. However, the receiving party (eg a merchant) is identified to the bank, which keeps this information private. This design helps preserve privacy while also supporting efforts against tax evasion and unlawful transactions. The central bank only sees the transaction amount and not the parties involved.

3.3. Digital Euro

Project Aurum Phase 2 took inspiration from ongoing digital euro research⁷. The digital euro is being designed by the European Central Bank (ECB) with privacy as a central foundation, aiming to deliver the highest privacy standards of any electronic payment system. To achieve this, the Eurosystem employs a privacy by design approach that integrates strong technological safeguards and the European Union's rigorous legal protections from the outset. A distinguishing feature of the digital euro is its offline payment mode, which offers cash like privacy, ensuring that transaction details are known only to the payer and the recipient, without internet connectivity or third party visibility. Online payments also preserve user confidentiality through a system in which the ECB receives only pseudonymised data, preventing it from identifying users or linking them to specific transactions, while intermediaries like banks access only the minimum information needed for AML and CFT compliance and must seek explicit consent for any commercial data use.

Critically, the ECB itself never uses personal data for commercial purposes, reinforcing the digital euro's role as a public good rather than a revenue generating platform. User data remain inaccessible to the ECB in identifiable form, as all information it receives is pseudonymised and therefore cannot reveal personal identities. Intermediaries are strictly limited in what they may access, viewing only the narrowly defined personal data required by EU law, with any additional use – including commercial profiling – dependent on the user's explicit permission. The privacy framework is strengthened by state of the art PETs and continuous assessment of emerging cryptographic methods to support anonymity, secure offline functionality and resilience against future threats. These technological safeguards operate alongside robust legal oversight by independent data protection authorities,

ensuring compliance with Europe's stringent data protection laws. Together, these measures aim to safeguard individual privacy while balancing legitimate regulatory needs, ensuring that the digital euro remains secure, trusted and aligned with fundamental European values.

4. High-level system architecture

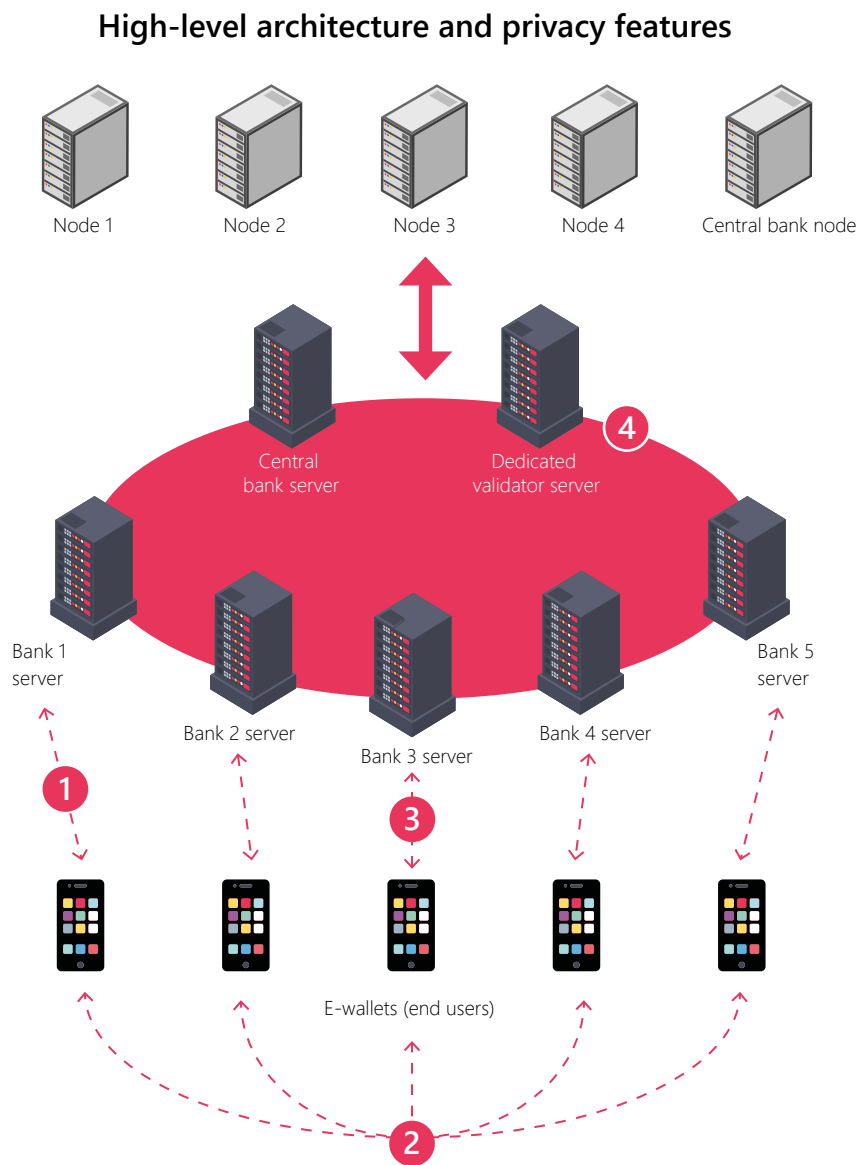
The system of Project Aurum Phase 2 builds on the two-tier architecture of Project Aurum Phase 1. The architecture is relevant for central banks because it illustrates how responsibilities and data access can be separated across the system, while preserving payment integrity. It consists of two main components: digital cash (e-wallet) on the retail layer and the interbank system on the wholesale layer. This separation is important for privacy because retail payment information does not need to be visible to every participant in the wholesale layer, while the central bank can retain its role in issuance and settlement functions without automatically accessing all retail transaction details.

The interbank system on the wholesale layer includes the central bank, banks and validators as participants. This system is built on a distributed ledger technology (DLT) infrastructure, ensuring security and transparency in transactions among the participants. The DLT network on the wholesale layer conducts four types of transactions:

- The issuance of digital cash from the central bank to a financial intermediary.
- The redemption of digital cash at the central bank by a financial intermediary.
- The deposit of digital cash by a financial intermediary for the purpose of digital cash distribution to the e-wallet platform.
- The release of digital cash to a financial intermediary in response to digital cash redemption by the bank from the e-wallet platform.

The digital cash system on the retail layer is bank-based e-wallet network involving financial intermediaries, bank customers and validators. Each bank customer has an e-wallet, which is provided as a mobile phone application and is attached to the customer's bank. All e-wallet activities, such as payments, are conducted through the customers' respective banks. The e-wallet system operates on a non-DLT infrastructure. Digital cash is represented in the form of an unspent transaction output (UTXO) token to ensure payment integrity. The main operations of digital cash on the retail layer include:

- Facilitating the exchange of fiat currency with digital cash and vice versa.
- Enabling end user payments and the receipt of digital cash.
- Handling end user requests to trace the transaction history of digital cash.



Privacy features

- 1 Privacy-preserving credential issuance
- 2 Evolving pseudonym generation
- 3 ZKP generation
- 4 Double-spending prevention by proof checking

5. PETs used in Aurum Phase 2

Building on the overall architecture, this section highlights the core PETs used in Aurum Phase 2:

- **Evolving pseudonyms using BBS+ signatures.** The Aurum Phase 2 prototype addresses the tension between privacy and public policy objectives such as anti money laundering (AML), countering the financing of terrorism (CFT), fraud prevention and financial stability by adopting evolving pseudonyms. Users complete know-your-customer (KYC) procedures through a duly licensed bank, where their legal identity is securely held and is not exposed to the wholesale layer. After verification, end users may generate and use multiple pseudonyms. Each pseudonym is unlinkable to the end user's real identity (eg name), yet verifiable as belonging to a legitimate, KYC-verified account. This architecture allows for privacy-preserving operation within the system, prevents external parties like merchants from transaction linkage or behavioural profiling, while compliance obligations are fulfilled through bank-managed traceability and legal accountability. After completing KYC, the user receives a credential, in the form of BBS+ signature, from the duly licensed bank on their certified public key. This credential allows the user to create pseudonyms above without revealing the public key itself.
- **Zero-knowledge proofs (ZKPs).** Evolving pseudonyms are not enough to safeguard end user identity. Even when both the payer and payee use pseudonyms, the centralised infrastructure can correlate transactions. Therefore, in the Aurum Phase 2 prototype ZKPs are used to restrict visibility of payment details (including payment amounts), while still allowing the transaction to be verified as valid. The design mimics the money movement of physical cash. As in settlement with bills and coins, legal finality occurs simultaneously at the moment of payment and each coin is stored separately in the user's wallet. This prevents a centralised infrastructure from correlating payments for surveillance purposes.
- The technique to **partition ledgers and data** is also employed. In the Aurum Phase 2 prototype, partitioning occurs on two levels: not only are the wholesale ledgers and retail ledgers kept separate as shown in Graph 1 so that the central bank cannot access the retail ledger, the ledgers across banks are also kept separate. The outcome of this architecture is a partitioned data approach, in which the physical segregation of personal data across different intermediaries offers higher confidence in privacy protection.

While the main report focuses on the privacy features, functionalities and their policy implications, Annex B and C provide a technical overview of the underlying design and cryptographic mechanisms for readers seeking a deeper understanding of the implementation.

6. Balancing privacy and controls

This section explains how the Aurum Phase 2 prototype explores flexible ways to balance privacy with the role of regulated intermediaries, lawful access and compliance controls in practical payment scenarios. It illustrates how different controls could be configured depending on policy requirements, risk appetite, user needs and the desired level of privacy. The prototype includes options such as: greater privacy for low value, everyday transactions, similar to cash, stronger checks or traceability for higher risk uses, configurable onboarding rules depending on legal requirements, and safeguards that protect consumers while still allowing recovery or intervention in defined cases.

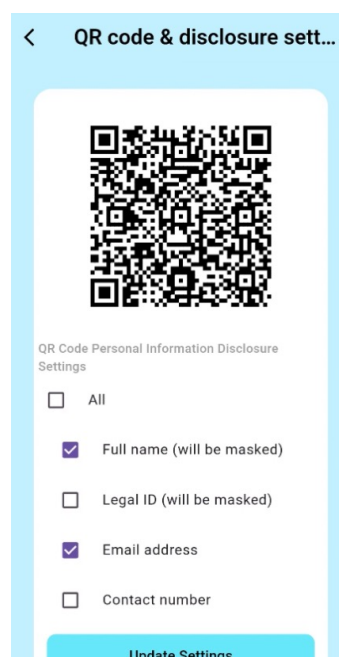
6.1. Selective disclosure

Selective disclosure allows information to be shared in a controlled way for specific payment scenarios, including voluntary sharing by users and disclosure triggered by compliance controls. The payment process is similar to QR code-based electronic payments, while privacy protections are embedded in the system. A payer initiates a payment by opening the payment screen and scanning the payee's QR code. They then select a payment account from their wallet and enter the amount. By default, no personal information is shared unless required by compliance measures. In certain situations, the payer can voluntarily choose and share selected personal information with the payee in the payment screen to enable specific programmable functions:

- **Payee** may choose to disclose selected personal information when generating a QR code to receive payment. This information will be visible to the payer before the payment is confirmed, enabling transparency when desired.

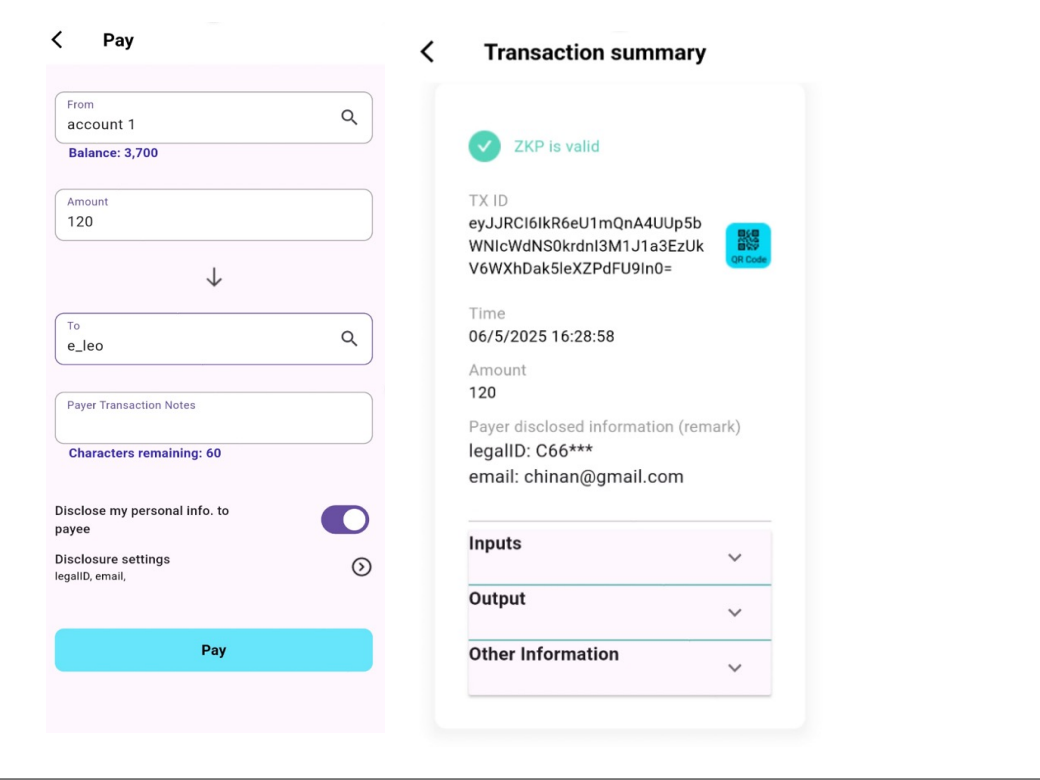
KYC verified account QR code with privacy disclosure

Graph 2



- **Payer** may also voluntarily choose to disclose selected personal information as part of the payment. However, when a payment amount **meets or exceeds a bank defined disclosure threshold**, payer information disclosure is automatically required in accordance with the compliance policy. In such cases, the payer’s **full name and legal identifier become viewable in masked format** on the transaction summary screen.

Payer’s information shown to payee in the transaction summary Graph 3



6.2. Anonymous wallets

The concept of full anonymity may not be well received from a compliance perspective. Tourism is one exception. Foreign tourists may demand strong payment privacy to minimise their payment trails. They may also be reluctant to share their personal data such as passport information. **A controlled anonymous account arrangement could balance privacy with compliance needs by imposing low wallet and spending limits, as well as binding to mobile devices.** For central banks, this illustrates how privacy settings could be calibrated for specific use cases, rather than applying the same level of risk controls to every wallet. It allows self-hosted wallets to be subject to a common transaction limit alongside other payment instruments, reducing the risk of regulatory arbitrage.⁸

Overall, to prevent the same person from opening multiple anonymous accounts via different banks, all anonymous accounts should be managed by a dedicated intermediary in the system, eg a neutral entity such as a post office. In our design,

8. Minto et al (2026).

this intermediary may offer an anonymous accounts service, allowing only one account per legal identifier and device. The end user must present a legal identifier at the counter to the member of bank staff, who verifies the identification document and activates the anonymous account without requiring the user to expose sensitive data. Cash can be accepted to fund the user's wallet, allowing the user to enjoy a high degree of anonymity for low-value transactions.

The Aurum Phase 2 prototype thus demonstrates the technical feasibility of anonymous wallets. The anonymous account is subject to configurable restrictions set by the bank. Banks can adjust the account's limitations individually through the web portal, ensuring that e-wallet limits are equal to or greater than the available balance. The onboarding arrangement is aligned with the principles of equity vis-à-vis public goods where residents may not provide formal proof of identity or possess the technical proficiency to handle cumbersome KYC processes.⁹

Can I hide my identity from my payer/payee?

Yes, the anonymous wallet can achieve end-to-end privacy so that the counterparty can never attribute it to the real identity. This is an improvement in comparison with an account-based setting such as an instant payment system in which the recipient needs to share an account identifier (account number or mobile phone number) with the counterparty. If it is a static alias (wallet ID), the counterparty may link to the real identity via indirect means.

In the highest privacy setting, both payees and payers can remain anonymous to each other. In this case, only pseudonyms are exchanged in QR codes to complete a payment transfer and these pseudonyms are not linked to the corresponding identities.

6.3. Fractional locking of funds

For central banks, fractional locking of funds illustrates how controls could be applied more proportionately when fraud or illicit activity is suspected. In the banking system an account can be active or suspended. In practice, banks can also freeze or restrict access to specific funds within an account without suspending the entire account (eg when only part of the balance is subject to earmarking or similar restrictions). The Aurum Phase 2 prototype provides an option in between to lock part of the funds in the account. Aurum Phase 2 differs in how this control is represented technically: instead of treating the balance as one pool of funds and applying "holds" at the account layer, it can apply a lock at the level of individual digital cash coins. For example, if the end user receives the funds from a suspicious third party, the funds received could be locked while the account and other funds can remain usable. The design in Project Aurum Phase 2 can provide flexibility to lock the wallet or funds in the wallet.

9. OECD (2023).

In other words, the design supports locking: (i) a specific coin; (ii) a subset of coins within a wallet; or (iii) the whole wallet depending on the risk event. A wallet may consist of multiple coins transferred from various payers. If one incoming payment is considered suspicious, the bank can temporarily lock only the coin(s) received in that transfer, while leaving the rest of the wallet usable. This provides a clearer separation between affected and unaffected value than account-level holds on a pooled balance. Like bank accounts, the wallet as a whole can be locked temporarily in the case of fraud.

6.4. Configurable onboarding process

Configurable onboarding illustrates how access requirements for digital cash could vary depending on legal requirements, risk controls and privacy expectations. In the Aurum Phase 2 prototype, there is a high degree of flexibility in the arrangements to set the privacy threshold for user onboarding. The objective is to allow the bank to enforce a uniqueness constraint (one user, one wallet) and prove that the user has one and only one wallet in the ecosystem, without revealing any PII.

The onboarding process can be configured according to privacy appetite and jurisdiction-specific regulatory requirements. The access tiers can be applied in conjunction with various compliance controls and measures so that regulators may evaluate the trade-offs in residual risks and usability. Rather than representing a linear progression from “no KYC” to “full KYC”, these tiers reflect alternative mechanisms to establish authenticity and uniqueness, combined with transaction limits, device constraints and other risk controls. The approaches include:

- No identity checks. Controls with no identity attribution, such as issuance limits, transaction caps or rate controls, without binding the wallet to an identity attribute.
- Binding to a specific mobile phone, reducing the risk of multiple registrations while avoiding storage of legal identity data.
- Alternate proof mechanisms, in which end users obtain a one-time or limited-use proof of eligibility through an anonymising process (eg tourists can obtain a unique voucher at the immigration counter with a requirement to link to passports).
- Interface to a third-party identity service provider, which presents a unique and non-linkable tokenised account identifier to the bank, as practiced by the “iAM Smart”¹⁰ government ID system.
- Limited access to the identity wallet or security enclave in the mobile device. With a trusted protocol to interface with the trusted execution environment (TEE), the bank may obtain proof of legitimacy via ZKP without revealing the real identity.
- Simplified checks without storing personal data. The bank validates the end user’s legal ID and only keeps the privacy-preserving unique identifier to prevent duplicate registration.
- Comprehensive checks to store personal data.

10. www.iamsmart.gov.hk.

To further expand the scope to cross-border due diligence checks, the compliance level can be enhanced by integration with automated compliance checks embedding jurisdiction-specific policy and regulatory requirements, which Project Mandala¹¹ focused on. For the onboarding process for commercial companies, it is also possible to leverage harmonised data connectivity across jurisdictions, as seen in Project Aperta.¹²

7. Privacy improvements in Aurum Phase 2

The table below translates common privacy concerns into concrete design considerations explored in the Aurum Phase 2 prototype. It illustrates how PETs and design choices can address these concerns by limiting unnecessary access to identity and transaction data, while preserving the information needed for payment processing and compliance controls.

Privacy concerns and how they are addressed in our design Table 1

Privacy concerns expressed by the general public	How this concern is addressed in our design
<i>Digital cash issuer (central bank) can know my identity.</i>	Customer identity is only kept at the duly licensed bank that onboards the end user. The duly licensed bank has a legal and contractual obligation to safeguard this information. The central bank cannot access the retail ledger and therefore cannot see the customer identity.
<i>A centralised payment infrastructure can see my transactions, including account details and identity.</i>	Similar to physical cash (coins or bills) in a wallet, digital cash tokens are kept in the user's digital wallet. Each transaction is an independent event preventing the linking of any past transactions. No centralised infrastructure can see the transaction amount or user identity.
<i>Merchants can collect and profile my spending behaviour based on my payment transaction data.</i>	Each transaction is an independent event preventing linking of any past transactions. The same end user will be exhibited as a new user for each transaction. Even if merchants merge their ledgers, they cannot reconstruct or derive the purchase history.
<i>The counterparty bank knows my personal details.</i>	The counterparty bank only gets essential data of the payee, including the payee's pseudonym and payment amount. The personal particulars of the payer, including account numbers and names, are not shared by default.
<i>Public blockchains can track my payment history.</i>	The customer base of each bank is kept only by that bank. It is not accessible by the validator, counterparty bank or the central bank. The bank payment ledgers are isolated and partitioned; hence no single party can reconstruct the payment history.
<i>Cyber attackers can exfiltrate a huge amount of personal data from concentrated data repositories.</i>	The design implements a partition of data and segregation of responsibilities. If the validator is compromised, the end user identities would not be stolen. If one bank is compromised, only the customers' data of that bank may be at risk, but the counterparties' customer identities will not be stolen. If the merchant is compromised, no identities will be stolen. ¹³

11. BISIH (2024).

12. www.bisih.org/about/bisih/topics/open_finance/aperta.htm.

13. The data compromise assumes data loss in the payment data in Aurum's components only. It does not take into considerations if personal data are stored in other databases in the organisation.

8. Analysis of trade-offs in the Aurum Phase 2 design

Privacy in digital cash design inevitably involves trade-offs: additional privacy protections can slow transaction processing or make the system harder to adapt for complex financial products. Wallets that maximise privacy may also be harder to recover if access is lost, much like losing physical cash. These are policy relevant choices, not purely technical ones.

8.1. Performance and scalability

Project Aurum Phase 2 demonstrates that privacy-enhancing digital cash is technically feasible, but its operational design must carefully balance privacy, usability and performance. The pseudonym design protects end-user identity from third parties while allowing the user's bank to recover identity for AML/CFT compliance; at around 2 KB, it is small enough to fit in a single QR code, though further optimisation would improve accessibility for older devices or poor scanning conditions and scalability when deploying in a large-scale system. The encapsulation of identifiers in a compact QR code can support financial inclusion by enabling participation from less technologically savvy users who may only be able to afford lower-cost mobile devices. On cryptographic performance, zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) are well suited to digital cash because verification is fast and lightweight, but proof generation remains the main bottleneck. GPU acceleration materially improves feasibility, reducing proof generation which could support larger and more private transactions. To address coin fragmentation and high-volume use cases, such as merchants consolidating many small payments, the design also introduces optional batch processing, which improves efficiency by avoiding full ZKP generation but reduces privacy by allowing the validator to link input coins within one backward transaction layer. Overall, the design offers a flexible architecture in which users may choose between stronger privacy through regular transactions and higher efficiency through batch processing, with future optimisation of pseudonym size and hardware-accelerated proof generation key to broader deployment. Scalability can be achieved through a combination of distributed system and database scaling techniques. These include spreading the workload across multiple servers, handling transaction checks separately from database updates, dividing the database into smaller sections to reduce congestion, and allowing unrelated transactions to be processed at the same time. Brazil's experimentation of Drex confirms that trade-offs persist among the "privacy trilemma" of privacy, scalability and programmability.

8.2. Limited programmability

A design that limits data sharing can strengthen privacy, but it may also constrain some forms of programmability. For central banks, this highlights a policy trade-off: more privacy can reduce the amount of information available for automated payment functions. In a DLT system, programmed payments can be triggered by smart contracts automatically as counterparties join forces in the consensus on the same chain. In Project Aurum Phase 2, data partitioning is applied so that the information about the counterparties is not visible in real time in the payment network. In this model, programmability is not provided through a general purpose virtual machine, but through conditions embedded in individual coins. The validator may enable conditional payment, such as merchants sending coins to rebate customers with the restriction that they can only be spent at the same merchant. Depending on the privacy design, such conditions can be expressed in plaintext, which allows direct enforcement but exposes metadata, or in encrypted form supported by ZKPs, which enhances privacy but requires more complex validation. The use of BBS+ signatures further allows attributes to be selectively disclosed, enabling conditions to be tied to specific credential properties without revealing full user data. How such programmability is realised is the choice of individual jurisdictions. To retrieve real-world events for payments, banks may obtain data from other trusted data sources. For example, banks can track the delivery status of a package to trigger a payment to a seller. Since each coin requires user signing for payment, programmability may require the user to delegate temporary custody to a bank, which introduces counterparty risk compared with cash-like models. Overall, programmability in this approach is limited to predefined conditions on transferability and off-chain logic enforced by intermediaries, rather than open-ended composability as in account-based smart contract systems. In the Drex experimentation, a higher level of privacy protection was found to impair programmability.

8.3. Backup and recovery

Backup and recovery raise an important policy trade-off in privacy-preserving digital cash. Stronger user control and privacy can reduce reliance on intermediaries, but may also make it harder to recover funds if access credentials are lost. The payment process requires digital signatures from both the end user and the bank, thus making the payment resilient to fraudulent transactions. The non-custodial nature of the coin enables it to be stored in an offline medium like a smartcard or Hardware Security Module (HSM). The end users may leverage third-party custodians to safeguard their private keys and digital cash. In a digital cash system, the coins ultimately represent the liability of the central bank.

The trade-off is most visible in the anonymous wallet setup. Since there is no linkage between the e-wallet and the owner's identity at maximum privacy levels, the funds cannot be recovered. The end user of such an anonymous e-wallet thus needs to accept a risk similar to that of losing physical cash as in the real world or losing private keys of cryptocurrency wallets.

9. Other learnings

During the exploration, it was observed that the PETs that were adopted offer benefits that extend beyond improved privacy protection. The underlying cryptographic techniques employed in these solutions can also support broader applications in tokenisation, cyber security and secure data collaboration. This section explores these additional advantages and how they may contribute to the integrity and resilience of financial infrastructures.

9.1. Collaborative compliance

A privacy-preserving digital cash system can make system-wide compliance analysis more complex because transaction data are not visible in one place. For central banks, the policy question is how suspicious patterns could be detected across institutions without recreating broad visibility over individual users' payment histories. To balance the needs, a separate data-sharing network could be created to construct a limited and purpose-specific "global view" of money transfers, focused on predefined risk indicators rather than full transaction histories or wallet-level linkability. According to the findings of Project Hertha¹⁴, "payment systems were particularly effective in identifying complex typologies involving many accounts across many banks and payment service providers. A different set of PETs such as federated learning and multi-party computation (MPC) could help with this by enabling the computation of agreed analytical outputs (eg risk scores, anomaly flags or aggregated indicators), while ensuring that raw transaction data and personal identifiers remain confined to originating institutions. The platform could be operated by an independent third party that has strong trust, or be designed so that no single operator has unilateral visibility or control, for example through confidential computing or distributed governance arrangements. Alternatively, if the system operator is not a trusted entity, a TEE could be used. The work in Project Aurora¹⁵ can fit with Project Aurum Phase 2 to detect money laundering activities without sharing personal data.

The Aurum Phase 2 design is also compatible with robust privacy-preserving commercial solutions¹⁶ to detect illicit transactions in production operations. With PETs, no personal data will be made available to this operator. There is a trade-off among computation power, data-sharing frequency and response time for results. Even if the anonymous e-wallet setup is adopted, selected transaction-derived signals can still be incorporated within the network to detect suspicious behaviour, without revealing end user identities or reconstructing individual transaction paths. Even though the e-wallet owner's identity remains untraceable, it can be temporarily locked to stop fraud or money laundering activities. The accessibility of personal data are thus shielded from the federated learning platform while enabling data-sharing for detecting money laundering and fraud.

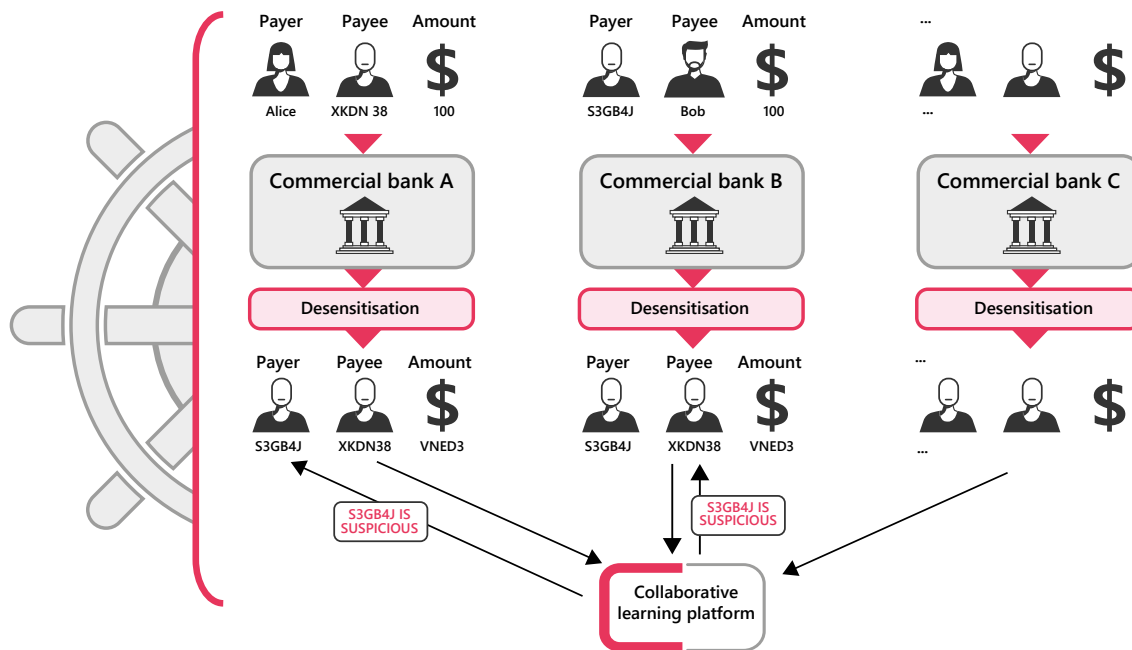
14. BISIH (2025).

15. BISIH (2023).

16. BIS (2023a).

Collaborative data analysis to identify suspicious wallets

Graph 4



9.2. Continuity of access across intermediaries

The pseudonym design also raises a useful design question around portability of user access. In the current setup, users onboard through a specific bank where KYC is conducted and this bank effectively becomes the single point of access mediation. Although users operate within the system through pseudonymous identifiers, their ability to access system functionalities remains technically bound to the bank that initially verified them. If that bank becomes unavailable, the user may lose access altogether, despite their pseudonymous presence remaining logically valid.

This dependency does not compromise user privacy, as real identity data are never exposed beyond the bank. However, it represents a structural limitation in how access rights are anchored and maintained. For future development, this raises the need for access portability, enabling users to retain their system access rights even when switching to a different bank. Such flexibility could be achieved through transferable access tokens or cryptographically verifiable artifacts that decouple system access from a fixed bank relationship. These solutions could, in the future, be implemented using mechanisms similar to verifiable credentials (VCs), allowing users to carry forward their access rights across different financial intermediaries without re-exposing their legal identity. This direction would reduce structural dependency on a single bank, enhance user autonomy and enable a more resilient and modular access architecture across multiple intermediaries.

9.3. Auditability using pseudonyms

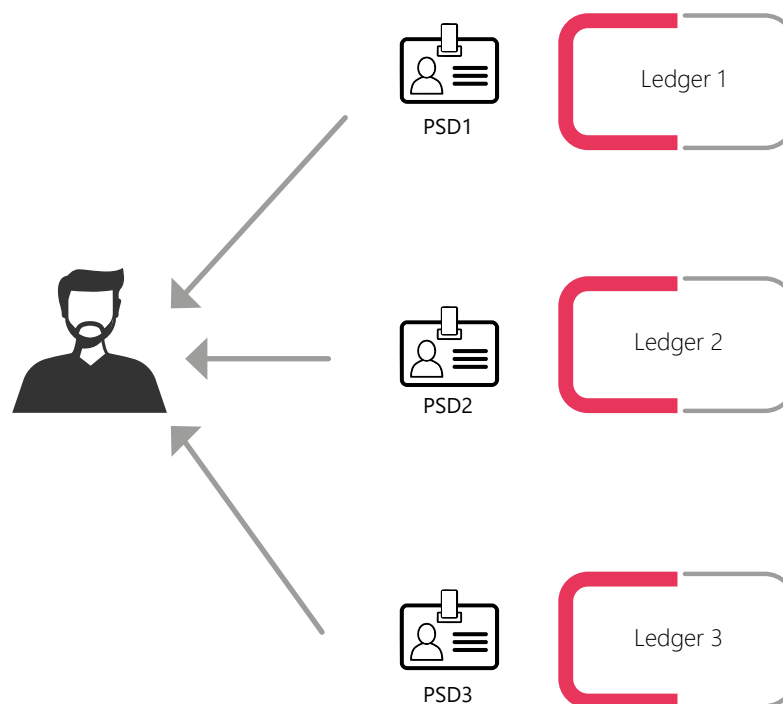
Pseudonyms may support auditability without making all transaction data broadly visible. The policy value is that authorised tracing can remain anchored at the intermediary level, while other participants do not automatically see the user's real identity.¹⁷ In this context, auditability does not rely on the broad transparency of transaction data, but on the ability of authorised parties to verify and, when necessary, trace activity via certified intermediaries.

While digital assets such as central bank money, stablecoins and real-world assets may be processed in different platforms, the pseudonym could be generated without involving an external party and the identity could be protected from other transacting counterparties. Even with the pseudonym itself, law enforcement agencies can look up the end user identity by checking with the issuing bank. This is in line with Rule 17 "Reliance on third parties" in *The FATF recommendations* that financial institutions may be permitted to rely on third parties to perform Customer Due Diligence measures.¹⁸

While pseudonyms can be reused in various platforms, they remain linkable by the issuing bank, which represents a deliberate trade-off between privacy and supervisory oversight. This design protects users from profiling by other users and infrastructure components but does not provide anonymity with respect to the intermediary.

Pseudonyms across platforms

Graph 5



17. BIS (2023b).

18. Financial Action Task Force (2025).

If the pseudonym size could be further reduced, it is possible to incorporate it into blockchain protocols. The pseudonym size in Aurum Phase 2 may be large for incorporation in some blockchain systems. But this is also dependent on the privacy requirements of the pseudonym. For example, if we only require the pseudonym to be certified by the intermediary with an anonymity property (ie no recovery of the end user's identity), the pseudonym size can be reduced by around 30%. Anyway, interoperability and auditability across platforms depend not only on representation size, but also on governance arrangements, trust assumptions and how platforms choose to record and interpret pseudonym usage.

Finally, the privacy implications of using certified pseudonyms differ depending on the environment. In Aurum Phase 2, payments are not publicly observable, which limits correlation risks. In contrast, if the same certified pseudonyms were reused on public ledgers, the public visibility of transaction histories could significantly increase privacy risks, particularly in the event of data leakage or compromise at the intermediary. Such trade-offs should therefore be carefully considered when applying this mechanism beyond the Aurum payment setting.

9.4. Custody and ownership proofs for tokenised digital assets

For central banks, the wider relevance of this experiment is that similar privacy-preserving proof techniques may be useful beyond digital cash. The Aurum Phase 2 design can be applied to support custody and ownership proofs for tokenised digital assets, by enabling privacy-preserving verification of value and control that can be referenced by tokenised representations on other platforms – without revealing more information than necessary.

Theoretically it could be extended to other use cases where the transfer of tokens is not frequent, particularly where ownership transfer is the primary state change and asset governance rules are relatively stable. For example, the token could represent high-value central bank reserves or digital assets, and the design could allow the tokens to be securely stored by the commercial banks or custodians. The token-based and zero-knowledge nature of the coins make them largely platform agnostic from a transfer and verification perspective, provided that participating platforms recognise the same trust anchors and verification semantics. The proof of value can be verified universally with an API call to the validator to enquire if it is spent or not, without needing to enrol in a platform, subject to appropriate access controls and governance over validator queries. The proof of value in the coin in the Aurum Phase 2 prototype is complete and can be linked back to tokenised wholesale central bank money or Real-Time Gross Settlement (RTGS) money movement. The use case can be expanded to proof of reserve across payment and digital asset platforms where zero-knowledge techniques can support privacy preserving proofs of aggregate holdings rather than the disclosure of individual positions. Any party with access to the validator can verify the value easily and quickly. To meet the reserve requirements of digital assets, the custodian can provide evidence to the public, regulators and auditors the size of the reserves by counting the coins in custody, while additional

mechanisms may be required to govern issuance, redemption and linkage to underlying off-ledger assets. This improves the transparency and auditability of tokenised money or digital assets across platforms particularly with respect to ownership and reserves verification, while preserving confidentiality at the level of individual positions.

9.5. Quantum resilience

As shown in Project Aurum Phase 2, the tokenisation ecosystem faces a complex set of quantum-related threats that could pose significant risks to its security and resilience. Further research is needed to assess the potential impact of such threats on tokenised financial market infrastructures and to identify effective mitigation strategies to achieve quantum resilience and agility. Covering the architecture and operation of both wholesale and retail layers, our prototype provides a basis for further exploration of quantum threats to a tokenised ecosystem.

Quantum computing represents a revolutionary shift in computational capabilities, posing significant threats to current cryptographic systems due to the ability of quantum computers to solve problems considered computationally infeasible by classical computers. The primary threat posed by quantum computing to the widely adopted cryptographic technologies at present arises from Shor's algorithm¹⁹, which can efficiently factor large integers and compute discrete logarithms.

In Project Aurum Phase 2, the ZKP scheme fundamentally relies on cryptographic assumptions in Elliptic curve cryptography (ECC) and the encryption and signature schemes are also ECC- and Rivest-Shamir-Adleman cryptography (RSA)-based. Therefore, cryptographically relevant quantum computers (CRQCs) running Shor's algorithm may efficiently compromise foundational assumptions of these cryptographic schemes.

The quantum threat necessitates the development and deployment of quantum-safe cryptography. It involves mathematical problems that quantum algorithms have not demonstrated efficient solutions for, such as lattice-based, multivariate polynomial and hash-based cryptographic schemes. These approaches remain secure against known quantum attacks, providing alternatives to secure digital infrastructure of digital cash against future quantum adversaries.

Transitioning to quantum-safe cryptography poses challenges due to performance considerations, in terms of both storage and running time. For example, BIS Project Tourbillon showed that implementing quantum-safe cryptography would severely increase transaction processing time. Particularly in digital cash systems, the volume of transactions is expected to be substantial for country-wide adoption. In the meantime, researchers are actively refining post-quantum ZKP techniques to mitigate performance gaps and maintain robust cryptographic assurances against quantum threats. It remains an open question whether a solution exists that is both secure in the post-quantum era, as well as efficient in performance for the digital cash setting.

¹⁹. Shor (1994).

10. Conclusion

Project Aurum Phase 2 explores a policy question for digital cash: can people make routine payments without exposing unnecessary personal information, while authorities retain appropriate tools to manage risks? The project delivers a digital cash prototype with better data privacy safeguards than existing setups for commercial payments, while still supporting public policy objectives such as anti money laundering, fraud prevention and financial stability.

The prototype's use of pseudonymisation, supported by BBS+ signatures and ZKPs, improves privacy while enabling intermediaries to retrieve end user identities for AML/CFT purposes when necessary, thereby maintaining traceability for compliance reasons. In practice, this means that payments can be validated and settled without exposing who paid whom, or how much, to parties that do not need that information. Banks remain able to meet their obligations, but sensitive personal data is not routinely shared across the system.

For central banks, the policy relevance of Project Aurum Phase 2 lies in showing how privacy choices can be explored at the design stage of digital cash, rather than treated only as a legal or operational safeguard after launch. The prototype is not a production-ready model, but an experimental way to examine how ordinary payments could offer a degree of cash-like privacy while preserving the role of regulated intermediaries, lawful access and compliance controls. This makes privacy something that can be supported through technical design, institutional arrangements and legal safeguards, rather than a promise that depends only on institutional restraint.

A key contribution of Phase 2 is showing that privacy and control can be adjusted to reflect local policy choices. The prototype provides features that enable jurisdictions to balance privacy, financial inclusion, financial crime prevention and consumer protection in accordance with their legal frameworks and risk appetite.

The project also makes clear that stronger privacy is not free of trade offs. Additional privacy protections can slow transaction processing or make the system harder to adapt for complex financial products. Wallets that maximise privacy may also be harder to recover if access is lost, much like losing physical cash. These are policy relevant choices, not purely technical ones.

Project Aurum Phase 2 supports the conclusion that privacy enhancing approaches can help digital cash meet public expectations without undermining regulatory objectives. With careful design and governance, digital cash does not need to choose between protecting individual privacy and maintaining effective control over financial crime. Instead, it can embed both as core public policy principles, leaving room for each jurisdiction to decide where the balance should sit.

Acknowledgements

Project teams

Bank for International Settlements (BIS)

Benedicte Nolens (Centre Head, BIS Innovation Hub Hong Kong Centre)

Jack Ho, Adviser (Project Lead)

Italo Borssatto, Adviser

Shauna Daswani, Team Coordinator

Hong Kong Monetary Authority

Michael Law, Senior Fintech Director

Lester Wong, Associate Fintech Director

The Hong Kong Polytechnic University (PolyU)

Prof Man Ho Allen Au, Professor and Associate Head (Research and Development), Department of Computing & Director of The Research Centre for Blockchain Technology (RCBT)

Dr Dennis Liu, Principal Project Fellow

Edith Yiu, Executive Manager & Senior Project Fellow

Alven Leung, Research Associate

Hong Kong Applied Science and Technology Research Institute (ASTRI)

Alan Cheung, Chief Director

Peifung Eric Lam, Director

Tim Wong, Project Manager

We would also like to thank Mert Askaroglu, Miguel Diaz, Henry Holden, Jon Frost and Lucy Wong of the BIS for their review of the report and their feedback.

Bibliography

Au, M, W Susilo and Y Mu (2006): "Constant-size dynamic k-TAA", in R De Prisco and M Yung (eds), *Security and cryptography for networks*, Springer.

Auer, R, R Böhme, J Clark and D Demirag (2025): "Privacy-enhancing technologies for digital payments: mapping the landscape", *BIS Working Papers*, no 1242.

Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System and Bank for International Settlements (2020): *Central bank digital currencies: foundational principles and core features*.

Bank of Canada, Swiss National Bank, European Central Bank, Bank of England, Bank of Japan, Board of Governors Federal Reserve System, Sveriges Riksbank and Bank for International Settlements (2024): *Central bank digital currencies: system design*, November.

BIS (Bank for International Settlements) (2023a): *BIS and Reserve Bank of India announce winners of G20 TechSprint 2023*, press release, 4 September.

——— (2023b): "Blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report 2023*, June, Chapter III.

BISIH (BIS Innovation Hub) (2023): *Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders*, May.

BISIH (BIS Innovation Hub) (2023): *Project Tourbillon demonstrates cash-like anonymity for retail CBDC*, November.

BISIH (BIS Innovation Hub) (2024): *Project Mandala: shaping the future of cross-border payments compliance*, October.

BISIH (BIS Innovation Hub) (2025): *Project Hertha: Identifying financial crime patterns in real-time retail payment systems*, June.

BISIH, De Nederlandsche Bank and Deutsche Bundesbank (2023): *Project Atlas: mapping the world of decentralised finance*, October.

Blum, M, P Feldman and S Micali (2019): "Non-interactive zero-knowledge and its applications", in O Goldreich (ed), *Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali*, Association for Computing Machinery.

Boneh, D, X Boyen and H Shacham (2004): "Short group signature", in M Franklin (ed), *Advances in cryptology – Crypto 2004*, Springer.

Deutsche Bundesbank (2026), *The digital euro: key elements and outlook*, article in *the Monthly Report*, March.

Cavoukian, A. and P, & Rossos, P. G. (2009): *Personal health information: A practical tool for physicians transitioning from paper-based records to electronic health records*.

Financial Action Task Force (2025): *International standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations*, updated October.

Groth, J (2016): "On the size of pairing-based non-interactive arguments", in M Fischlin and J-S Coron (eds), *Proceedings, part II, of the 35th Annual International Conference on Advances in Cryptology, Eurocrypt 2016*, Springer.

Jiang, J (2023): Privacy Implications of Central Bank Digital Currencies, 54 Seton Hall L. Rev. 69 (2023).

Looker, T, V Kalos, A Whitehead and M Lodder (2023): *The BBS signature scheme*.

Minto, A, A Kosse, T Shirakami and P Wierts (2026): "From cash to crypto: towards a consistent regulatory approach to illicit payments", *BIS Working Papers*, no 166.

Noether, S and A Mackenzie (2016): "Ring confidential transactions", *Ledger*, vol 1.

(OECD) Organisation for Economic Co-operation and Development (2023): *Central bank digital currencies (CBDCs) and democratic values*, OECD Business and Finance Policy Papers.

Pérez-Solà, C, S Delgado-Segura, G Navarro-Arribas and J Herrera-Joancomartí (2019): "Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies", *Royal Society Open Science*, vol 6, no 1.

Shor, P (1994): "Algorithms for quantum computation: discrete logarithms and factoring", in *Proceedings 35th annual symposium on foundations of computer science*, IEEE

Annex A Data access matrix

Based on the privacy threats, the roles and responsibilities in the payment ecosystem and assumptions about the business characteristics of digital payments today, we created the access matrix below for the Aurum Phase 2 privacy-preserving system for digital cash. It illustrates the ability of PETs to minimise data exposure to a centralised payment system and intermediaries, while maintaining usability and compliance controls. The matrix is for illustrative purposes and the accessibility is subject to policy, legal and regulatory considerations in different jurisdictions.

The entities listed in the rows represent the data processors responsible for collecting, storing and processing the data. The columns specify the types of data involved. The notation “D” (for default) indicates that the corresponding entity requires access to the data by default for operational purposes. The notation “O” (for optional) signifies that the information may be shared voluntarily by users. A dash (“-”) denotes that the entity will not have access to the data, thus minimising data exposure.

Table A.1 Data access matrix

Table A.1

Transaction data involved								
Entities in digital cash system	Payer PSD	Payee PSD	Payer's legal identity	Payee's legal identity	Payer's balance	Payee's balance	Amount	Additional transaction data (eg transaction note)
System operator (eg central bank)	-	-	-	-	-	-	-	-
System validator	-	D	-	-	-	-	-	-
Payer's bank	D	D	D	O	D	-	D	D
Payee's bank	-	D	O	D	-	D	D	D
Other bank	-	-	-	-	-	-	-	-
Payer	D	D	D	O	D	-	D	D
Payee	-	D	O	D	-	D	D	D
Other user	-	-	-	-	-	-	-	-
Compliance authority	-	-	-	-	-	-	-	-

Compliance authority does not have direct access to the retail ledger by default. PSD stands for pseudonym.

We highlight improvements in the data access matrix compared with other payment rails:

- **Payee and payer can remain anonymous to each other.** No identifiable data including account number or name need to be shared between payee and payer to make the payment.
- **Reduce exposure of payer identities to payee bank.** As shown in the diagram, the payee bank cannot access the payer identities and it cannot access its pseudonym either. The payee bank only gets a validated acknowledgement of payment received from another bank, without knowing any form of identifier that may link to the payer identity.
- **The payment amount is hidden from the validator.** The payment value is in encrypted form; therefore, the validator only knows that some tokens are transferred from one bank to another bank. Not seeing the payment amount can effectively prevent the validator from correlating or tracing payment transactions by a unique payment amount.
- **The validator can maintain payment integrity without touching real data.** Each party should only store and process data that are necessary or required for its operations in a payment system. For example, the validator only ensures the integrity of a payment between a payer and payee but is not tasked with storing their PII and transaction data.
- **More resistant to collusion risk.** In addition to the privacy threat from a single party in the ecosystem, we also try to address collusion risk with two categories of entities. For example, a merchant payee could collude with the system validator to extract personal data. To eliminate this risk, the design minimises data types and volume to be stored in a single party and reduces the overlapping data types to prevent linking through a common data field.

Annex B Technical details on PETs adopted

The following section describes how the privacy features in the prototype are implemented using PETs. While the main report focuses on the policy considerations and functional outcomes, this annex provides a technical overview of the underlying design and cryptographic mechanisms for readers seeking a deeper understanding of the implementation.

1. BBS+ signatures

BBS signatures were initially proposed by Boneh, Boyen and Shacham.²⁰ Subsequently, Au, Susilo and Mu presented the first, provably secure version of BBS signatures²¹ (BBS+ signatures), which improve the efficiency of ZKPs for anonymous credentials. BBS+ signatures are being standardised by the W3C Verifiable Credentials Working Group.²²

BBS+ signatures allow “selective disclosure”, meaning a signer can sign multiple messages and produce a single constant-size output signature. A prover, possessing the messages and the signature, can generate a proof in which they can choose which messages to disclose, while revealing no information about the undisclosed messages. The proof itself guarantees the integrity and authenticity (signed by the signer) of the disclosed messages. In practical applications, this makes BBS+ signatures ideal for privacy-preserving authentication systems, especially in environments in which users must prove their legitimacy without revealing unnecessary information.

What does a BBS+ signature do?

A BBS+ signature is a type of digital signature that supports selective disclosure. It allows someone to prove that part of their information is true, without showing everything. Imagine your identity card is digitally signed by the government, instead of handing over the whole card, you could use a BBS+ signature to prove just your age while keeping your name, address or other details private. The organisation checking your proof can then verify it against the government’s public key, without ever needing to see the hidden information.

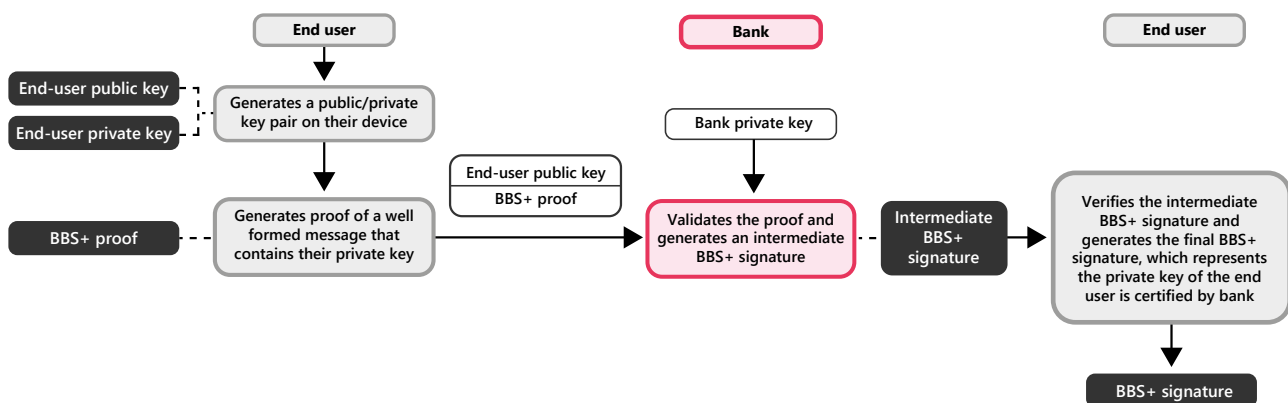
20. Boneh et al (2004).

21. Au et al (2006).

22. Looker et al (2023).

We incorporate the generation of privacy-preserving proofs for the BBS+ signatures process into the pseudonym creation mechanism. This allows end users to show that their public key has been certified by a bank, without exposing the public key itself. The certified key then forms the basis for generating cryptographically verifiable constructs used throughout the system, including pseudonyms (explained in the next subsection), while also enabling the bank to retrieve the real identity associated with a given pseudonym when necessary.

Graph B.1



A pseudonym is a data token with a combination of random numbers and letters, which is a non-sensitive replacement for sensitive information such as personal identity and bank account number. The replacement can be reversible or irreversible, which means that the actual identity information can or cannot be retrieved from the pseudonym depending on the actual implementation. The hidden nature of the actual identity information is essential in the Project Aurum Phase 2 setting in which the payer or payee does not want their identity to be revealed in transactions.

23. Noether and Mackenzie (2016).

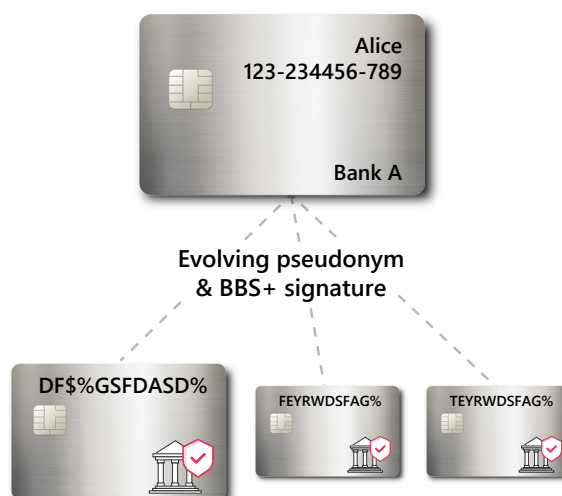
What does a pseudonym do?

A pseudonym is a string of random characters that represent a user. It is commonly used in blockchain technologies. Instead of directly using the account number or name, the user can be represented by the pseudonym in the ledger. In this way, the ledger owner knows someone is involved in certain actions without knowing who the person is. However, pseudonymity alone is not sufficient to protect user privacy. If the mapping between pseudonym and user identity is divulged, the whole series of actions involved with the users are also leaked.

In Project Aurum Phase 2, the end user, as a prover, can generate multiple pseudonyms based on a BBS+ signature issued by the bank. Each pseudonym is derived from the end user's certified public key, without revealing the public key itself. During the pseudonym creation, the end user produces a proof of possession of a valid BBS+ signature on their public key. This proof convinces any verifier that the pseudonym originates from a public key that has been certified by a bank, while keeping both the public key and the BBS+ signature hidden. As a result, the pseudonym acts as an anonymous credential, cryptographically attesting to the end user's legitimacy without disclosing their identity. The pseudonym is exchanged between payer and payee in the form of a QR code.

Indeed, we propose the use of evolving pseudonymisation for end user (ie payer and payee) identities, in terms of public keys, to protect identity privacy. Evolving pseudonymisation is a privacy-preserving technique in which a user's pseudonym changes over time or across different interactions, while still allowing the system to link actions made by the same user if necessary.

After the end user obtains a BBS+ signature from the bank, they can create different pseudonyms for sending and receiving money. To generate a pseudonym, the user uses their private key, the BBS+ signature issued by the bank and other parameters. The result is a pseudonym that functions as a temporary public key. This pseudonym includes a proof derived from the BBS+ signature, demonstrating that it is linked to a legitimate, bank-verified public key. Other parties can verify the validity of this pseudonym using the bank's public key, without learning the actual identity of the user.



3. Zero-knowledge proofs

Transaction unlinkability cannot be guaranteed if only pseudonymisation is implemented in digital cash systems. On the one hand, if an end user utilises the same pseudonym for more than one transaction, parties who have access to transaction data will be able to determine that these transactions originated from or are designated to a particular end user. Moreover, even if an end user generates and uses new pseudonym(s) for each transaction, these transactions can still be linkable because a pseudonym used to receive funds from a transaction, say A, will be used to pay funds in another transaction, say B. The same pseudonym appears in the transaction information relating to A and B, and thus A and B can be linked. Subsequently, a transaction graph can be constructed by an entity (eg a validator) that processes transactions, even though it may be assumed that it does not have knowledge of this information. Such tracking methods have been prevalent on public blockchains.²⁴

A ZKP²⁵ is effective in ensuring transaction unlinkability. It aims to provide a proof that a statement is true without giving away information beyond the fact that the statement is true. For example, a statement may read: "The input sum, which is encrypted, is sufficient for this payment transaction." In digital cash systems, a ZKP can hide the information, including the payer's pseudonym and the payment amount, from verifiers, while verifiers can still be convinced that the hidden information is valid for a legitimate transaction.

24. BISIH et al (2023).

25. Blum et al (2019).

What is a ZKP?

A ZKP is a form of cryptographic technology that can be used to prove knowledge of a secret without needing to share the secret.²⁶ By way of analogy, a user can prove his knowledge of the path out of the maze without showing the explicit route. ZKP is a cryptographic method to achieve this objective.

By encrypting coin IDs, the coin identity can be hidden and therefore cannot be tracked. In Aurum Phase 2, one of our core objectives is to enable transaction unlinkability, ensuring that a validator cannot trace or connect multiple transactions back to the same user (the payer). When the payer initiates a transaction involving several coins, the payer's bank encrypts the coin ID(s), unique identifiers for each coin, before including them in the transaction, concealing both the source and value of the coins. By doing so, transaction privacy is achieved as a result of the following two properties:

- The validator does not learn which coins are being used.
- The payer does not need to disclose any details about the input coins, such as their values or associated pseudonyms.

While preserving privacy, the payer is obliged to prove the input coin is authentic to ensure payment integrity. To enforce this, we use a ZKP. The payer and the payer's bank generate a ZKP that allows the validator to verify the transaction is valid, without learning anything about the coins or the payer. The ZKP proves the following:

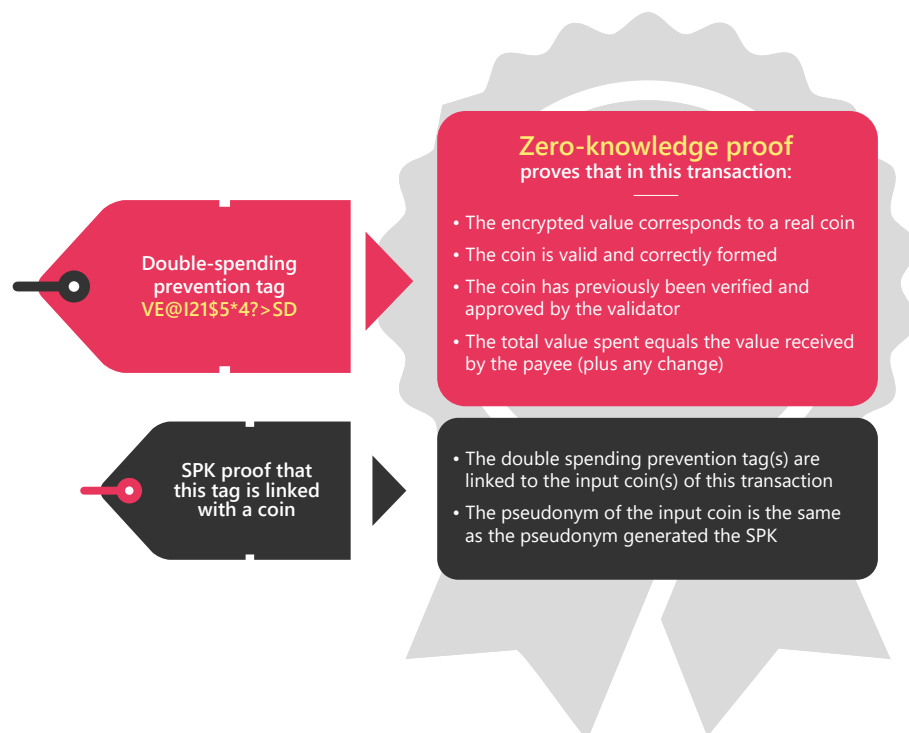
- Each encrypted coin ID corresponds to a real, existing coin.
- The output coin(s) created in the transaction is valid and correctly formed.
- The input coin was previously verified and approved by the validator.
- The total value spent equals the value received by the payee (plus any change).
- The double-spending prevention tag(s) are linked to the input coin(s) of this transaction.
- The pseudonym of the input coin(s) is the same as the pseudonym generated by the signature proof of knowledge (SPK), confirming the tag was generated by the payer.

26. www.youtube.com/watch?v=fOGdb1CTu5c.

To prove the input coin is unspent without revealing the coin identity, the system uses double-spending prevention tags. Each tag is uniquely tied to a coin, allowing the validator to check whether a coin has already been spent, without learning anything else about the coin or the payer. At the same time, the ZKP assures the validator that the sum of the input coin value is equal to the sum of output coin values (including any change). This verification is done without revealing the actual amounts, preserving both privacy and transaction integrity.

Attestations guaranteed by ZKPs

Graph B.3

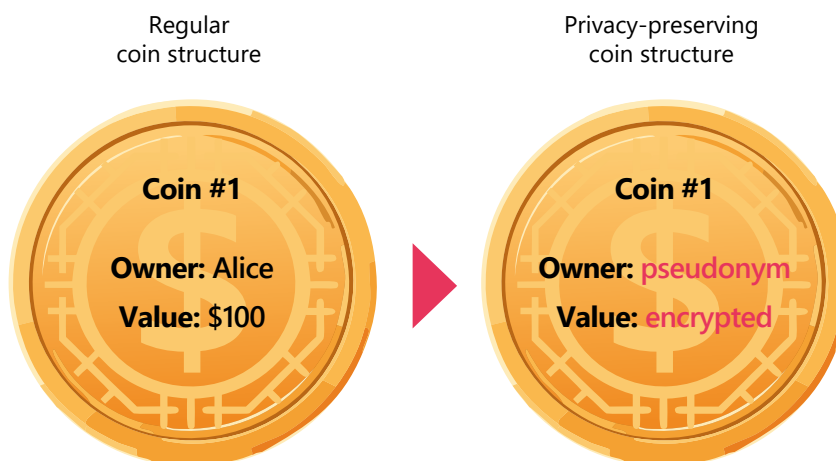


4. Privacy-preserving coin structure

In Project Aurum Phase 2, we adopt a token-based approach and define digital cash as a coin. Each coin represents a monetary value and is owned by an end user or a bank. Each coin is identified by a unique coin ID.

Illustration of the privacy-preserving coin structure

Graph B.4



To protect user privacy while maintaining verifiable ownership, each coin embeds the owner's identity in the form of a pseudonym and its value is encrypted using the coin owner bank's public key. Other than the coin owner, only the coin owner's bank has access to the identity of the coin holder and to the value of the coin. Neither validators nor any other third parties can access or infer the ownership or monetary value associated with the coin.

What makes our coin design unique?

The coin structure preserves the integrity of the UTXO design and lifecycle, and further improves privacy. The face value is encrypted. By doing so, other than the coin owner and the coin owner's bank, no one knows the coin owner's identity or the face value of the coin. Without knowing the payment amount, the validator can ensure payment integrity through verifying the ZKP generated by the payer and their bank, proving that the sum paid by the payer is always equal to the sum received by the payee. The payee receives a new coin and has no knowledge about the previous coin spent by the payer. This decouples transactions that would otherwise be associated through shared account identifiers and enhances privacy in interbank payments.

5. Unique double-spending prevention tag & signature proof of knowledge mechanism

To spend a coin, the payer does not disclose the coin detail directly to the validator. Instead, the payer generates a double-spending prevention tag ("the tag") and a corresponding cryptographic signature proof of knowledge (SPK). Both the tag and SPK are derived using the pseudonym's private key, which is securely generated from the payer's own key. The tag and SPK prove ownership of the coin without revealing the real identity of the owner.

The tag uniquely identifies a specific coin, but is designed so that no verifier, including the validator, can infer which coin the tag corresponds to. The SPK proves that the tag was generated by the coin owner. The payer's bank is not involved in the generation of the tag or the SPK and therefore does not require access to the payer's private key, ensuring that the payer retains the autonomy to spend the coin.

Once the SPK is verified, tags are used by the validator to detect double spending. Since each tag uniquely identifies a coin, the absence of the tag in the validator's database indicates that the coin has not been spent.

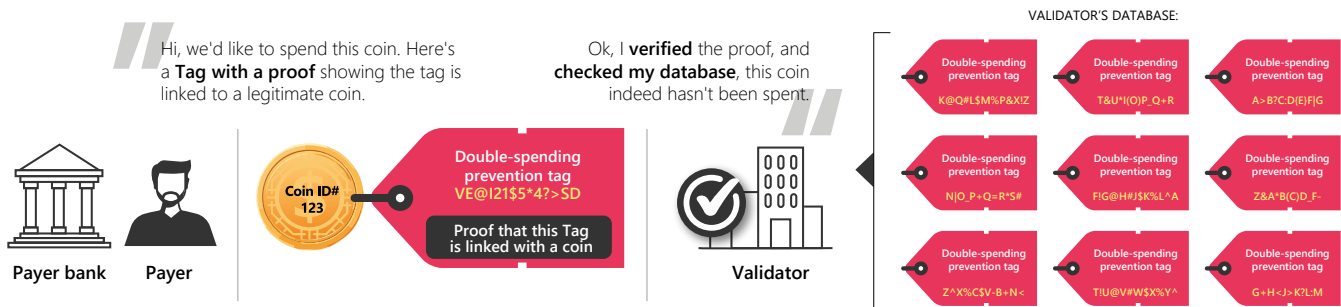
To effectively prevent double spending without sacrificing privacy, the tag generation must be strictly deterministic for the generating user while appearing entirely pseudo-random to the network. The tag uniquely identifies a specific coin, but is designed so that no verifier, including the validator, can infer which coin the tag corresponds to. Technically, the tag is generated from a set of fixed inputs, specifically the coin's randomness, the user's pseudonym, the user's private key and the bank's system parameters. Because this derivation is deterministic, any attempt to spend the same coin twice will always output the exact same tag, allowing validators to reliably detect duplicate spending attempts. At the same time, this cryptographic construction is strictly one way. The tag acts as a privacy-preserving identifier that reveals nothing about the underlying coin or the user's real identity. Furthermore, to prevent malicious forgery, the tag is cryptographically bound to the SPK. This ensures that the SPK mathematically proves the tag was correctly derived from a valid coin and the legitimate owner's private key, without exposing any underlying sensitive data to the network.

Why is the double-spending prevention tag needed in digital cash?

Settlement in physical cash is achieved when the payer pays cash to the payee without the ability to engage in double spending. A digital coin, on the other hand, can be copied into multiple credible copies unless double-spending controls are applied. The double-spending prevention tag enables the validator to determine whether a coin has already been spent before. Once a coin is spent, the validator records the tag in a database so that the same coin cannot be spent again. Payment finality is therefore achieved at the level of the validator. As part of the privacy by design of the Aurum Phase 2 prototype, this unique and novel tag minimises the coin details that the validator needs to know to achieve settlement finality.

Illustration of the double-spending prevention tag

Graph B.5



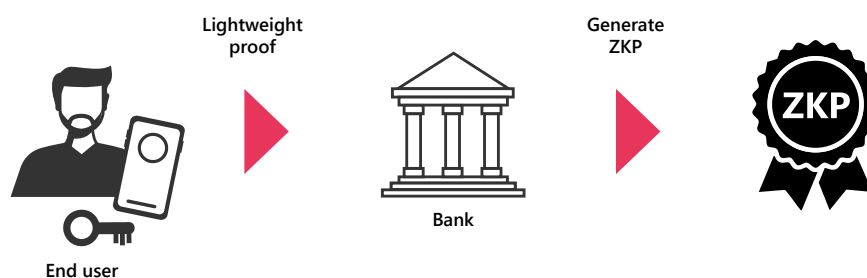
6. Two-step ZKP generation to enhance usability

While ZKPs offer strong privacy and verifiability, their implementation in payment systems faces practical constraints. Generating a full proof requires substantial computation power that can overwhelm smartphones, leading to slower transactions. Alternatively, letting banks handle proof generation would require access to users' private keys, which weakens end user privacy.

In Aurum Phase 2, we introduced a novel approach that splits ZKP generation into two steps, balancing security and usability. Payers keep full control of their private keys and only need to generate a lightweight proof on their own mobile devices. The banks then complete the process by handling the heavy computation required for full ZKP generation.

Two-step generation of ZKP

Graph B.6



The detailed steps are as follow:

- **Step 1:** the payer generates a **lightweight proof** of input coin ownership. Specifically, this lightweight proof consists of a double-spending prevention tag and a corresponding SPK bundle. When a payer initiates a transaction, their mobile device generates this tag and an SPK for each input coin. The SPK serves as a lightweight, elliptic curve-based ZKP demonstrating that the tag correctly identifies the input coin and was generated by the legitimate owner using the pseudonym's private key, without revealing the coin itself or the user's real identity. By isolating the computationally light task of creating the tag and SPK on the user's mobile application during the actual payment, the system efficiently delegates the heavy lifting of generating the full ZKP to the payer's bank in the next step.
- **Step 2:** the payer's bank generates a **full ZKP** on the transaction proposal. By taking the lightweight proof, the payer's bank confirms legitimate ownership of the input coin(s) and completes the full ZKP generation for the statements shown in Graph 7. This process adopts an arithmetic circuit-based zk-SNARK, which flexibly proves multiple verifiable computational statements within a single transaction while producing proofs that are both compact and easy to verify. As the full ZKP generation is computationally intensive, it is performed on the bank's secure infrastructure without compromising the user's control of their owned assets and privacy.

This approach significantly improves user experience by allowing fast and responsive interaction on lightweight devices such as smartphones, without compromising privacy or security. At the same time, offloading the heavy cryptographic computation to the bank ensures that the full ZKP can still be completed efficiently, making the system practical for real-world deployment without requiring users to have high-end hardware.

Annex C Transaction flow

1. Overall transaction flow

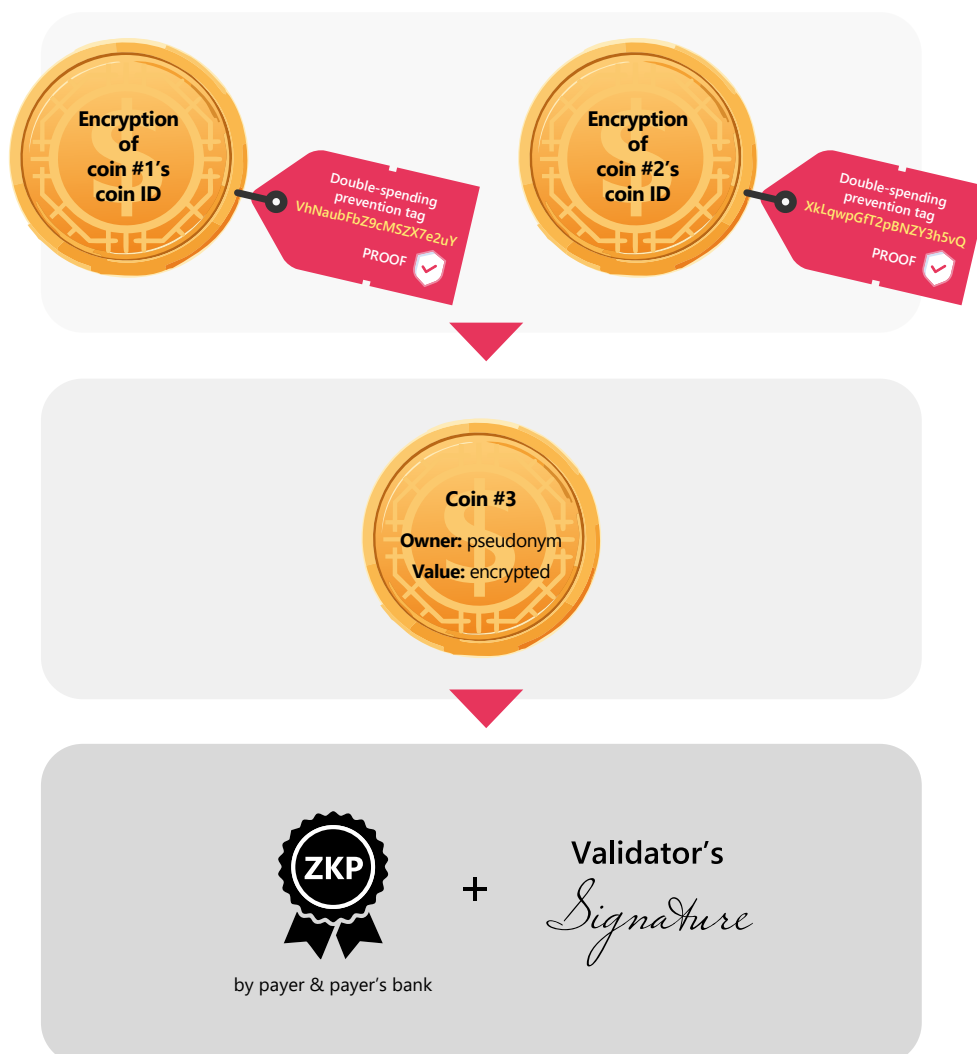
To preserve privacy while maintaining transaction integrity, our design ensures that all parties involved receive only the information necessary to perform their roles. The design discloses only the information each party needs to know according to the desired access matrix, using encryption, BBS+ signature scheme, pseudonym-based ownership and ZKPs to protect sensitive details such as coin ownership and transaction amounts. The below describes the standard transaction flow under this model:

- **Step 1:** to initiate a payment, the payer and the payer's bank jointly construct a transaction proposal, specifying the coins to be spent (input coins). For each input coin, the payer generates a tag and a cryptographic proof to demonstrate legitimate ownership without revealing the coin itself. The payer's bank then creates at least two output coins, typically one for the payee and, if applicable, another for the payer to receive any remaining balance (ie change). To preserve privacy, the coin ID of each input coin is encrypted. For output coins, the payee's or payer's pseudonym is used as appropriate and the monetary value is encrypted using the respective bank's public key, ensuring that only the intended recipient and their duly licensed FI can access the coin's value. The payer's bank then generates a ZKP to prove to the validator that the transaction is legitimate, that the input coin values equal the output coin values and that the transaction corresponds to the tag and SPK provided by the payer, the payer's bank generates a ZKP supporting the claim. The complete transaction proposal is then submitted to the validator for endorsement.
- **Step 2:** after verification of the transaction proposal, SPK and ZKP check that the same tag does not exist in its database, the validator creates a digital signature in the transaction proposal, after which the validator passes the endorsed transaction and output coin to the payee's bank.
- **Step 3:** the payee's bank verifies the transaction by checking the SPK, ZKP and the validator's signature. Once verified, it updates its internal ledger and forwards the output coin to the payee's wallet for verification and secure storage. The coin can then be spent by the payee in a future payment transaction.

To prevent malicious behaviour, such as constructing an incorrect set of change outputs, the system enforces transaction correctness through ZKPs and validator verification.

The endorsed transaction proposal

Graph C.1



2. Encrypted remarks message for bank communication

When submitting the transaction proposal, the payer's bank also provides an encrypted remarks message to the validator, who forwards it to the payee's bank. The remarks message allows the payer's bank to convey necessary information to the payee's bank, such as the payer's name or other optional compliance check details. The message is encrypted using a dedicated communication key, which is itself protected and can only be accessed using the payee bank's public key. To ensure message integrity, a hash of the encrypted message is included within the transaction proposal, allowing the payee's bank to verify the message upon receipt. Even the validator cannot access or view the contents of the encrypted remarks message.

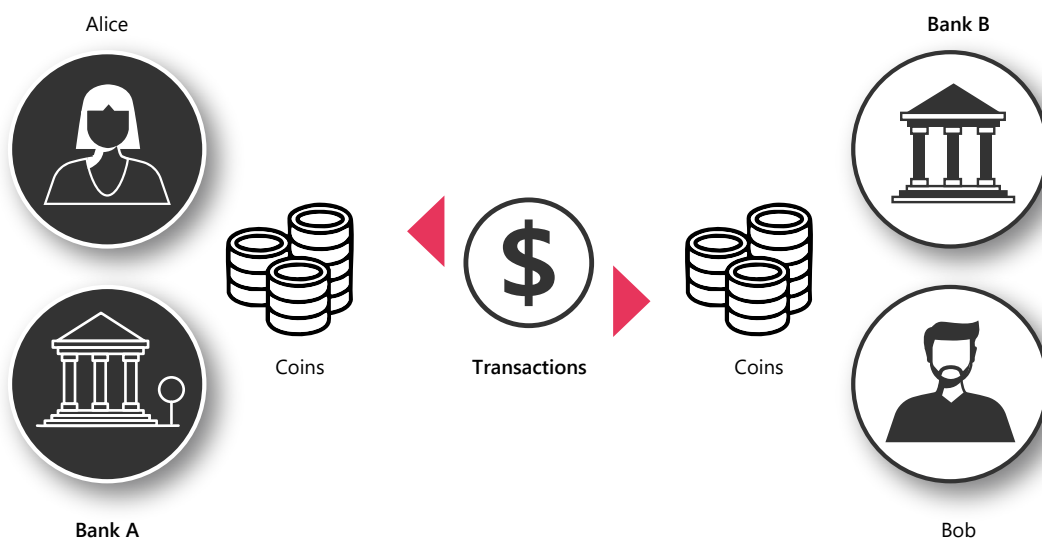
3. New coin scheme

In Project Aurum Phase 2, a new coin and transaction concept is used to enhance the UTXO model to hide complete transaction input and output amounts and their relationships from the validator. In the real world, people or banks make transactions with coins to form a payment. There are two major components, coin and transaction, for a new coin scheme.

As in Project Aurum Phase 1, a shared custodian account is implemented in the interbank system. It is managed by a DLT smart contract and is used to store tokenised reserves taken from banks as backing assets when such banks perform a digital cash distribution. When a bank requests the issuance of digital cash from the interbank system, the equivalent amount of tokenised reserve will be transferred from the bank's tokenised reserve account to the custodian account by the smart contract to be the backing asset. The reverse is done when the bank requests redemption of the digital cash. This arrangement ensures that every bit of digital cash is fully backed by wholesale central bank reserves, technologically proven and auditable.

Real-world payment example

Graph C.2

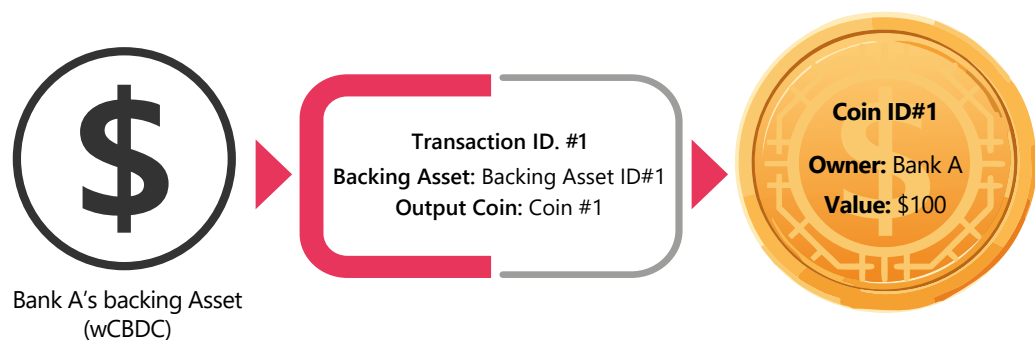


4. Coinbase transaction

Initially, the bank makes a coinbase transaction to request new coins through a distribution process using a backing asset, equivalent to the amount of wholesale central bank money in the interbank system. Each coin has its own ID, owner pseudonym and value. For the coinbase transaction, the input is the backing asset.

Whenever the validator has validated a coinbase transaction, it will add a record in its storage to store the backing asset ID and the transaction ID of the coinbase transaction. Whenever a validator is asked to validate a coinbase transaction, it will search its storage to determine whether the backing asset in the coinbase transaction has already been used in an earlier digital cash distribution to prevent double issuance. This ensures full auditability in the wholesale layer.

Coinbase transaction: new coin scheme for coin distribution by a bank Graph C.3



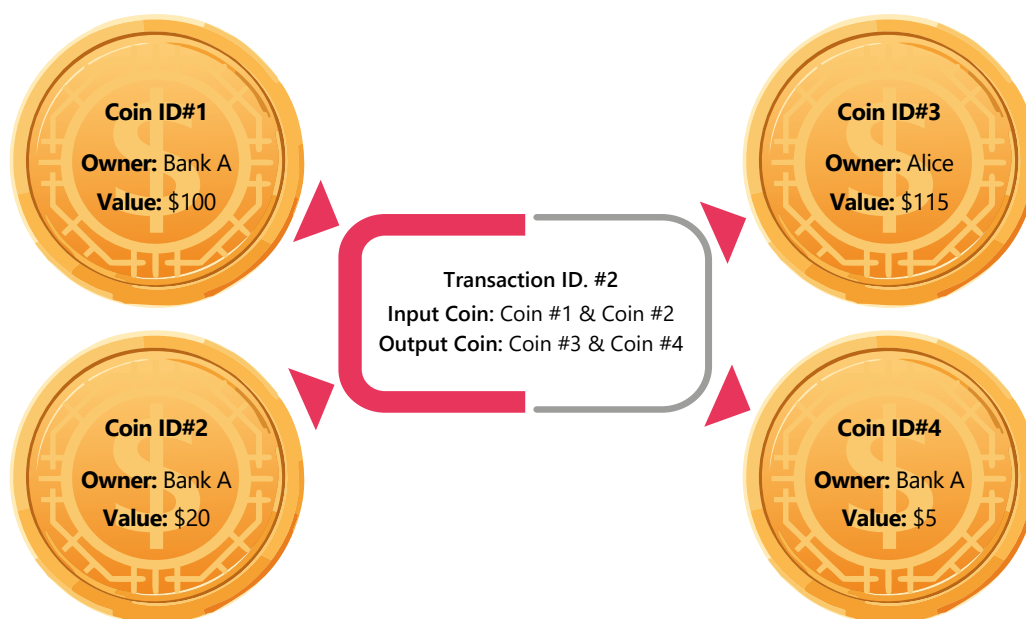
The coin IDs and coin values shown in this graph are for illustration purposes only. Both are encrypted within the actual transactions.

5. Regular transaction for payment

The bank has several coins, each with different values. The figure below shows a case where bank A transfers \$115 to Alice upon her request. The bank uses multiple coins to pool enough for Alice's requirement. The total input is \$120, resulting in a \$115 coin for Alice and a \$5 coin returned to the bank as change. Currently, bank A's coin #1 and coin #2 are marked as spent and will not be used again. Coin #3 and coin #4 are newly created for Alice and the change for bank A, respectively.

Illustration of a regular transaction (bank A pays Alice \$115)

Graph C.4



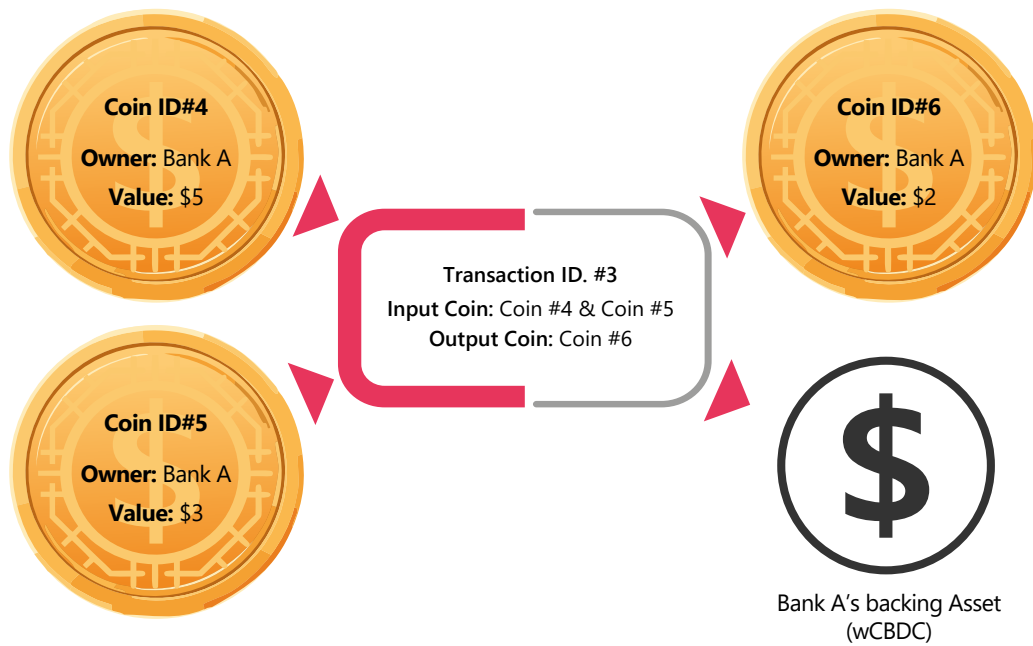
The coin IDs and coin values shown in this graph are for illustration purposes only. Both are encrypted within the actual transactions.

6. Redemption transaction

The bank intends to redeem \$6 to backing assets using their two coins, which have a combined value of \$8. The redemption transaction results in a new \$2 coin for bank A and the remaining amount becomes a backing asset.

Illustration of a redemption transaction where bank A redeems \$6

Graph C.5



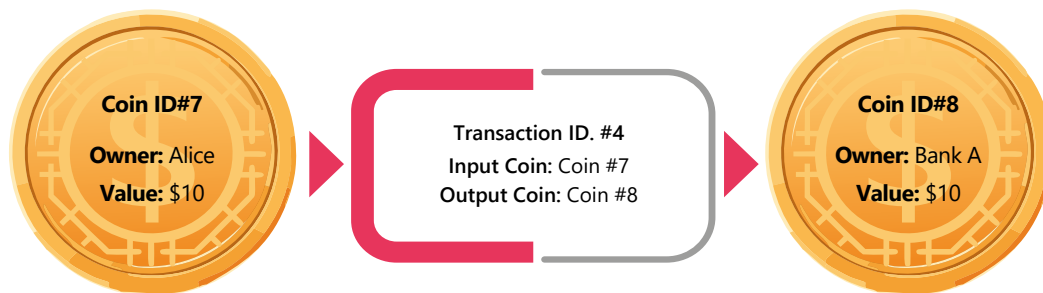
The remaining \$6 will be added to bank A's wholesale reserve balance.

7. Decree transaction

In normal times, each coin can only be moved by its owner. There are exceptional cases in which the coin will be transferred to a third party without the owner's key, eg confiscation of illegal financial gain ordered by a court. The system provides a special transaction type called decree transaction, to handle such exceptional cases. The transaction can only be triggered by the bank. It is expected that very strong controls in the form of administrative measures should be adopted to ensure they are not abused. This is aligned with existing compliance practices in the banking industry when it comes to confiscation of the proceeds of crime and the enforcement of sanctions obligations. Upon receiving a subpoena from the court, the bank intends to transfer the ownership of a \$10 coin from Alice back to bank A.

Illustration of a decree transaction

Graph C.6

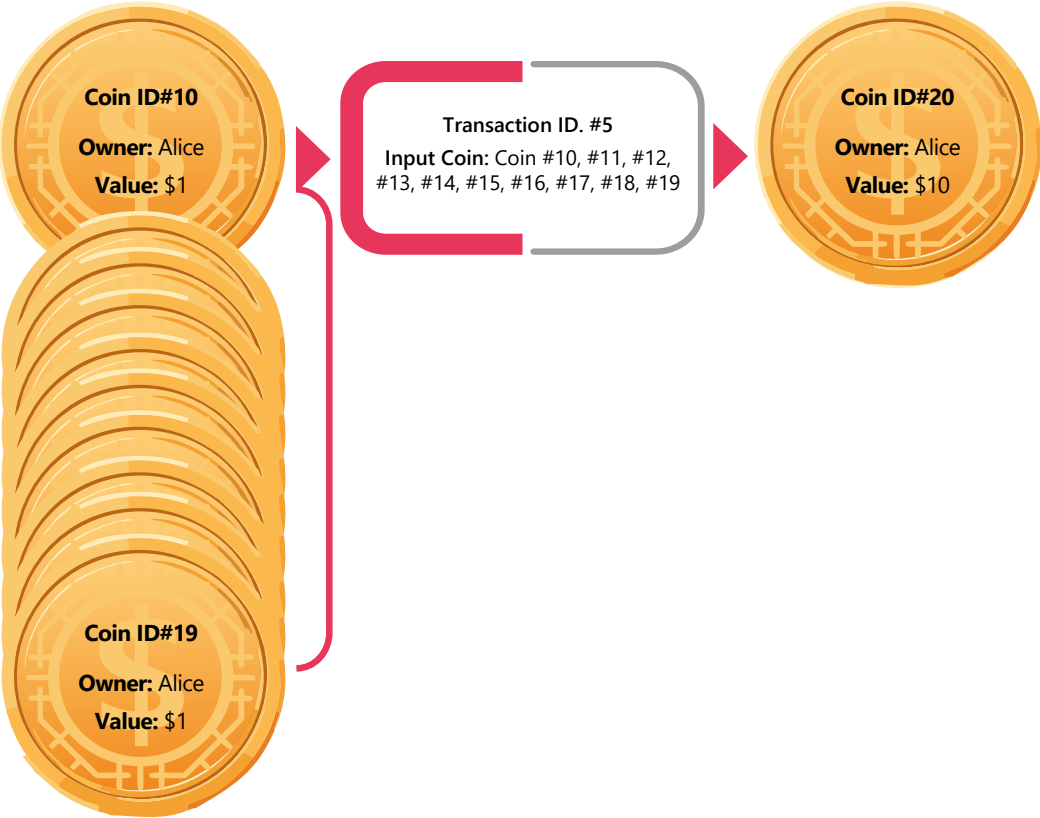


8. Batch transaction

A batch transaction is one in which an individual merges their unspent coins into a single new coin through their bank. It reduces the time required for validators to verify ZKPs associated with numerous small-value coins. This approach can reduce operational complexity and improve performance.

Illustration of a batch transaction

Graph C.7



Ten \$1 coins are merged into a \$10 coin for Alice

Annex D Performance

1. Pseudonym Size

The aim of pseudonymisation is to protect the identity of an end user from unwarranted third parties and to allow the end user's bank to recover the end user's identity from the pseudonym for AML and CFT legal and regulatory compliance purposes.

To achieve the above goals, in our implementation, a pseudonym consists of:

- Proof of certification of the end user's public key by their bank.
- Encryption of the end user's public key
- An initialisation vector (one-time unique value).

The Aurum Phase 2 pseudonym is around 2 KB and 1.5 KB after compression. For distribution for payment purposes, the end user can use any offline and online communication channels and storage media, and a pseudonym can also be fitted into a single QR code, which is a well adopted means for mobile payments nowadays. While a 12 MP smartphone camera (with autofocus and decent lighting) should handle the scanning easily, older mobile devices with a 5 MP camera might struggle to read the pseudonym from the QR code with low lighting. Although most mobile devices today are equipped with high-resolution cameras, there remains room for optimising the pseudonym size to support broader accessibility.

2. Cryptographic performance

Modern ZKP systems require converting statements to be proved by mathematical constraints and rely on computationally expensive cryptographic operations.

The more statements to be proven, the more constraints there are to generate a ZKP. In other words, the proof generation time increases if the amount of hidden information to be proven in a transaction increases.

A zk-SNARK²⁷ is a specific kind of ZKP in which the proof is succinct, meaning that the proof itself is short and can be verified by the verifier quickly. zk-SNARK is particularly suitable for digital cash systems in which the verifiers may have limited computational resources. For example, the payee may use their mobile phone to verify a ZKP for a transaction. It also reduces the validator's and payee bank's verification costs since the transaction volume is substantial for digital cash systems.

Despite fast verification time, the proof generation process is the major performance overhead in transaction generation. In Project Aurum Phase 2, the proof generation time for a single input coin is 2.86 seconds and it grows to 29 seconds for 20 input coins in a single transaction (Amazon Elastic Compute Cloud (g4dn.xlarge): 4 vCPU, 125 GB NVMe SSD, 16 GB RAM).

27. Groth (2016).

The Aurum Phase 2 design allows a very large number of input coins theoretically, but due to the fact that the time required for proof generation grows with an increasing number of input coins and the corresponding increase in size of the proof and verification keys, we set a limit that the payer may select up to 20 input coins in each transaction. This implementation approach still covers most cases of transactions in similar UTXO-based systems, which adopts a coin-based transaction model. For example, popular systems such as Bitcoin have an average of 2.12 UTXO/transaction while Litecoin has an average of 6.78 UTXO/transaction.²⁸

Hardware acceleration is essential to the performance improvement of ZKP proof generation because expensive cryptographic operations can be offloaded from a CPU to dedicated hardware components, eg a field-programmable gate array (FPGA), a reprogrammable chip that can be tailored for specific cryptographic tasks and a graphics processing unit (GPU), a processor designed to handle many calculations in parallel for faster computation.

The parallelism nature in cryptographic operations in ZKP generation is a perfect match for parallelisation capability in processing these hardware components. Due to the fact that GPUs are mass produced and widely distributed in consumer electronics, gaming PCs and data centres, there is better software support in the community, while field-programmable gate array (FPGAs) are produced in more specialised, low-volume settings, such that ZKP acceleration with GPU is one of the dominant trends in the ecosystem (eg Filecoin).²⁹

In Project Aurum Phase 2, GPU acceleration can be made possible by adopting Ingonyama's ICICLE library,³⁰ which offloads some operations to the GPU to boost ZKP generation performance. The testing platform in AWS is also equipped with NVIDIA Tesla T4 GPU (RTX 20 series). As a result, the proof generation time for a single input coin improved to 0.4 seconds (7.15 times faster) and 1.76 seconds (16.48 times faster) for 20 input coins in a single transaction. With GPU acceleration, the restriction on the maximum number of input coins can be relaxed so that it can provide better privacy protection to batch processing transactions (to be discussed in the next section) with acceptable performance.

3. Batch processing

Given that the cryptographic operations are expensive, we propose a batch transaction option to strike a balance between performance and privacy level. The higher privacy level of a regular transaction comes at the expense of performance. If the validator is a trustworthy party that does not collude with other parties, payments can be more efficient, while maintaining reasonable privacy with regard to intermediaries and threat actors in the ecosystem.

28. Pérez-Solà et al (2019).

29. lotus.filecoin.io/storage-providers/get-started/hardware-requirements.

30. dev.ingonyama.com.

As an inherent limitation in UTXO systems, frequent small payments may bring about fragmentation of coins and impede performance. End users may receive a substantial number of coins frequently. For example, a retail shop that sells small monetary value items receives coins from its customers daily. The shop may want to “combine” the coins into a single coin. However, because the number of input coins may be substantial (hundreds of coins or more), proof generation will be comparatively slower than a regular payment transaction (approximately 2–6 coins), resulting in inefficiencies. We, therefore, introduce an optional “batch transaction” with relaxed privacy protection, which allows the end user to reveal the coins to be spent to the validator. This type of transaction requires no arithmetic-circuit type of ZKP proof generation, which is much faster but comes at the expense of “pseudonym linkability.”

The nature of a batch transaction implies that all input coins belong to a single identity, allowing the validator to logically link each batch input coin back to the immediate prior transaction that originally generated it. However, this retroactive graph inference is strictly confined to a single backward hop and does not completely degrade the unlinkability guarantees of the broader system. As the inputs of those prior regular transactions are securely hidden by the end users’ evolving pseudonyms and ZKPs, the validator cannot resolve or trace the lineage of the funds beyond this immediate layer. As a result, the actual identities of the end user and previous owners remain completely unrevealed and the resulting transaction graph remains shallow and localised.

The design of Project Aurum Phase 2 allows flexibility for the end user in the choice of the desired privacy level for a batch transaction. Besides the relaxed privacy approach introduced in the previous paragraph, the end user can combine coins using regular transaction(s). “Pseudonym linkability” can be avoided due to the security properties provided by regular transactions.

In sum, batch processing can improve operational efficiency but does so at the cost of reduced privacy, as it introduces partial transactional linkability by the validator.

Compared with Project Aurum Phase 1, the introduction of ZKP mechanisms in Phase 2 increases transaction latency. In particular, ZKP generation during coin requests and regular payments constitutes the primary source of processing overhead. Additional verification steps, including pseudonym validation, SPK verification and output coin checks, further contribute to overall transaction time.

Annex E Resilience to privacy risks

1. Pseudonym Size

The Project Aurum Phase 2 project team conducted a self-assessment on privacy protection by comparing the access matrix against the linking and profiling risks. The design effectively reduces the linking and profiling threat to the payer's identity and the payment transaction.

Privacy level

Table E.1

Privacy setting	Linking/profiling																				
	Govern-ment			Central bank			Validator			Payer's bank			Payee's bank			Payee			Any other third party		
	I	T	H	I	T	H	I	T	H	I	T	H	I	T	H	I	T	H	I	T	H
KYC verified wallet	2	2	2	2	2	2	3	3	3	1	1	1	3	3	3	3	3	3	3	3	3
Anonymous wallet	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

Notation:

H = holding; *I* = identity; *T* = transaction.

Scale:

1. Low privacy, easy to know.
2. Medium privacy, difficult but still possible to know.
3. High privacy, not visible under the prototype design.



Bank for International Settlements (BIS)

ISBN 978-92-9259-986-7