WHITE PAPER

Revolutionizing Cross-Border Transactions with Permissioned DeFi

CO-AUTHORED WITH

BCG

Fireblocks

Revolutionizing Cross-Border Transactions with Permissioned DeFi

This article was produced in collaboration with BCG.

Cross-border payments make up a vast and often inefficient movement of money around the world. In 2021 alone, some $1.2 trillion in payments crisscrossed the globe. Among the challenges is that these transactions result in significant expenses for both financial institutions and users. Though the system has improved over the years, it remains far from perfect, and payers and payees would welcome a new way of cross-border payment.

A combination of digital assets and permissioned, decentralized finance (DeFi)—a blockchain-based financial technology—may finally support a cross-border payment system that is faster, cheaper, and more verifiable.

This article, coauthored by BCG and Fireblocks, a digital asset security platform, proposes a hypothetical payment model based on permissioned DeFi. For end users who make and take payments, the model offers more flexibility. For institutions that build this model, Know Your Customer (KYC) verification provides more control over payments. We estimate that the average transaction cost in the new model will be 60%–80% cheaper than the cost incurred by traditional models.

Understanding how this new model works and the assets that firms need to participate is key to realizing its potential.

Table of Contents

How a Permissioned DeFi-Based Model for Cross-Border Payments Works

You may already be familiar with a cross-border payments model based on permissionless DeFi. Permissionless DeFi offers advantages over traditional payments, but it also carries risks. (See Appendix A: The Limitations of Traditional Payments and Permissionless DeFi) One of its benefits is the ability to execute a near-instant transfer of actual value across borders. Additional benefits of permissionless DeFi include better traceability (transactions are logged on the blockchain), more user control over their assets, and the ability to interact directly with each other. However, permissionless DeFi transactions are left exposed by insufficient anti-money laundering (AML) and KYC functions, opening the way for fraud and erroneous payments. These weaknesses are why institutions have been reluctant to adopt the technology at scale.

Permissioned DeFi addresses these concerns by combining the efficiencies of the permissionless model with the required risk and compliance controls to offer significant advantages over traditional payments. In the cross-border payment context, these verification functions would help businesses face some of the endless challenges of managing financial risk.

The process for an end user to send a cross-border payment through permissioned DeFi goes through several steps.

Prior to the on-chain transaction, institutions X and Y undergo a KYC process that meets a platform-level KYC standard, conducted by whitelisters, a group that approves users. (See Exhibit A.) The whitelister adds their wallets (digital wallets A, B, C, and D, respectively) to the allowed list.

Institutions X and Y could either act as whitelisters or appoint third parties to manage whitelisting. Other market participants, such as liquidity providers and arbitrageurs, go through a KYC process with the whitelisters.

The next steps are as follows:

1. A sender triggers a cross-border fiat money transfer.

Once a sender has been successfully KYC-approved, the sender can initiate a cross-border transaction. The sender can be an individual, a business, or an institution.

2. An on-ramp instruction is sent to an on- and off-ramp service provider (OOSP).

OOSPs act as entry and exit points for funds moving from the traditional fiat financial system to a token-based model. The OOSP debits the sender's fiat balance and credits the sender's digital wallet with the amount of a specific type of token worth the same value as the fiat amount.

This model can use various types of tokens. These digital assets are tied to the value of a corresponding fiat currency and act as the transaction's main payment format. In short, these assets are the money that changes hands during the payment. Examples include bank-issued stablecoins and central bank digital currencies (CBDCs). (**See** Appendix B: Stablecoins, Tokenized Deposits, and Central Bank Digital Currencies)

3. After the token is received in the digital wallet, it must be wrapped by a service provider into a token accepted by the permissioned DeFi model.

Wrapping is a crucial step to enable interoperability across various blockchains. A wrapped token represents a different token existing on another blockchain with equal value.

In the wrapping process, the wrapping platform locks the initial token in the smart contract and mints the same amount of the corresponding wrapped token. Before the wrapped token wallet can accept the token, a whitelister must check that the wallets involved in the transaction are KYC-approved and whitelisted to allow the transaction.

The smart contract then queries the on-chain/off-chain list of approved wallets with the whitelister(s) and confirms wallet B's approval.

4. The smart contract deployed on the permissioned DeFi protocol handles the transfer of the wrapped token to the receiver side.

This permissioned DeFi model uses an automated market maker (AMM), which are smart contracts that provide a pool of tokens, or a liquidity pool, to determine prices and facilitate trades. Examples of AMMs include Uniswap.

These assets are critical to the speed and stability of permissioned DeFi. AMM smart contracts enable an atomic swap between the two different tokens, ensuring near-instant settlement. Blockchain and the DeFi protocols built on top of them run 24/7, avoiding issues with settlement risk and fluctuations in traditional foreign exchange during market hours.

As shown in the exhibit in step 4:

- The tokenized US dollars are transferred through wallet B to the liquidity pool.
- The swap function is executed with wallet B as the sender address and wallet C as the recipient address.
- The AMM smart contract then transfers the tokenized euro to wallet C.

5. Receivers can use the token on another blockchain network.

They must unwrap the received wrapped token through an unwrapping platform. This sends the unwrapped token to the receiver’s digital wallet.

6. If the receiver prefers to receive fiat currency, the optional off-ramp or burning step will then be applied, depending on token type, to receive the fiat currency.

This would entail burning the token and crediting of the corresponding value of fiat to the receiver’s bank account.

As the slideshow shows, a number of entities must participate in this cross-border payment model for full effectiveness.

Quantifying the Cost Savings of Permissioned DeFi for Cross-Border Payments

This model offers both payment service providers and end customers considerable potential savings.

Payment providers must account for operational, IT expenses, and compliance costs.

Traditional Payments

The authors have estimated that traditional payment costs reach an average of $8 per transaction for payment service providers like banks. About 80% is related to operational and IT costs—or roughly $6.40. Compliance-related efforts account for about 15%–20% of the $8 of the traditional payment, amounting to approximately $1.20 to $1.60 per transaction.

Permissioned DeFi-Based Payments

For payment service providers using the permissioned model, the combined estimated operational and IT costs per transaction range between $0.05 and $0.09—far less than the $6.40 estimate.

Assuming that compliance costs for a permissioned transaction will be the same as for a traditional payment, the total estimated transaction cost in the permissioned model is $1.25 to $1.69—roughly 80% less expensive than the base cost of a traditional transaction (if the fee structure is in absolute amounts).

The cost-effectiveness of this solution lets financial institutions offer competitive prices, making it possible to charge lower fees compared to traditional models, reaching as low as a fraction of a percent.

Key Considerations for Implementation

Businesses planning to set up or participate in a permissioned DeFi-based model for cross-border payments should keep in mind the following considerations.

SPEED Permissioned DeFi-based payment models can settle transactions rapidly, while wrapping and unwrapping tokens may take a few minutes (depending on the blockchains used in the model). Foreign exchange conducted on smart contracts can occur almost instantly.

Processing duration varies depending on the platform, the type of tokens involved, and the network status. If users exchange within the network, the transaction will be instant. It can take up to an hour if the payment goes from the traditional fiat financial system through the permissioned DeFi-based model.

SMART CONTRACT RISK There may be flaws in the smart contract code that handles the wrapping and unwrapping of tokens. This could allow for vulnerabilities that result in loss or theft of funds or assets. Extensive auditing and testing can lower the risks of coding errors.

WALLET SECURITY User wallets that interface with smart contracts to wrap and unwrap tokens must be highly secure. Be mindful that any wallet vulnerability could expose the keys that control assets and allow theft or loss of funds.

TECH DEVELOPMENT Companies can join ecosystems to access various robust verification and operational capabilities required. For example, an ecosystem can provide robust identity management systems essential for transactions on the blockchain.

CAPITAL EFFICIENCY Transactions in DeFi are always gross settlement transactions, meaning each transaction is executed individually. Netting of different transactions with each user in the network is not possible.

GOVERNANCE DESIGN A well-conceived governance model, overseen by a consortium of stakeholders, provides a clear decision-making framework to ensure transparency, fairness, and accountability for the parties involved. Rules will guide conflict resolution and dispute management.

REGULATION As regulation around financial technology, data privacy, and related issues continuously evolves across jurisdictions, adopters should stay prepared to adjust their payment model to comply if and when regulation addresses permissioned DeFi-based models.

Implementation of this model must include integration into existing payment systems through gateways and the creation of related messaging around payment instructions. However, as these setups vary widely, we will not discuss these details in this paper.

Implementing the Model

As business leaders seek to establish a permissioned DeFi-based cross-border payments model, below are a few actions to consider at the onset.

Scope out requirements and key objectives and seek out the necessary infrastructure required.

These necessary elements include custody wallets for participants in the transaction; AML/KYT services can screen for illicit transactions from compromised wallets. Analytics services can track the movement of all circulating tokens.

Ensure interoperability with existing payment infrastructure.

Financial institutions and senders should integrate the model with their existing orchestration layers and connect to existing messaging layers like SWIFT.

Engage industry coalitions, competitors, regulators, and consumer advocacy groups.

Awareness of permissioned DeFi will only grow if adopters inform their ecosystems of the advantages and workings of the model. Finding consensus on functional requirements and standardized processes should be the aim of participants in these payment models.

Permissioned DeFi offers several benefits in the cross-border payment context including lower transaction costs, more accurate foreign exchange conversion, stronger security, and faster transaction times. Due to the greater transparency and efficiency inherent to a permissioned DeFi model, anyone from small financial institutions to multinational banks can transact with any other KYC-approved counterparty around the world—an important step toward a more efficient global financial system.

APPENDIX A

Limitations of Traditional Payments and Permissionless Decentralized Finance

Traditional cross-border payments rely on several actors adding their services to what, on the surface, looks like a simple exchange between payer and payee. Unfortunately, this process can take several days, incurring fees for the payer and payee at each step until the payee finally receives the payment.

For instance, when a sender pays US dollars to a receiver who prefers Japanese yen, the sending bank and receiving bank bookend the transaction. The sending bank typically confirms the transaction path in a corresponding banking network. Foreign exchange operations convert the fiat currencies from one to another.

While these limitations slow down payments, a permissioned DeFi model for cross-border transactions is much faster and more transparent. **(See Exhibit B.)**

Permissionless DeFi carries several risks that emerge both in cross-border payment and broader financial use cases.

LACK OF REGULATION At the time of this report, DeFi is not regulated by traditional financial regulators, which exposes investors to various risks like fraud, market manipulation, money laundering, and terrorist financing.

SECURITY RISKS DeFi platforms are vulnerable to cyberattacks, and smart contracts sometimes contain bugs or vulnerabilities that hackers can exploit for their gain.

LIQUIDITY/MARKET RISKS The relative lack of liquidity in DeFi markets can result in price volatility and sudden losses for investors.

CUSTODY AND OPERATIONAL CHALLENGES Users have full control and custody over their assets in wallets, which means they are responsible for storing, securing, and managing their assets themselves. They will also need to manage these wallets to access DeFi protocols, which can limit accessibility for users who are not adequately equipped with sufficient services and knowledge.

SCALABILITY DeFi protocols are built on blockchain networks that can be slow and expensive to use, particularly during periods of high network congestion.

APPENDIX B

Stablecoins, Tokenized Deposits, and Central Bank Digital Currencies

A permissioned model achieves stronger verification in part through stablecoins and central bank digital currencies (CBDCs). These tokens have an inherent level of Know Your Customer KYC) verification applied. The following list of tokens explains the uses and functions of each. (See the exhibit.)

AUTHORS

Sagar Sarbhai
Global Head, Business Solutions and Advisory
Fireblocks

Douglas Hsu
Research Lead, Business Solutions and Advisory
Fireblocks

Adam Hart
Director of Strategic Alliances
Fireblocks

Kaj Burchardi
Head of BCG Platinion Netherlands
BCG

Bihao Song
Principal IT Architect, BCG Platinion
BCG

Stefan Wang
IT Consultant, BCG Platinion
BCG

The authors would like to thank Nikolai Pomortsev for his contribution to this article.

Fireblocks

About Fireblocks

Fireblocks is an enterprise-grade platform delivering a secure infrastructure for moving, storing, and issuing digital assets. Fireblocks enables exchanges, custodians, banks, trading desks, and hedge funds to securely scale digital asset operations through patent-pending SGX & MPC technology. They have secured the transfer of over $4 trillion in digital assets and have a unique insurance policy that covers assets in storage & in transit.

For more information, please visit www.fireblocks.com.

$4T
DIGITAL ASSETS SECURELY TRANSFERRED

1,000s
INSTITUTIONAL CUSTOMERS

130M+
WALLETS CREATED

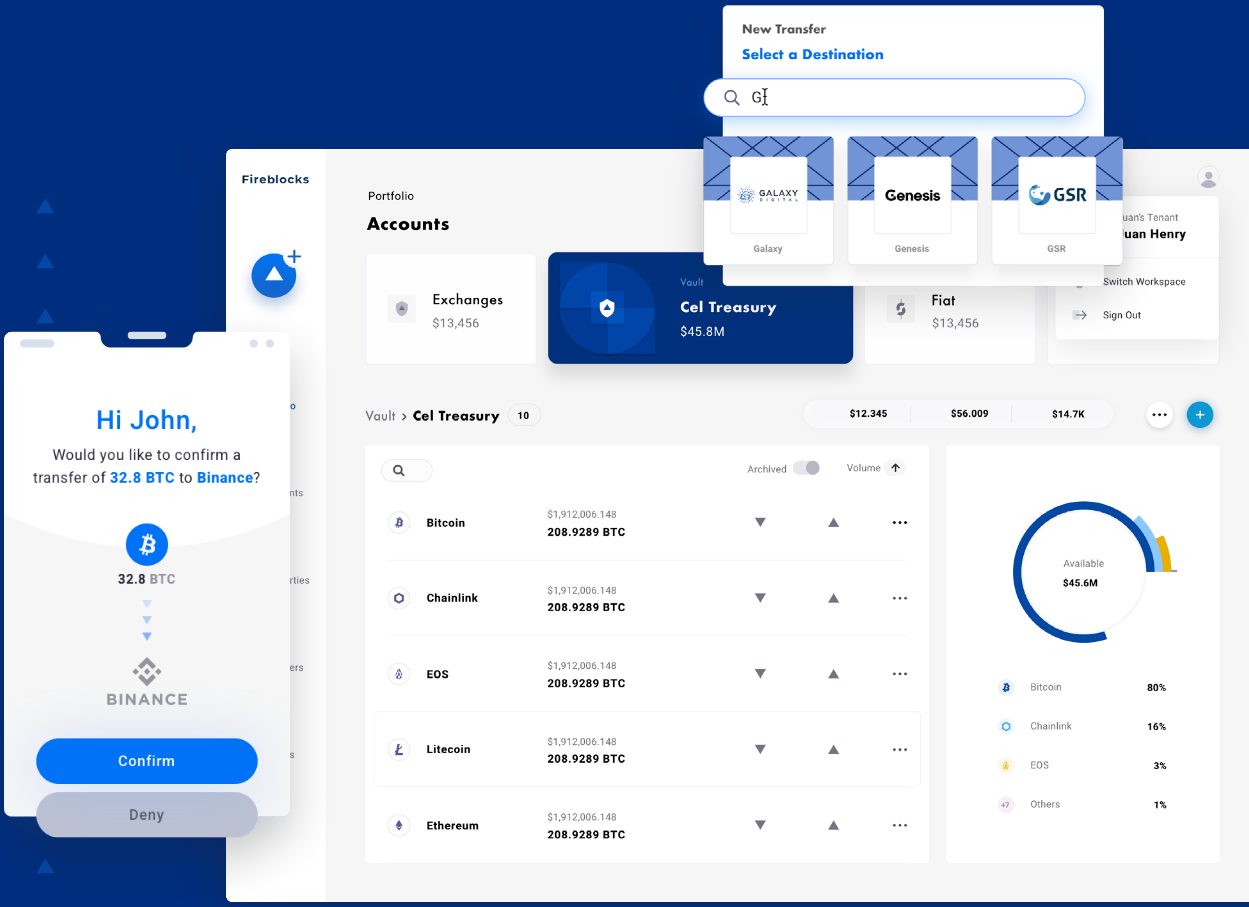
CCSS Qualified Service Provider Cert ID: CCSS00001 Issued by C4

AICPA SOC 2 — AICPA Service Organization Control Reports — Formerly SAS 70 Reports

ISO 27001: 2013 certified — Information Security Management System

ISO 27017: 2015 certified — Cloud Security

ISO 27018: 2019 certified — Privacy



New Transfer
Select a Destination
GI

Galaxy
Genesis
GSR

Fireblocks

Portfolio
Accounts

Exchanges $13,456
Vault Cel Treasury $45.8M
Fiat $13,456

Juan's Tenant
Juan Henry
Switch Workspace
Sign Out

Vault > Cel Treasury 10

$12.345 $56.009 $14.7K

Archived Volume

Bitcoin	$1,912,006.148	208.9289 BTC
Chainlink	$1,912,006.148	208.9289 BTC
EOS	$1,912,006.148	208.9289 BTC
Litecoin	$1,912,006.148	208.9289 BTC
Ethereum	$1,912,006.148	208.9289 BTC

Available $45.6M

Bitcoin	80%
Chainlink	16%
EOS	3%
Others	1%

Hi John,

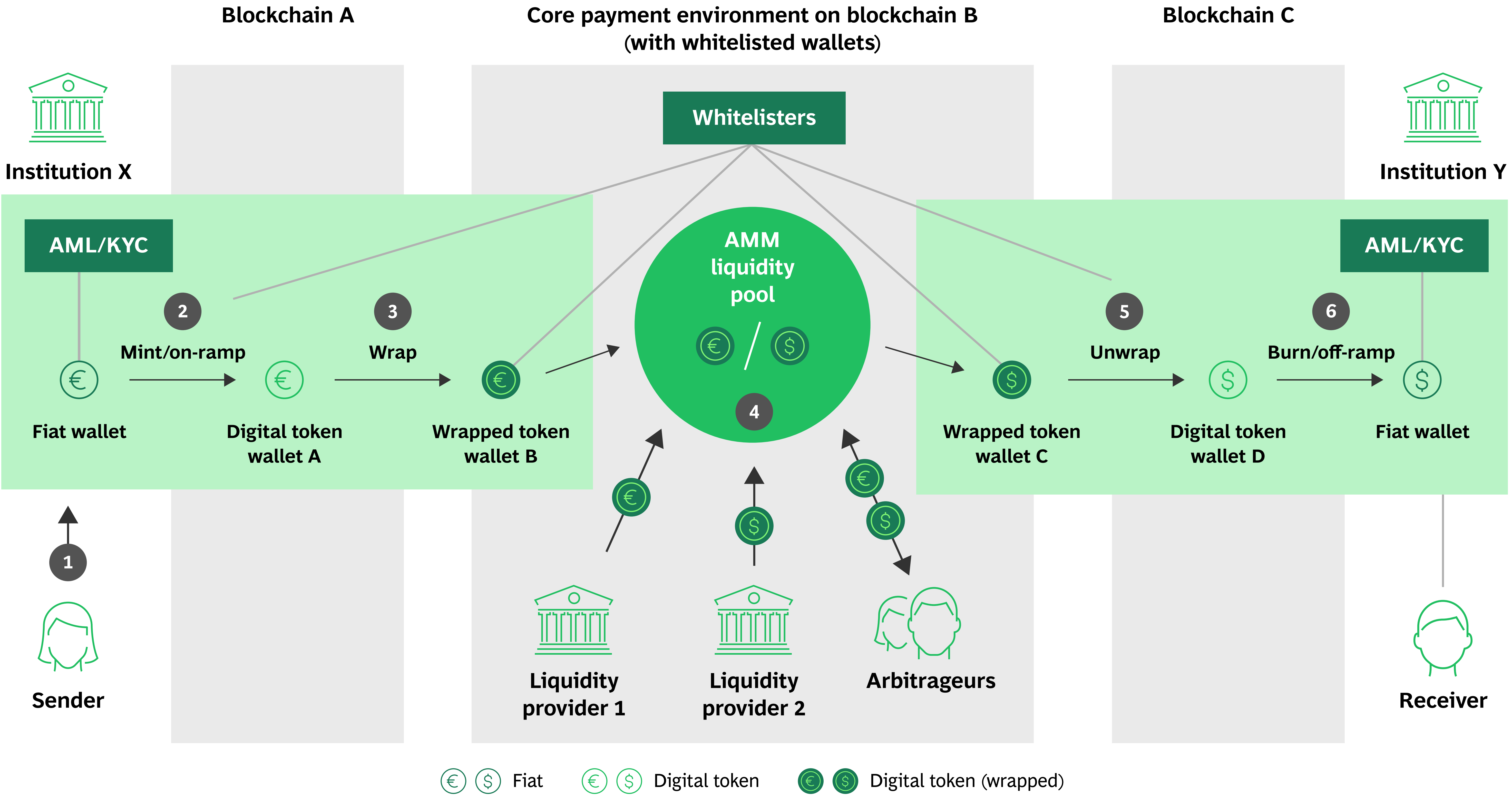
Would you like to confirm a transfer of **32.8 BTC** to **Binance**?

32.8 BTC
BINANCE

EXHIBIT

A

Cross-Border Permissioned DeFi Model



Source: Fireblocks and BCG analysis.
Note: AML = anti-money laundering; KYC = Know Your Customer.

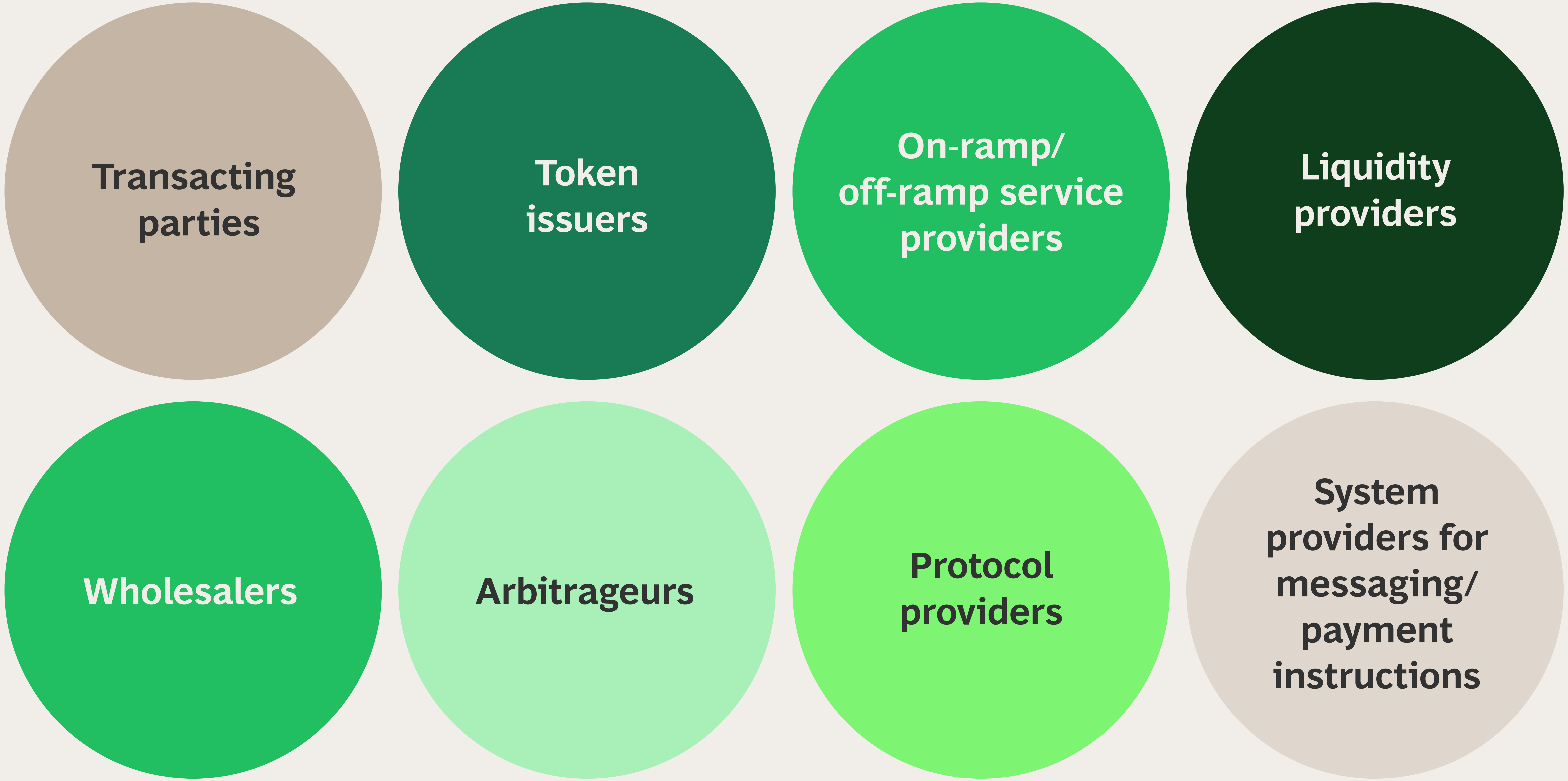
Fireblocks

EXHIBIT

B

Participants in the cross-border permissioned DeFi model

The eight key participants



Transacting parties

Token issuers

On-ramp/ off-ramp service providers

Liquidity providers

Wholesalers

Arbitrageurs

Protocol providers

System providers for messaging/ payment instructions

Source: Fireblocks and BCG analysis.

Transacting parties in the cross-border permissioned DeFi model

Source: Fireblocks and BCG analysis.

Note: PSPs = payment service providers; AML = anti-money laundering; KYC = Know Your Customer; KYT = Know Your Transaction.

Role

Transacting parties

Likely participants

Commercial banks, retail banks, PSPs

Incentive to participate

- Near instantaneous 24/7 settlements
- Transaction data visibility
- Potentially lower costs, no pre-funding

Key considerations

- Wallet infrastructure for custody of tokens
- Connectivity to the DeFi protocols
- AML/KYC/KYT checks

Token issuers in the cross-border permissioned DeFi model

Source: Fireblocks and BCG analysis.

Role

Token issuers

Likely participants

Transacting banks that choose to control the issuance of the token

Incentive to participate

For coin users:

- Revenue from creation and redemption fees and interest income
- Excess reserves can be deployed in liquidities

Key considerations

- Token lifecycle management (smart contract design, mint and burn, governance, custody, etc.)
- Token recalling or freezing mechanisms

On-ramp/off-ramp service providers in the cross-border permissioned DeFi model

Source: Fireblocks and BCG analysis.

Role

On-ramp/off-ramp service providers

Likely participants

- A digital asset exchange if the token is an open stablecoin
- A regulated bank that issues its own stablecoin
- A non-bank party that issues its stable coin supported by commercial banks

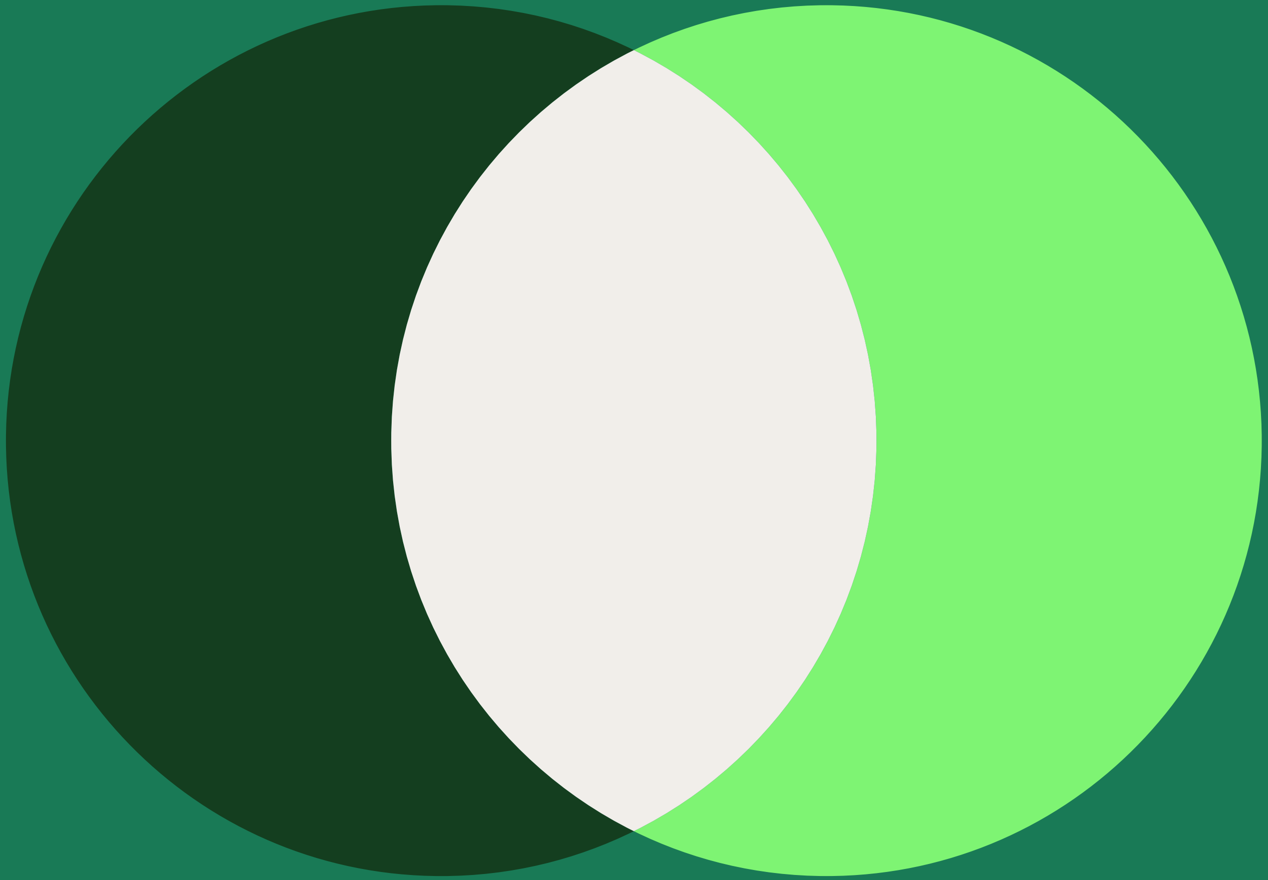
Incentive to participate

On- and off-ramp fees captured

Key considerations

Wallet infrastructure for custody of the tokens on behalf of their clients and their own treasury management

Liquidity providers in the cross-border permissioned DeFi model



Source: Fireblocks and BCG analysis.

Role

Liquidity providers

Likely participants

FX market makers, commercial banks

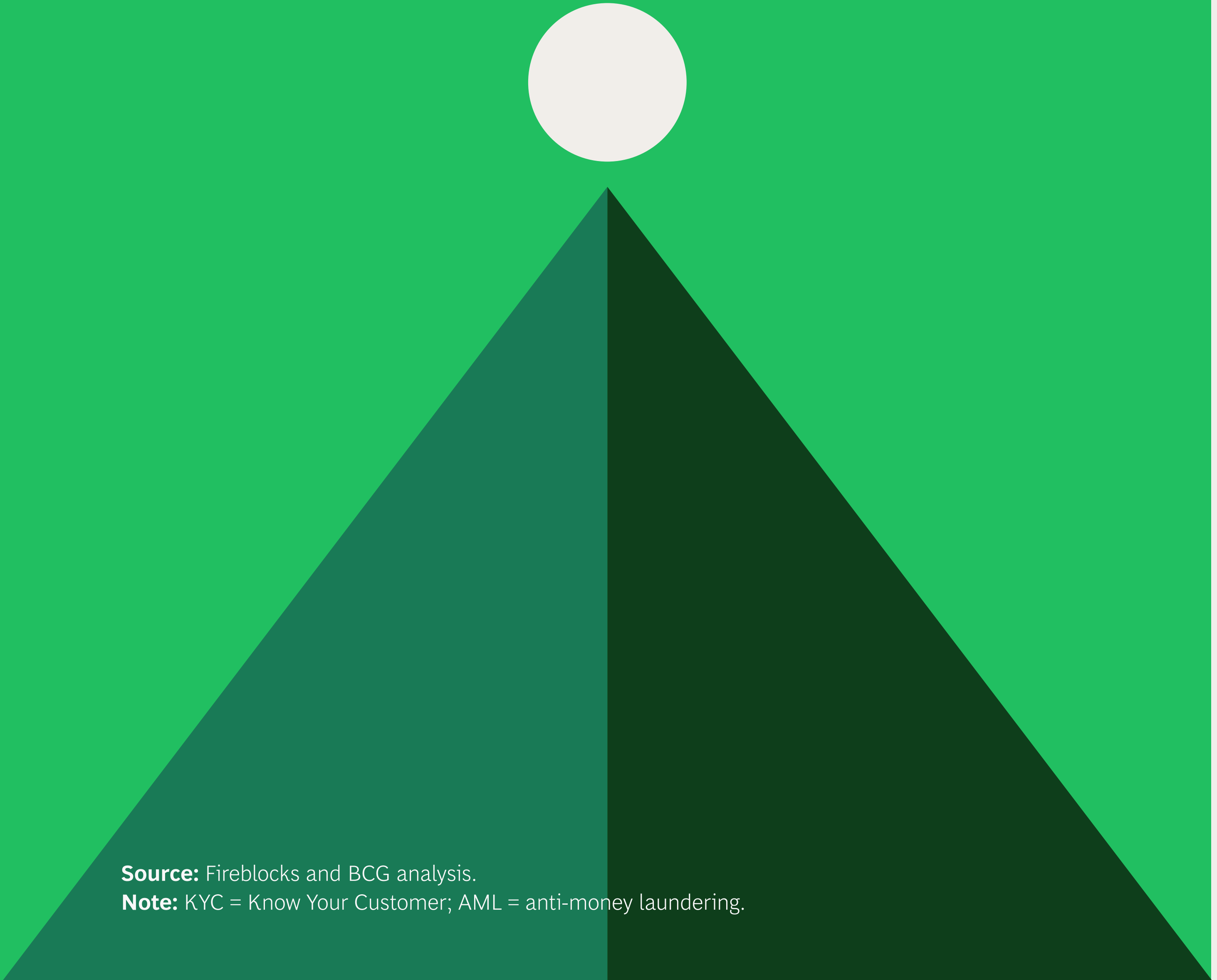
Incentive to participate

Earn transaction fees by providing liquidity to the model

Key considerations

- Wallet infrastructure for custody of tokens
- Connectivity to the DeFi protocols
- Sourcing initial liquidity of the tokens

Wholesalers in the cross-border permissioned DeFi model



Source: Fireblocks and BCG analysis.
Note: KYC = Know Your Customer; AML = anti-money laundering.

Role

Wholesalers

Likely participants

- Transacting parties
- An appointed neutral third party to conduct KYC/AML checks on participants and wallets

Incentive to participate

For third parties and infrastructure providers: potentially earn fees during the wrapping process

Key considerations

- Compliance framework and requisite licenses
- Connectivity to DeFi protocols

Arbitrageurs in the cross-border permissioned DeFi model

Source: Fireblocks and BCG analysis.

Role

Arbitrageurs

Likely participants

FX market makers

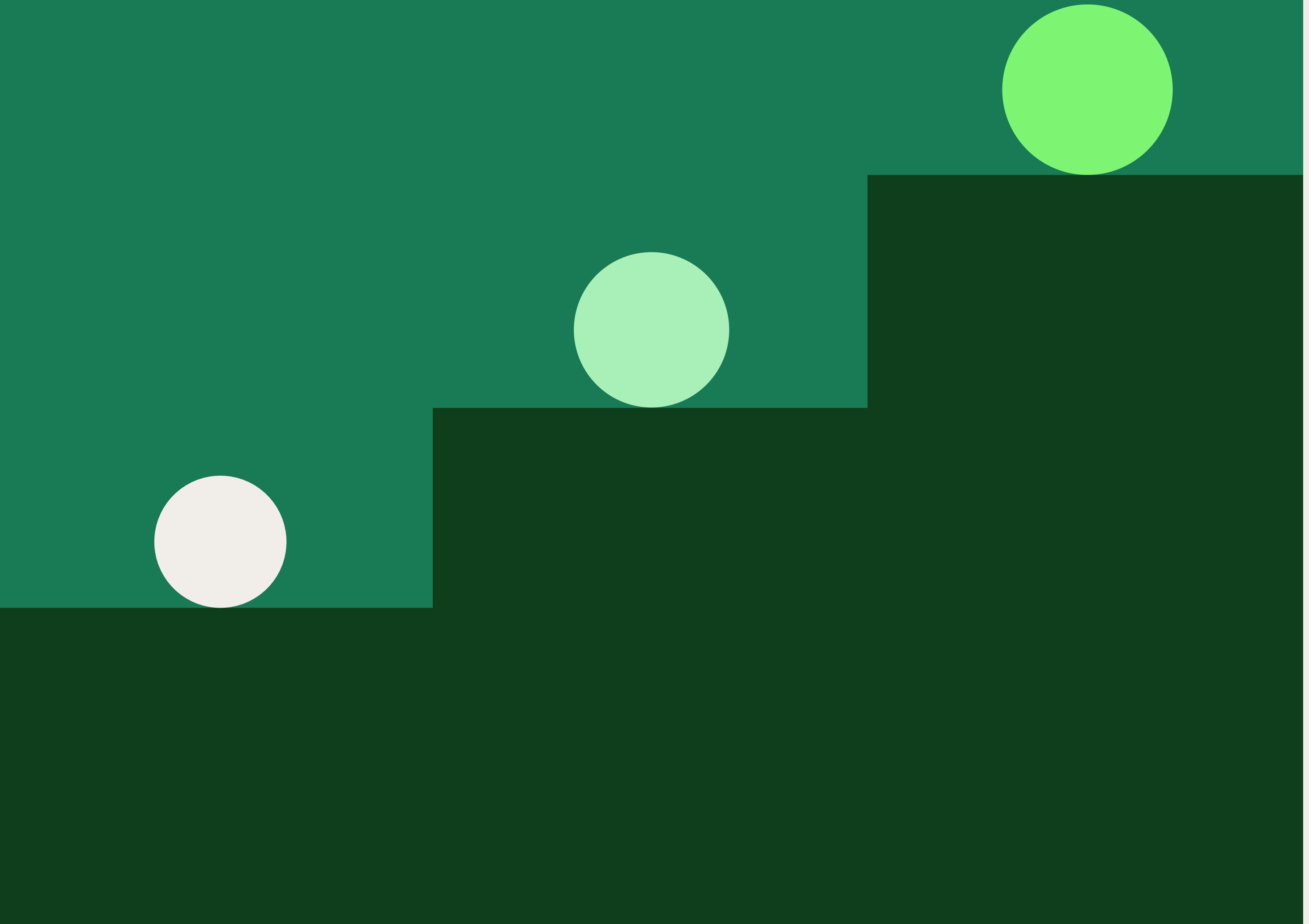
Incentive to participate

Profits generated from collecting the bid-offer spread

Key considerations

- Accurate price feeds for both on- and off-chain data
- Connectivity to smart contracts
- Custody of tokens
- Access to liquidity venues to trade tokens

Protocol providers in the cross-border permissioned DeFi model



Source: Fireblocks and BCG analysis.

Role

Protocol providers

Likely participants

Automate market making protocols

Incentive to participate

Increased usage and total value of assets locked on their protocol, which leads to increased revenue

Key considerations

- Governance for the permissioned pools
- Security of smart contracts

System providers for messaging/payment instructions in the cross-border permissioned DeFi model

Source: Fireblocks and BCG analysis.

Role

System providers for messaging/payment instructions

Likely participants

- Messaging networks (SWIFT)
- Oracle networks

Incentive to participate

Future-proofing by offering value-add products to new markets

Key considerations

- Reconciliation of messaging layer and the blockchain-based settlement layer
- ISO 20022 compatibility
- Standardization