REDEFINING TRANSACTION BANKING IN A DECENTRALIZED WORLD OF DIGITAL MONEY

Call for open source and open innovation project participation

September 2024

In this paper, we propose a lean experiment design to formulate and validate hypotheses and gain practical experience on how decentralized digital money can change the role of commercial banks. The results from this experiment will be applicable to improve the existing- and develop new commercial bank business models surrounding both private (e.g. stablecoins) as well as public (the Digital Euro) forms of digital money. Learnings from prior initiatives show that for successful experimentation public-private, low-barrier, and open-source collaboration is required whilst ensuring compliance to regulatory demands. The time to experiment is now to drive change for the future of banking.

Why? In the increasingly decentralized landscape of digital money, the question of whether banks will retain their right to compete in transaction banking remains unsolved. With increasingly faster and more efficient transactions outside the current banking system (e.g. stablecoins), the emergence of more specialized players offering new investment and service opportunities (e.g. crypto ETFs), and a growing fragmentation of various forms of digital money (e.g. CBDCs[1] like Digital Euro), banks face the challenge of staying the trusted gateway for their customers. However, prior research projects in this area were often one-dimensional, driven by a single organization, and executed in isolation.

What? To maintain and expand on their customer relationship capital while leveraging open, public, and decentralized infrastructures, banks need to define how they can equally become the gateway into the world of digital money for the broader market and society at large. This requires a transition from being the trusted, central owner, and facilitator of transactions to becoming an access point to a decentralized public infrastructure, which complies with the highest regulatory, legal, and ethical standards.

How? This project mirrors the idea of an open, collaborative, and inclusive financial system by creating a unique and first of its kind setup. We adopt an open public-private partnership model to collaboratively explore user-driven, technological, and regulatory requirements and opportunities for banks that seek to become the central access points for their existing and future customers to an increasingly decentralized world of digital money. To achieve this, the goal of this project is to jointly define foundational standards and requirements that apply to the banking industry at large yet allow each banking participant to leverage their user/customer base and develop new revenue/business models. Our initial hypotheses are that such standards and requirements will evolve around (1) common identity and KYC[1] services and standards, (2) on-chain privacy and selective disclosure, and (3) on-chain transaction monitoring.

Context and scope. The European Union with a focus on the public decentralized infrastructure for Digital Euro and focal CBDCs. The project is open to all banks and partners

[1] Central Bank Digital Currencies, https://cbdctracker.org/

in this space and designed as a community-experiment to build on existing knowledge, while generating new insights, ideas, industry standards, and partnerships.

Structure. The remainder of the paper is structured in the following way. First, we will present our perspective on the current and future states of the Digital Euro and its underlying infrastructure. The purpose of this section is to create a common understanding and foundation of our project. Second, we will present the position of the different participating banks in relation to the Digital Euro to make sure all participants are “on the same page” as to the individual interests and perspectives of each other. Third, we will elaborate on the size of the market opportunity in relation to decentralized transactions we seek to exploit by engaging into this project. Fourth, we will integrate the different chapters and lay out our intended experiment design and conclude by articulating our call to action.

1 Digital currencies and the path to Finternet

Many have sought to define the future of money including the role of CBDCs. One such foundational effort, Get Ready for the Future of Money[1] (Mikhalev, Burchardi, Kok, Song. 2020, BCG), has laid important groundwork. We assert that public Blockchain- and Distributed Ledger Technology (DLT) are central to the evolution of the digital financial ecosystem, providing a robust foundation for what we term the “Finternet” — a decentralized financial network at its core built on public permissionless blockchains with autonomous smart contract like Ethereum.

How do we reach the Finternet?

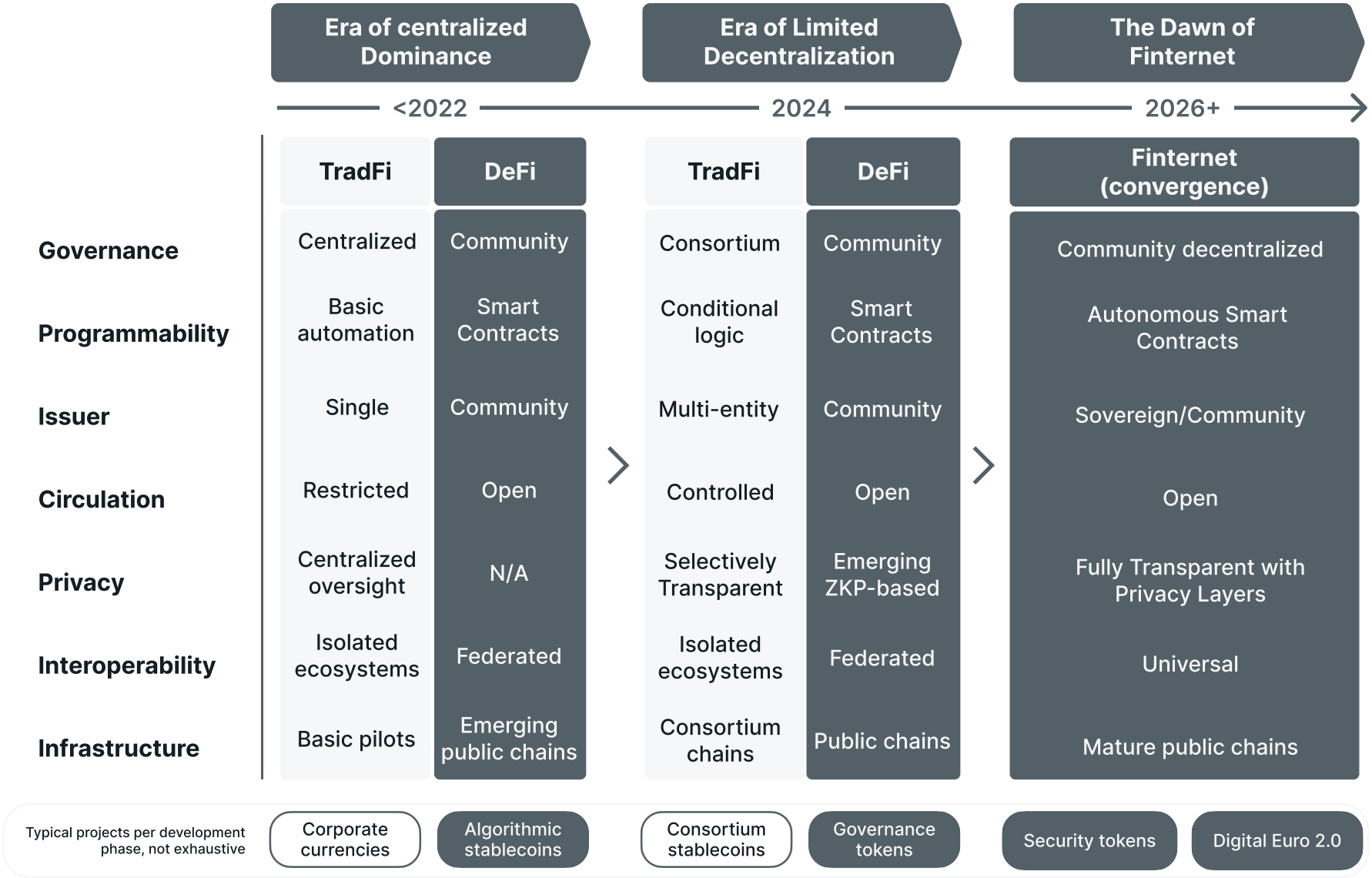
Many have sought to define the future of money including the role of CBDCs. One such foundational effort, Get Ready for the Future of Money[1] (Mikhalev, Burchardi, Kok, Song. 2020, BCG), has laid important groundwork. We assert that public Blockchain- and Distributed Ledger Technology (DLT) are central to the evolution of the digital financial ecosystem, providing a robust foundation for what we term the “Finternet” — a decentralized financial network at its core built on public permissionless blockchains with autonomous smart contract like Ethereum.

Phase 1: "Era of Centralized Dominance"

The "Era of Centralized Dominance," which lasted up until approximately 2022, was defined by centralized control, limited innovation, and an initial, often superficial, engagement with blockchain technology within the existing financial frameworks. This phase was marked by the dominance of TradFi, where the design and implementation of digital currencies were managed by single entities, such as central banks or large financial institutions, with a restricted circulation model and minimal public involvement.

[2] Know Your Customer
[3] https://www.bcg.com/publications/2020/get-ready-for-the-future-of-money
[4] Traditional Finance and Decentralized Finance

As the public decentralized infrastructure matures, effectively becoming the Finternet, the worlds of TradFi and DeFi converge



Digital currencies and the path to Finternet

Key characteristics of the Era:

Centralized Governance and Control

During this period, the governance of digital currencies remained firmly centralized, with banks and other financial institutions retaining complete authority over their issuance and management. The approach was risk-averse and mirrored the existing models of fiat currency management, focusing more on control and less on community-driven or decentralized governance.

Minimal Programmability and Innovation

In terms of programmability, these early digital currencies offered little beyond basic automation. The technology implemented in this era often consisted of rudimentary digital representations of money that could execute simple, predefined actions, such as conditional payments or transfers. The concept of autonomous programmable smart contracts, which could automatically execute complex transactions based on real-time data and triggers, was still nascent and largely unexplored.

Isolated Issuer Models

The issuers were typically single entities, such as central banks or a consortium of commercial banks, that operated within closed-loop networks. The networks were isolated from broader digital ecosystems, thereby limiting their utility and adoption. These closed environments did not allow for interoperability with other systems, stifling any potential for collaboration or integration with emerging decentralized DeFi platforms.

Restricted Circulation and Limited Transparency

Circulation models were restricted to a limited set of participants—often within a single jurisdiction or within a tightly controlled group of financial institutions. This restricted model did not encourage open participation from the broader financial community or the public. Privacy models were also based on centralized oversight, which meant that while transactions were controlled and monitored by a central authority, there was minimal transparency or user control over data.

Early Experiments and the Rise of Vanity Projects

This phase saw a surge in early experiments with blockchain technology, often initiated by large corporations or consortiums looking to capitalize on the blockchain trend. For instance, corporate currencies built on closed-loop blockchain networks were explored by multiple commercial banks. However, many of these initiatives either failed or continued to persist as vanity projects with questionable business cases. The high operational costs associated with maintaining these networks were not justified by the limited gains in disintermediation or enhanced trust—largely because these models did not attempt genuine decentralization or address fundamental trust issues.

Influence on Early CBDC Designs

Early CBDC designs were heavily inspired by public blockchain models but were still tethered to traditional approaches. They were aimed at retail use cases, yet lacked the transformative qualities needed to harness blockchain's full potential. No major pilots or live deployments of CBDCs were truly blockchain-based; instead, they relied on traditional technologies. The idea of implementing programmability beyond basic automation was considered too complex and resource-intensive, given the challenges associated with deploying a blockchain network capable of serving an entire national population.

Fragmented and Isolated Ecosystems

The interoperability dimension in this era can be described as isolated ecosystems, where each experiment or project functioned independently with little to no interaction with other networks or platforms. This lack of interoperability resulted in inefficiencies, redundancies, and missed opportunities for collaboration across the financial sector.

Basic Infrastructure and Pilots

The infrastructure supporting digital currencies during this era was characterized by basic pilots. These were preliminary tests and sandbox environments, limited in scale and scope, that focused more on understanding blockchain's potential rather than creating scalable, real-world solutions. The technology was largely unproven for large-scale, real-time applications in national or global financial systems.

The "Era of Centralized Dominance" was marked by a cautious and controlled approach to the adoption of digital currencies, heavily influenced by the legacy TradFi frameworks. The lack of genuine innovation, interoperability, and meaningful decentralization limited the progress of digital currency projects, rendering many early attempts ineffective or relegating them to mere experiments. This era set the stage for the subsequent Era of Limited Decentralization, where stakeholders began to open up and explore more collaborative, semi-decentralized approaches to harnessing the potential of blockchain technology for digital currencies.

Phase 2: "Era of Limited Decentralization"

The "Era of Limited Decentralization", arguably the current era, marks a cautious transition from fully centralized digital currency models to more open, collaborative, and semi-decentralized frameworks. This phase is characterized by consortium-based designs, hybrid models, and incremental innovations that aim to balance the benefits of DeFi with the control and stability of traditional finance TradFi.

Key characteristics of the Era:

Consortium Governance
Governance evolves from centralized entities to multi-party consortiums involving multiple banks and financial institutions. While this reduces counterparty risk (as the claim on a consortium is arguably more reliable than a claim on a single entity, and improves resilience) it remains a semi-decentralized model with limited community involvement and transparency.

Multi-Entity Issuance
Issuance is handled by multiple entities (e.g., banks or financial consortiums), bridging the gap between traditional financial institutions and decentralized platforms. This model shares risks and responsibilities but still operates within controlled, permissioned networks.

Conditional Programmability
The programmability of digital currencies moves beyond basic automation to conditional logic, enabling more use cases, applications, and complex financial operations such as programmable payments. However, the full potential of autonomous smart contracts remains untapped, limiting deeper innovation.

Controlled Circulation
While circulation becomes more open than in the previous era, it remains tightly regulated within consortium networks to ensure compliance and control, hindering broader public participation.

Selective Transparency
Privacy models advance with selective transparency using cryptographic techniques like Zero-Knowledge Proofs (ZKPs), balancing the need for privacy and regulatory compliance. However, transparency is selectively granted rather than universally available.

Federated Interoperability
Digital ecosystems begin to connect through federated interoperability, allowing limited cross-network operations. While this represents progress from isolated ecosystems, true universal interoperability is not yet achieved.

Hybrid Infrastructure
The infrastructure is a mix of emerging public chains (e.g., Ethereum L2/L3) and consortium chains. This hybrid approach allows experimentation with scalable, semi-public blockchains while retaining elements of central control.

Incrementalist CBDC Approaches
CBDC projects in this era, such as the Digital Euro, take an "incrementalist" approach, offering digital alternatives while maintaining strict regulatory control. These projects are cautious steps rather than bold moves toward full decentralization.

Selective Ecosystem Participation
Participation remains limited to established financial players and trusted partners, with some inclusion of fintech and tech companies, reflecting a cautious approach to innovation.

The "Era of Limited Decentralization" represents a period of cautious experimentation and gradual adaptation, where digital currency designs begin to incorporate some decentralized elements without fully embracing them. Consortium-based models, selective transparency, and hybrid infrastructures characterize this phase as a bridge between the centralized past and the more open, interoperable future envisioned in the Dawn of Finternet. This era sets the groundwork for a deeper convergence of TradFi and DeFi, preparing the financial ecosystem for a more integrated, decentralized landscape.

Phase 3: "The Dawn of Finternet"

"The Dawn of Finternet" (2026 and beyond) represents the culmination of the transition toward a fully decentralized and interoperable financial ecosystem where Central Bank Digital Currencies (CBDCs), cryptocurrencies, and digital assets converge on mature public blockchain infrastructures. This era is defined by the widespread adoption of established decentralized protocols, such as Ethereum's Layer 2 (L2) and Layer 3 (L3) solutions, for both national digital currencies and enterprise use cases in the Web3 space. As societal demand for greater financial freedom, innovation, and direct participation continues to grow, CBDCs and cryptocurrencies are set to operate seamlessly in a unified, decentralized environment.

Key characteristics of the Era:

Community Decentralized Governance

Governance evolves to a fully community decentralized model, where decision-making is distributed among a wide array of stakeholders, including central banks, commercial entities, decentralized organizations, and the public. This approach democratizes monetary policy, reduces power concentration, and limits political influence, creating a more balanced and transparent governance structure.

Autonomous Smart Contracts and Full Programmability

The era is marked by the extensive use of autonomous smart contracts, which provide full programmability for a wide range of financial transactions and services. These smart contracts will enable SMEs to build new applications (ventures) and automate complex workflows such as cross-border payments, real-time compliance checks, and asset tokenization, enabling seamless and trustless interactions across different financial platforms.

Sovereign/Community Issuance Models

Issuance of digital currencies transitions to a sovereign/community model, where both national governments and decentralized communities can issue and manage their digital currencies on public blockchain networks. This hybrid model combines the stability of sovereign issuance with the flexibility and inclusiveness of community-driven models, allowing for greater adaptability to market and social dynamics.

Open and Universal Circulation

Digital assets in this era enjoy open and universal circulation. With established interoperability standards and protocols, digital currencies can be easily transferred and exchanged across multiple networks, enabling a truly global and inclusive financial system. This open circulation model supports peer-to-peer transactions, reducing reliance on intermediaries and lowering transaction costs significantly.

Fully Transparent Privacy with Privacy Layers

Privacy in this phase achieves a balance between full transparency and privacy protection through advanced cryptographic techniques such as zero-knowledge proofs (ZKPs) and the resulting privacy layers. This ensures that while transactions are transparent and verifiable to meet compliance requirements, users can maintain privacy and selectively disclose information as needed.

Universal Interoperability Across Networks

The infrastructure of the "Finternet" is built on universal interoperability, where different blockchains, payment systems, and digital currencies interact seamlessly. Cross-chain protocols, atomic swaps, and bridges enable instant and secure value transfer across diverse networks, effectively converging CBDCs and cryptocurrencies in a single, unified financial ecosystem.

Mature Public Chains and Scalable Infrastructure

The underlying infrastructure consists of mature public chains (like Ethereum, Avalanche, or Cosmos) that provide scalable, secure, and decentralized environments for both public and private use cases. These chains support Layer 2 and Layer 3 solutions to address scalability, cost-efficiency, and privacy concerns, making them ideal for large-scale adoption by national governments, enterprises, and individuals.

Decentralized CBDC Adoption

As decentralized infrastructure matures, there is a compelling case for CBDCs to embrace decentralization – Central Bank Digital Currencies Need Decentralization[1] (Mikhalev, Burchardi, BCG, 2021):

- Enhanced Democracy and Power Distribution: Leveraging public blockchain infrastructure, CBDCs can democratize access, reduce concentration of power, and minimize political influence in monetary policy decision-making.
- Reduced Currency Volatility: Particularly in emerging economies, decentralized CBDCs can provide more stability, mitigating the risk of political and economic shocks.
- Lower Payment Costs: By enabling peer-to-peer transactions, CBDCs can drastically reduce payment costs. In this model, commercial banks could focus on providing identity verification, Know Your Customer (KYC) services, on-chain privacy, selective disclosure, and transaction monitoring standards.

This is particularly beneficial for emerging economies, where decentralized CBDCs could reduce currency volatility and provide stability against economic shocks.

[5] https://www.coindesk.com/policy/2020/05/23/central-bank-digital-currencies-need-decentralization/

Early adopters of decentralized CBDCs will gain a significant advantage by enhancing the competitiveness of their (supra)national currencies. Benefits include more efficient and secure payment systems, reduced corruption, improved governance, and greater economic resilience. These advantages will make decentralized CBDCs a compelling choice for countries looking to modernize their financial infrastructure.

"The Dawn of Finternet" signifies and begins the full realization of a decentralized, interoperable financial network where CBDCs and cryptocurrencies coexist and collaborate seamlessly. It is driven by public demand for openness, freedom, and innovation, supported by mature blockchain infrastructures and decentralized governance models. Commercial banks and financial institutions shift their roles to provide value-added services such as identity verification (KYC), on-chain privacy, selective disclosure, and real-time transaction monitoring, ensuring both privacy and compliance.

02 Our positions on the Digital Euro

The position of ABN AMRO on the Digital Euro

The ABN AMRO position on the arrival of the digital euro focuses on the processes banks are tasked with, as those processes are essential for the digital euro to become a success. The aim is to contribute to a design of those processes in such a way that are efficient for banks, effective to be compliant, providing opportunities for fee income with additional services and contribute to trust in the financial system as a whole. Processes that allow the decentralized world to emerge. The constructive and collaborative attitude has led so far to a good understanding of the impact on commercial banks based on the current design and is now building on that collaborative network with key partners and a close relationship with the central bank for the next steps. ABN AMRO has been able to give valuable input in the design process on how the funding/defunding and conversion can work smoothly and now allows to focus on processes that enable compliance, so the system effectively adheres to the EU's AML/CFT framework and PSD2/PSD3 in accordance with the EU's General Data Protection Regulation. The insights required to give valuable input on these components need to be gained by experimentation as the right balance between privacy and compliance can no longer be achieved by positioning alone.

03 The rise of the decentralized transactions market

As an untapped opportunity for banks

As illustrated further, the decentralized transactions market is experiencing significant growth, driven by the rapid mass market adoption of public blockchain based stablecoins and native cryptocurrencies like Bitcoin and Ether. Both asset types are reshaping the financial landscape with expanding market volumes and a growing user base, challenging the traditional transaction banking model and providing banks an opportunity to innovate collaboratively.

Stablecoins: Dominating Decentralized Transactions

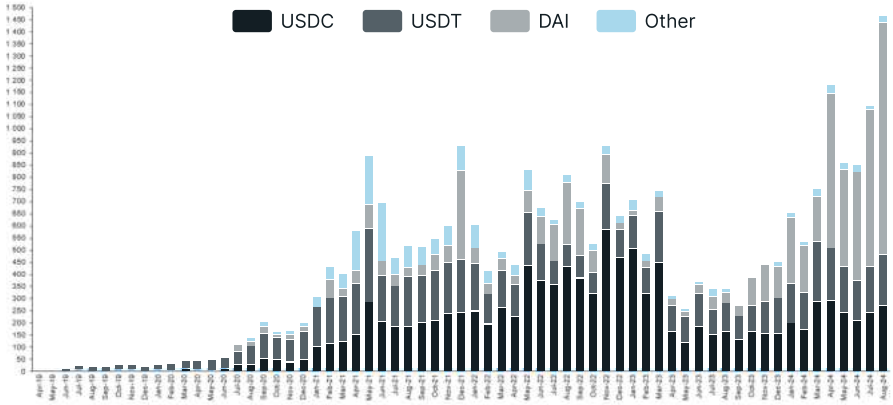
Stablecoins have become a cornerstone of the DeFi ecosystem, acting as a bridge between traditional finance and digital assets. The total market capitalization of stablecoins has surged to over $120 billion in 2024, making them a preferred medium of exchange for traders and investors seeking stability amidst volatile markets. Three well-established examples include:

- USDT (Tether): With a market cap exceeding $80 billion and daily trading volumes over $40 billion, USDT dominates the stablecoin space. Its liquidity and acceptance across both centralized and decentralized exchanges make it a key player in global digital transactions.
- USDC (USD Coin): Valued at around $30 billion with daily trading volumes of over $6 billion, USDC's regulatory compliance and transparency have positioned it as a go-to for institutional investors. Its integration into DeFi platforms further amplifies its role in decentralized transactions.
- DAI: A decentralized alternative with a $5 billion market cap and $1 billion daily trading volume, DAI is pivotal in DeFi ecosystems, particularly in protocols like MakerDAO for collateralized loans. Its decentralized nature ensures it is less vulnerable to centralized control, appealing to those prioritizing autonomy.

Stablecoins now constitute nearly 80% of trading pairs on decentralized exchanges (DEXs), and their integration into payment systems has made them a powerful tool for cross-border transactions, with volumes reaching $20 billion in 2023.

Stablecoins are seeing widespread adoption across the digital asset landscape and are used for a diverse set of purposes

Global Ethereum on-chain transaction volume of stable coins per month (in $b)



Native Cryptocurrencies: Driving Market Activity and Innovation

Native cryptocurrencies, like Bitcoin (BTC) and Ethereum (ETH), are central to the decentralized transactions market, comprising over 60% of the total cryptocurrency market cap, which stands at approximately $1.5 trillion. Two well-established examples include:

- Bitcoin (BTC): With a market cap of $600 billion and daily trading volumes over $25 billion, Bitcoin remains a leader in cross-border payments, accounting for $30 billion in remittances in 2023—a 40% increase from the previous year. Its broad adoption by over 100 million users worldwide underscores its potential to replace traditional banking services for international transactions.
- Ethereum (ETH): Ethereum's $250 billion market cap and $15 billion in daily trading volumes highlight its critical role in powering DeFi, NFTs, and decentralized applications. With a total value locked (TVL) exceeding $70 billion in Ethereum-based DeFi protocols, it's clear that Ethereum is foundational to the decentralized finance ecosystem.

An opportunity to innovate Transaction Banking

We observe a rapid growth of decentralized transactions, which is led by the adoption of stablecoins and native cryptocurrencies as well as the arrival of CBDCs, e.g. Digital Euro. However, while several banks lack a clear strategy on how to tap into this growing market potential, there is wide agreement on the fact that solo initiatives and efforts will not pay off eventually. Instead, more open, collaborative approaches are required to serve customers who increasingly turn to decentralized alternatives for speed, cost efficiency, accessibility, and - the core business of traditional banks — facilitating transactions. The "attack vector" of non-traditional players include the following areas that put the current business model of banks under pressure:

1. Loss of Transaction Fees. Banks generate significant revenue from cross-border payment fees, remittances, and currency exchange. However, with stablecoins enabling instant, low-cost global transactions, these traditional revenue streams are rapidly eroding. Cross-border stablecoin transactions, already reaching $20 billion, bypass the need for intermediaries.
2. Disintermediation. Decentralized platforms remove the need for banks as intermediaries, allowing users to transact directly. This shift is particularly impactful for international payments, where decentralized networks like Bitcoin and Ethereum can provide faster, cheaper, and more secure alternatives compared to SWIFT and other traditional banking systems.
3. Reduced Demand for Banking Services. As more businesses and individuals adopt digital wallets and decentralized finance platforms, the demand for conventional banking services, such as checking accounts and international wire transfers, is declining. Stablecoins like USDC and decentralized

cryptocurrencies like Ethereum enable programmable transactions, lending, and borrowing directly on blockchain networks, bypassing traditional banks altogether.

4. Risk of Being Left Behind in Innovation. Traditional banks that adapt to this shift can take advantage and retain their relevance in the emerging Finternet. The rapid innovation in DeFi and blockchain technology, coupled with increasing user demand for decentralization, creates a highly competitive environment where traditional banks must either innovate or become obsolete.

The Future of Transactions is Decentralized

With the ability to provide faster, cheaper, and more secure transaction solutions without intermediaries, the decentralized market is positioned to capture a significant share of global transaction volumes. Against this background, the main question for banks is how to jointly embrace technological innovations and associated market potential brought forward by decentralized transactions proactively instead of reactively protecting old business models in isolation?

04 Experiment Design

The goal of this project is to collaboratively establish foundational standards and requirements that can be applied universally across the banking industry, while still enabling individual banks to leverage their existing customer bases and innovate with new revenue streams and business models. This experiment aims to create a framework that balances the need for industry-wide interoperability and security with the flexibility to cater to the unique needs of different financial institutions.

We expect the development of standards and requirements will focus on three critical areas:

1. Common identity and Know Your Customer (KYC) services and standards;
2. On-chain privacy and selective disclosure mechanisms;
3. On-chain transaction monitoring.

These focus areas are crucial in bridging the traditional financial systems with decentralized digital infrastructures, particularly in the context of Central Bank Digital Currencies (CBDCs) and decentralized finance (DeFi) applications.

The Future of Transactions is Decentralized

With the ability to provide faster, cheaper, and more secure transaction solutions without intermediaries, the decentralized market is positioned to capture a significant share of global transaction volumes. Against this background, the main question for banks is how to jointly embrace technological innovations and associated market potential brought forward by decentralized transactions proactively instead of reactively protecting old business models in isolation?

1. **Scalability & Performance.** The decentralized platform must demonstrate the ability to handle the high transaction throughput and volume typical of the financial transactions domain. This involves measuring key performance indicators such as latency, confirmation times, and overall network performance under various loads. Ensuring scalability is vital, as the solution must support real-time, high-volume transactions across customer bases of multiple financial institutions without bottlenecks.
2. **Privacy & Confidentiality.** Privacy and data protection are key in any financial ecosystem, especially one that utilizes decentralized technology. The experiment will evaluate privacy-enhancing features, specifically zero-knowledge proofs used to enable confidential transactions, protecting sensitive transaction data and maintaining confidentiality between participants. The objective is to implement on-chain privacy and selective disclosure mechanisms that allow for secure, compliant data sharing without compromising user privacy.
3. **Resilience & Fault Tolerance.** The robustness of the decentralized network must be tested against potential failures, attacks, and network partitions. This aspect of the experiment will assess the system's ability to maintain operations in adversarial conditions, ensuring data consistency, integrity, and overall network resilience. A resilient system is critical for sustaining trust among users and regulators in a decentralized infrastructure.
4. **Interoperability & Integration.** For the decentralized model to be adopted industry-wide, it must seamlessly integrate with existing financial systems, payment networks, and regulatory frameworks. This proof point will focus on demonstrating interoperability between different commercial banks' systems as they leverage public decentralized infrastructure. The goal is to create a cohesive ecosystem where decentralized and traditional systems can co-exist.
5. **Compliance & Regulatory Requirements.** Compliance with regulatory standards, including anti-money laundering (AML), KYC, and counter-terrorism financing (CTF) regulations, is non-negotiable. This component of the experiment will ensure that the resulting platform can enforce these regulations effectively, supporting transaction monitoring, audit trails, real-time reporting, and adherence to international standards. Establishing

these compliance mechanisms is crucial for gaining regulatory acceptance and building trust among global financial stakeholders.

6 **Security.** The experiment will conduct comprehensive security assessments and penetration testing to identify vulnerabilities and attack vectors. It will also focus on implementing robust authentication, authorization, and encryption protocols to protect sensitive data and prevent unauthorized access. These measures are essential to safeguard against potential breaches and maintain the integrity of the system.

By testing these proof points, we aim to identify a set of foundational standards that can govern the future of decentralized transactions facilitated by the banking industry. The success of this initiative will not only depend on technological capabilities but also on fostering collaboration between banks, regulators, and technology providers to enable a secure, scalable, and compliant decentralized financial infrastructure.

Key Technological Principles

Our experiment will adhere to several guiding technological principles to ensure transparency, scalability, and inclusivity in developing decentralized financial infrastructure:

1 **100% Open Source.** All components of the project will be fully open source to promote transparency, security, and collaboration across the financial and technology sectors. Open source development encourages peer review, reduces the likelihood of hidden vulnerabilities, and fosters innovation by allowing anyone to contribute to the project's improvement.

2 **Incremental Development with Maximum Reuse of Existing Public Open Source Technology.** The project will be built incrementally, leveraging existing public open source technologies to the greatest extent possible. This approach reduces development time, costs, and risks by building on proven technologies while ensuring the flexibility to adapt and evolve as needed.

3 **Open Participation.** The project will be open to participation from a wide range of stakeholders, including banks, technology providers, regulators, academia, and individuals who can contribute, such as community and key opinion leaders. Open participation ensures diverse perspectives are considered, leading to a more robust and universally acceptable solution.

4 **Progressively Decentralized Governance.** Governance of the project will start with a core group of stakeholders but will progressively decentralize to include a broader community. This ensures that decision-making processes are transparent, democratic, and aligned with the interests of all participants. Progressive decentralization also helps in building trust and ensuring the long-term sustainability of the ecosystem.

Public chain Considerations

The experiment aims to leverage Distributed Ledger Technology (DLT) to enable direct, peer-to-peer transactions that are securely verified and recorded across a decentralized network. DLT eliminates the need for traditional intermediaries, which can reduce transaction processing times and costs. However, to integrate this decentralized model into the existing financial infrastructure, certain key considerations must be addressed:

1. **Financial Infrastructure Compatibility.** While the decentralized model promotes efficiency, the system must still align with the fundamental requirements of the financial sector. This includes ensuring adequate liquidity is available, which will be provided by commercial banks. Additionally, settlements between banks will need to eventually occur in central bank money to ensure regulatory compliance and stability.
2. **Layer 2 (L2) and Layer 3 (L3) Solutions.** The experiment will consider using open-source privacy enabling solutions deployed on Ethereum L2 or L3. These solutions offer enhanced scalability, privacy, and lower transaction costs while benefiting from the security of the Ethereum mainnet. Similarly, protocols like zkSync, Starknet, and Arbitrum will be considered to provide Confidential DeFi solutions that enable private transactions with lower fees and higher throughput.
3. **Alternative Platforms.** Besides Ethereum-based solutions, other platforms such as Avalanche are also being considered for their capability to run Confidential DeFi subnets. These subnets can provide customizable environments that support privacy features and regulatory compliance while maintaining high performance and scalability.

A Potential Transaction Privacy and Selective Disclosure Solution Design

To address privacy and compliance needs, the experiment will focus on designing a transaction solution that leverages zero-knowledge proofs, specifically zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), to enable private transactions while still adhering to regulatory requirements:

1. **Development of a Token Standard Using zk-SNARKs.** The solution will involve developing a new token standard that incorporates zk-SNARKs directly into its framework. This standard will allow transactions to be conducted privately, where the details of the transaction (such as the sender, receiver, and amount) are hidden from public view while still being verifiable by network nodes.
2. **Issuance of Privacy-Enhanced Tokens.** Tokens using zk-SNARKs will be issued to protect transaction details. By integrating zk-SNARKs into the token's transfer functions, transactions can be validated without revealing sensitive information. An alternative approach, particularly for Nightfall or Starlight, could involve using

a certificate-based system to ensure privacy while still enabling compliance with regulatory requirements.

3 **Selective Disclosure and Regulatory Compliance.** To balance privacy with regulatory requirements, our experiment incorporates a selective disclosure mechanism that leverages the inherent transparency, security, and immutability of blockchain technology. While blockchain networks are designed to maintain comprehensive transaction records through a consensus-driven process — where each transaction is verified, grouped into blocks, and cryptographically linked to previous blocks — ensuring that these records remain secure and immutable, the challenge is to achieve this without compromising the privacy of participants. Traditionally, blockchain stores information such as the time, date, transaction amount, and the details of users participating in the transaction. The extent of information disclosed about participants depends on the privacy implementation of the blockchain network. In this experimental phase, how privacy is structured will be a key focus, aiming to enable a robust compliance framework that supports both financial transparency and user privacy. The concept of selective disclosure allows us to approach compliance differently in DeFi environments, particularly for regulatory requirements like Anti-Money Laundering (AML), Counter-Terrorism Financing (CFT), and Know Your Customer (KYC) obligations. This will be achieved in the following ways, depending on the outcome of this project:

1 **Direct Access for Regulatory Authorities.** A critical innovation in this framework is providing direct, controlled access for regulatory authorities to the relevant transaction information when necessary. This selective disclosure model ensures that regulators can access detailed sender and receiver information under specific conditions, such as suspected fraudulent transactions, while maintaining overall privacy standards. This raises a key question: Would the traditional practice of reporting suspicious transactions be needed if regulatory authorities could directly access relevant data on the blockchain in real-time? This approach could significantly reduce the burden on financial institutions to report suspicious activities while enhancing the speed and precision of regulatory interventions.

2 **Traceability and Investigation of Fraudulent Transactions.** In cases where fraudulent activity is suspected, the selective disclosure mechanism allows the beneficiary's details to be quickly identified and investigated. This can be achieved without compromising the privacy of legitimate users. Only in specific cases where fraud or financial crime is detected will the necessary transaction and participant details be disclosed to authorized investigators, preserving the overall integrity and confidentiality of the blockchain network.

3 **Secure Subnet for KYC Information.** Each blockchain address can be linked to comprehensive KYC information stored on a separate, secure subnet. This

subnet would be accessible only to authorized entities, such as regulatory bodies and designated compliance officers, when necessary. Such a setup ensures that while transaction data remains private on the main blockchain, sufficient information is available on demand to meet compliance and reporting requirements. The use of the information on the subnet can increase efficiency and reduce costs for all participants as the information only has to be collected once instead of each party gathering all information individually.

4 **Whitelist and Blacklist Mechanisms.** By integrating whitelist and blacklist functionalities into the blockchain's compliance layer, the system can automatically flag addresses and transactions associated with known suspicious activities or sanctioned entities. This automated mechanism would be highly effective in preventing and detecting financial crimes, such as money laundering or the financing of terrorism (CFT). Addresses that comply with regulatory standards could be whitelisted, while those linked to illicit activities could be blacklisted, enabling a proactive approach to transaction monitoring.

5 **Automated Risk Categorization and Transaction Monitoring.** A blockchain protocol can employ automated analysis tools to assign a risk category to each transaction based on various factors, such as transaction size, frequency, or involvement of flagged addresses. Transactions with higher risk scores could trigger additional scrutiny or require enhanced due diligence, thereby supporting robust transaction monitoring without unnecessary intervention in low-risk activities. This automated categorization allows compliance teams to focus on high-risk areas, improving efficiency and effectiveness.

In our experiment, we intend to build the proposed system to not only meet but also surpass traditional compliance standards. It will provide regulators with the tools needed to combat financial crime while respecting the privacy and autonomy that decentralized technologies have. This hybrid approach allows for a balanced ecosystem where privacy and compliance coexist, aligning with the principles of both decentralized finance and regulatory oversight. It also ensures that processes can be supported in a common approach rather than reproduced by each commercial bank (or another ecosystem party).

Our perspective on Programmability

In the traditional finance world, programmability often refers to the ability to execute conditional payments, such as setting up automated transfers or payments that occur when specific criteria are met. However, our approach to programmability goes far beyond this limited understanding — it means harnessing the full power of smart contracts.

Smart contracts are not just about automating simple conditional payments; they are fully programmable electronic transaction protocols that, once developed by an independent party, can autonomously execute the terms of

any contract. These contracts can encapsulate complex business logic, ensuring that all terms — whether related to payment conditions, liens, confidentiality, or even enforcement actions — are fulfilled automatically and transparently. The use of smart contracts is designed to achieve several core objectives: minimizing both malicious and accidental exceptions, reducing the need for arbitration, cutting enforcement costs, and lowering other transaction-related expenses.

By utilizing smart contracts, entirely new use cases and business models will be developed. Unlike traditional conditional payments, which are relatively straightforward, smart contracts allow for the co-creation and co-design of sophisticated financial products and services that are tailored to specific user needs. These contracts can accommodate complex conditions, multi-party agreements, and dynamic variables, all of which can be encoded and validated before being deployed on-chain.

Intended Transaction Visibility

The proposed privacy model will determine different levels of transaction visibility for various participants in the network:

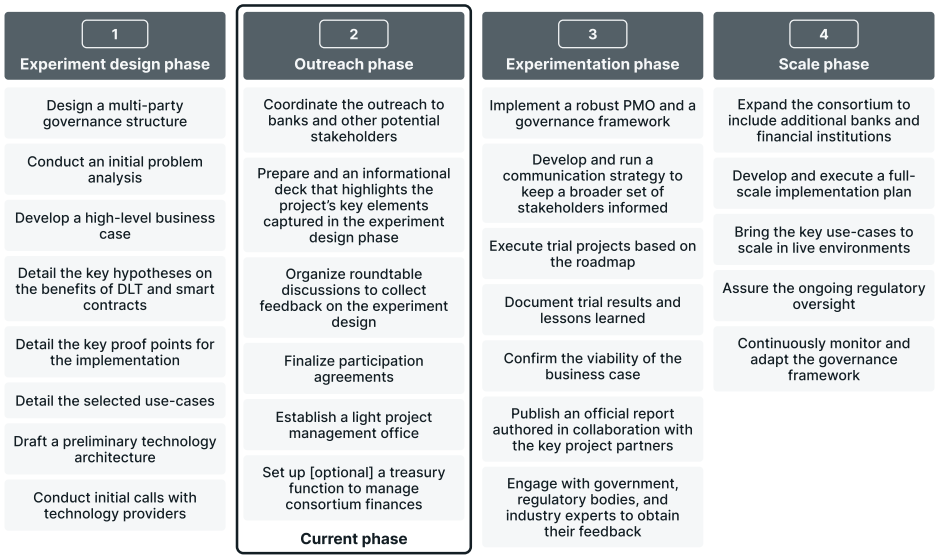
1. **Prover (Sender).** The sender, who generates the transaction, will have full visibility of the transaction details, including the recipient's address and the amount being transferred. The sender also creates a zero-knowledge proof that confirms the validity of the transaction without disclosing the specifics.
2. **Verifier (Network Nodes).** Network nodes (validators) will be able to verify the transaction's validity using the zero-knowledge proof. They will not have access to the actual details of the transaction, such as the amount or the recipient, ensuring privacy while maintaining trust and integrity in the network.
3. **Recipient.** The recipient will know they have received a transaction and will be able to see the transaction details related to their own wallet. This includes the sender's address (if disclosed by the sender) and the amount transferred.
4. **Public.** To the general public or anyone examining the blockchain, the transaction details are hidden. Observers will only be able to see that a transaction has occurred and that it has been validated. The specifics of the transaction, such as the parties involved or the amounts transferred, will remain confidential.
5. **Regulator.** Regulatory authorities will have access to transaction details through a selective disclosure mechanism. This mechanism will allow regulators to request and obtain specific information necessary for compliance and oversight while ensuring the privacy of other transaction participants.

Our experiment aims to establish a secure, scalable, and compliant framework for public decentralized transactions within the financial industry. The use of advanced cryptographic techniques like zk-SNARKs, combined with open public chain solutions and progressive governance models, will enable the creation of a robust and future-

proof decentralized financial infrastructure that meets the needs of all stakeholders.

05 Call To Action: join our emerging Ecosystem

Once the initial partners are aligned on the essential steps to kick-start the project, the focus will shift to building a robust public-private partnership. This partnership will form a vibrant community around the project, enabling participants to share lessons learned, generate new ideas, and demonstrate how innovative processes can work in practice. This community-driven approach will be fundamental to the project's success and will lay the groundwork for scaling and further adoption.



Outreach Phase: Building the Community and Ensuring Regulatory Engagement

During the Outreach Phase (Phase 2), the goal is to expand the consortium beyond the initial partners by reaching out to additional banks, financial institutions, technology providers, and other stakeholders. Coordinating outreach efforts will involve preparing informational materials, such as detailed project decks, to highlight the key elements captured during the experiment design phase. Engaging in roundtable discussions with these stakeholders will be crucial to gather feedback on the experiment design and refine the approach.

Engagement with regulatory bodies is especially critical during this phase to ensure the project aligns with legal and compliance requirements. Establishing early and continuous dialogue with regulators will help navigate the complexities of legal compliance and foster a regulatory environment conducive to innovation. This step will ensure that new processes, especially those involving smart contracts and privacy-preserving technologies we will use, e.g. zk-SNARKs, are utilized in a way that meets existing and evolving regulatory standards.

Experimentation Phase: Implementing and Testing in a Controlled Environment

In the Experimentation Phase (Phase 3), the focus shifts to implementing a robust governance framework and running the experiment based on a clearly defined roadmap. Given

that it is not the intention of this initiative to build and maintain a new DLT platform from scratch, leveraging an existing public blockchain is our intention. Utilizing a well-established platform, such as Ethereum with its Layer 2 or Layer 3 solutions, zkSync, or Avalanche, allows for scalability and greater flexibility in adapting to lessons learned during the pilot phase.

The experiment will involve developing use cases in close partnership with stakeholders, including clients and regulatory bodies, to validate their practicality and compliance. As lessons are documented and evaluated, the viability of the business cases will be confirmed. The insights gained will guide the refinement of both the technology and governance models, ensuring that they serve broader societal benefits.

Scale Phase: Expanding the Ecosystem and Ensuring Regulatory Oversight

If the pilot experiments are successful, the project will move into the Scale Phase (Phase 4), where the consortium will be expanded to include additional banks, financial institutions, and other relevant stakeholders. This phase focuses on executing a full-scale implementation plan, bringing the key use cases to live environments, and ensuring continuous regulatory oversight.

The community will continue to grow and evolve, incorporating new participants who can contribute fresh perspectives and expertise. The governance framework will be monitored and adapted to meet the dynamic needs of the expanding ecosystem, maintaining a balance between innovation and regulatory compliance.

Wrapping up

The success of this initiative is not solely determined by the technology or the immediate adoption of blockchain-based solutions. Rather, it is measured by the lessons learned, the ability to create a more efficient, transparent, and inclusive financial ecosystem, and the positive impact on society. By fostering collaboration between public and private sectors and engaging deeply with regulatory bodies, the project aims to lay the foundation for a future-ready, compliant, and decentralized financial infrastructure where commercial banks have a new – impactful and necessary – role to play.

Igor Mikhalev is a Partner and the leader of the Emerging Technologies Strategy pracrice at EY-Parthenon, helping clients – commercial and government organizations – develop novel decentralized business models and business ecosystems with blockchain technologies and digital currencies.

Prior to joining EY-Parthenon, Igor headed up Crypto, Digital Currency, and Digital Ecosystems topics at BCG. Igor is collaborating with academia (UvA, MIT) on research projects focused on CBDCs and the macroeconomic impact of the introduction of digital currencies.

Sebastian Kortmann is professor of Strategy and Innovation and the Director of the Amsterdam MBA

at the University of Amsterdam Business School. Sebastian has consulted with and/or provided training for firms, such as Boston Consulting Group, Porsche Digital, Thyssen Krupp, Nike, Johnsen & Johnsen, Audi, or BMW.

Furthermore, he has been named one of the "Top 40 under 40 most outstanding Business School Professors worldwide" by Poets & Quants.

Joris Dekker represents ABN AMRO on all Digital Euro related matters. He is co-author of a publication on "decentralized governance design, modeling fractional reserve banking towards an ecosystem with CBDC" and is author of the Dutch Banking association whitepaper on the opportunities for innovation in payments.

Thanks to his previous positions within ABN AMRO he is an expert in the working of Financial Market Infrastructures that are responsible for the movement of money and securities around the world and has broad experience in liquidity management.

Authors