White paper

April 2020

Central Bank Digital Currency: an innovation in payments

George Calle
Daniel Eidan

Table of Contents

1 Introduction

This paper examines the increasing interest around central bank digital currency (CBDC) across the globe, focusing on progress made to date. A range of projects completed over the past five years with differing scopes and mandates have provided useful insight, and now central bankers focused on issuing a digital currency may choose from a variety of implementations. This paper outlines the existing applications of CBDC, explores potential implementation options, and points to potential technological solutions.

This paper separates the benefits and findings from CBDC projects into two categories: wholesale and retail. Wholesale CBDC is limited to commercial banks, clearing institutions or other entities that have traditionally had access to central bank reserves. Retail CBDC has a larger user base, and can involve corporates, small businesses, and even individuals. The distinction between the two types is useful because different types of end users often have different requirements and preferences.

Wholesale CBDC is the latest step along a 50-year journey for central banks to use new technologies to enhance the efficiency and resilience of a wholesale payments system within a given currency zone. This made wholesale CBDC a perfect early blockchain project, as the network of users and participants was already fixed, and central banks refresh or examine technical improvements to their RTGS (real time gross settlement) systems every five to seven years.

Meanwhile, interest in the efficacy of retail CBDC has surged, and central banks around the world are conducting research and embarking on proofs of concept. There is a plethora of private sector options for individuals and businesses to interact with money. For example, many FinTech companies are providing new services on top of the existing banking infrastructure. Retail CBDC, however, is an opportunity to extend access to digital central bank money.

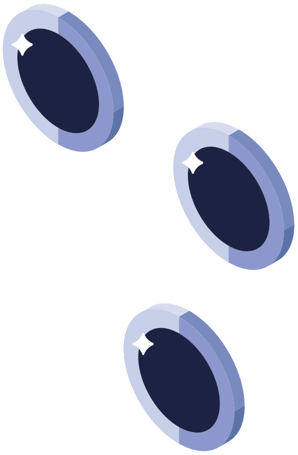
The reasons for issuing and using central bank digital currencies differ widely, depending on the particular central bank and the existing payment systems. Specifically, for retail CBDC, central banks' motivations include promoting financial inclusion, increasing seigniorage income, facilitating monetary policy, linking payments to identity, enabling participation in a tokenized financial ecosystem, fostering competition within the private sector, providing a cash alternative, or otherwise generally modernizing payments.

This paper does not debate the economics or monetary policy questions of a CBDC but instead focuses specifically on the technology–the medium on which the money is issued and how transactions are recorded. Just as the economies, consumer and industry preferences, and political makeups of currency zones comprised of nations and regions differ greatly, there will be no 'one size fits all' CBDC. Rather, CBDC will comprise a range of methods for a central bank to offer purchasing power to various participants, both at the wholesale and retail levels.

The gap between central bank innovation at the wholesale level and FinTech innovation at the retail level may soon narrow. Central banks planning to issue a retail CBDC have a lot to learn from existing wholesale CBDC projects, which can inform design decisions and inspire potential applications. At the same time, new emergent models show that a token-based CBDC architecture using blockchain may enable connections between wholesale and retail participants that previously could not and did not exist.

> A token is a digital representation of an asset. Tokens issued on a blockchain platform can be transferred directly between peers and executed on using smart contracts without the risk of the token being double spent.
>
> Central bank money can be represented digitally as a token as well as an account balance.

The next section of the paper walks through the different models of existing wholesale CBDC and explains how and why blockchain is used. Section three considers the array of models proposed for a retail CBDC, highlighting high profile developments. Section four connects the discussion around wholesale and retail CBDC applications to a potential high-level architecture for CBDC. The fifth section explains the specific advantages for blockchain-based CBDC systems, focusing specifically on the features of Corda to anchor the discussion. Section six looks forward to where this research may take us in the future.



2 Wholesale CBDC

Both the mechanics and scope of wholesale payments have progressed since the founding of Fedwire in 1970, the first payments system with capabilities similar to modern real time gross settlement (RTGS) functionality. Over the following decade, a few other large economies developed RTGS systems in order to reduce settlement risk, and by 2006, 93 countries had RTGS systems in place.[1] While RTGS decreased credit risk, this came at the expense of higher liquidity costs. This resulted in a growing demand for liquidity savings mechanisms (LSM) throughout the mid-2000's, which use netting to ease the amount of liquidity required for payments.[2] More recently, RTGS systems have increased the hours of operations and have broadened access to more participants in a given currency zone, though access is still generally very limited.

As central banks modernize these systems every few decades, CBDC provides a new tool in the ongoing evolution of wholesale payments. The key function of a wholesale CBDC is to allow banks to extinguish debts between each other resulting from the build-up of credit risk between them. The nature of blockchain enables this settlement to be real-time and atomic. As it pertains to settlement, the term 'atomic' describes a scenario involving two assets where the transfer of each is dependent on the transfer of the other—meaning either both transfers happen or neither happen.

This is a powerful concept applicable across any payment situation, especially when the payment leg is a tokenized wholesale CBDC, allowing financial markets to settle in central bank money with certainty. It becomes even more important for payments that require complex counterparty workflows and interactions between participants. This section discusses some of the findings from central bank projects across payments scenerios.

Findings from completed Wholesale CBDC projects

Atomic Delivery versus Payment

Payments, specifically wholesale CBDC which can be transferred easily between financial institutions, are an enabling force for a robust capital markets ecosystem.

Tokenizing central bank reserves may allow for additional operational improvements beyond what existing financial market infrastructures can provide, such as 24/7 access to the payment system and T+0 settlement. Current market infrastructures often require downtime or have settlement delays that are difficult to reduce. However, many blockchain-based networks live today do not require downtime (due to increased resilience without a single central operator), and many shorten settlement time by reducing reconciliation (as a network will always maintain a single version of truth for a given asset).

Further, today's cash payments system does not necessarily interact smoothly with the capital markets system. The Bank of Canada's Project Jasper culminated in a study of settling securities domestically with TMX, a Canadian stock exchange using digital central bank cash. In Phase 3 of this project, blockchain technology allowed for "loose coupling" of disparate payment and capital market infrastructures, without requiring a redesign of each infrastructure or requiring any changes to governance. Specifically, blockchain was used to help different systems interoperate more smoothly.

[1] Morten Bech and Bart Hobijn, "Technology Diffusion within Central Banking: The Case of Real-Time-Gross Settlement", Federal Reserve Bank of New York, September 2006.
[2] Morten Bech and Jenny Hancock, "Innovations in Payments", Bank for International Settlements, 01 March 2020.

Bank of Canada: Project Jasper Phase 3

Date: Paper published Oct 2018
Purpose: Securities settlement using DLT
Technologies: Corda
Participants: TMX, R3, Payments Canada, Bank of Canada, Accenture, Canadian banks
Findings:

- Securities and cash were brought on-ledger through the issuance of Digital Depository Receipts (DDRs) by CDS and the Bank of Canada, respectively, allowing POC participants to settle securities against central bank cash on the distributed ledger.

Enabling cross-border payments

Wholesale CBDC can expand access to members within a currency zone and to those outside of it, while still maintaining the same risk profile. Tokenized central bank money is an incredibly scalable tool for enabling international banks to hold reserves of any central bank without the requirement of that bank's corresponding central bank to guarantee the account.

Specifically, Wholesale CBDC can be used for atomic payment vs. payment (PvP), which has manifested in new applications in the FX markets. For example, in Project Inthanon-Lionrock, The Bank of Thailand, in conjunction with the Honk Kong Monetary Authority created a cross border corridor, enabled FX price discovery, and facilitated atomic PvP.[3]

Bank of Thailand: Project Inthanon Phase 3

Date: Paper published Jan 2020
Purpose: Leveraging DLT to Increase Efficiency in Cross-Border Payments
Technologies: Corda
Participants: Bank of Thailand, HKMA, R3, Thai banks, HK banks
Findings:

- A cross-border corridor network was created where funds transfers can occur instantaneously on a peer-to-peer basis.
- The design allows foreign exchange (FX) price discovery on the corridor network that enables on-demand FX conversion and FX settlement is done in an atomic payment-versus-payment (PvP) manner.
- Regulatory monitoring and compliance were put in place where feasible.

[3] "Inthanon-LionRock: leveraging distributed ledger technology to increase the efficiency of cross-border payments", Bank of Thailand and Hong Kong Monetary Authority, January 2020.

More efficient complex payment workflows

Finally, central bank run experiments show how core existing features of RTGS systems can be improved using blockchain. In one example, decentralized liquidity savings mechanisms may be more effective in reducing gridlock than existing approaches. Further, decentralized systems may enable banks to have more flexibility than they currently have using centralized liquidity savings mechanisms. Each bank could have more control and real time visibility of how their payments are netting network-wide, reducing reliance on the central operator for that netting calculation. Greater control and flexibility with liquidity would benefit all market participants.

A Proposal for a Decentralized Liquidity Savings Mechanism with Side Payments– Adam Furgal & Dave Hudson (R3), Rodney Garratt, Zhiling Guo

> “Project Ubin explores the use of distributed ledger technology for interbank payment and settlements with LSMs introduced for the purpose of gridlock resolution. Gridlock refers to a situation where banks are unable to settle any payments because the liquidity available to each participant in the payment system is less than any of their outstanding payment obligations. The standard approach to gridlock resolution is to look for netting cycles within the set of gridlocked payments that deliver net amounts that can be settled with available liquidity....The Corda workstream achieved the highest degree of decentralization in implementing the decentralized gridlock resolution. It proposed a graph-based queue-scan approach to facilitate the discovery of queued payments in the decentralized environment. It further developed a new cycle-based algorithm that consists of three stages: detect, plan, and execute.[4]

[4] Adam Furgal, Rodney Garratt, Zhiling Guo, Dave Hudson, "A Proposal for a Decentralized Liquidity Savings Mechanism with Side Payments", R3, 11 June 2018.

3 Retail CBDC

Unlike wholesale CBDC, retail CBDC does not currently exist in production. Retail generally refers to the general public, corporates and certain financial institutions that currently do not have access to central bank money. As a result, experiments in the space are incredibly novel. However, central banks across the world have are beginning to commit resources towards implementing retail CBDC.

We are at an important juncture where we can see multiple potential avenues through which a retail CBDC could exist in the near future. This section briefly walks through a recent history of retail payments, including as it pertains to blockchain based instruments. Then, the section explores a few notable proposals for a retail CBDC, providing frameworks for the different types of models to date.

Private sector payments innovation

Private sector payments innovation has come in two, completely separate movements:

For widely used payment systems, the initial body of work focused on the front end of the system–the interfaces users directly interact with. This included new ways of initiating payments, such as mobile and contactless payments, and overlay systems, which wrap existing settlement systems and most of an existing network around fresh interfaces.[5] This is exemplified by apps like Apple Pay and Venmo, which have identified new ways people are using digital technologies and are either building new applications or shaping existing services to fit the customer's convenience.

Over the past decade, an increasing number of nations have implemented faster or real-time payments systems for the general public. These systems include UK Faster Payments in the UK, IMPS in India and NPP in Australia. In 2019 14 countries implemented real-time payments, increasing the number of live systems to 54 globally.[6] While there is no standardized approach, these services provide new digital rails for payments generally within a currency zone, accessible to retail participants and open 24/7. Importantly though, these services are offered via consumers' bank accounts, and transactions are settled inter-bank.

Full stack payment solutions like WeChat and Alipay in China have established closed-loop payment systems. The significance of a closed-loop system is that it includes both payer and payee, which obviates any settlement across separate systems. This is an infeasible global solution, as it would lead to a coordination challenge, creates to concentration risk[7] and ultimately comes at the cost of a lack of interoperability.

Meanwhile, the very concept of cryptocurrency introduced a parallel revolution in open payments that has taken the exact opposite approach to the developments above. Satoshi Nakamoto's Bitcoin white paper did not accompany any user interface for engaging with the system. Rather, the paradigm shift was the decentralized nature of the network and the Bitcoin asset themselves. But while payments were the initial Bitcoin use case, as stated in the first line of the white paper's abstract, it turns out that Bitcoin is a very poor payment asset. Part of the issue is volatility. As a result, the private sector has responded with stablecoins, which are blockchain-based tokens that aspire to achieve a stable value, usually $1 USD.

[5] Bech and Hancock, 2020.
[6] "Flavors of Fast Report 2019", FIS, 2019.
[7] Bech and Hancock, 2020.

The space has quickly evolved from firms dubiously claiming[8] that they've backed their digital currency with reserves without proof, to a new crop of businesses that have registered with required regulators and undergo routine audits.[9] Recently, Wells Fargo has announced a pilot for a dollar-linked stablecoin for international inter-firm settlement[10] and J.P. Morgan has launched its JPM Coin for instantaneous inter-bank payments.[11]

Progress to date and a review of the literature

Central banks have a unique opportunity to leverage the outcomes of both technological movements. Issuing digital money to non-wholesale participants is a unique challenge for many central banks since they must account for the inclusion of participants whom they currently do not engage digitally. As a result, approaches to projects have varied significantly, and there has been a recent flood of research examining novel approaches. The BIS has categorized the approaches in three ways.[12]

- Hybrid: the central bank issues the CBDC but intermediaries facilitate retail payments
- Indirect: the CBDC is a claim on a wholesale intermediary
- Direct: the central bank issues CBDC directly to retail users

The remainder of this section will examine a few notable projects and proposals for a retail CBDC system, citing research from central banks themselves.

Hybrid CBDC

Many central banks are taking a collaborative approach with the private sector. For example, the Bank of England[13] is researching what it calls the 'platform model', in which the bank is the only entity allowed to create or destroy a token the 'core ledger', while leaving 'payment interface providers' (PIPs) to interact with end users. The proposal gives the PIPs the responsibility to maintain KYC checks, while also giving them the freedom to provide customers with additional 'overlay services'.[14] Additionally, The People's Bank of China has discussed a model in which the PBOC would issue and redeem retail CBDC through a network of domestic commercial banks.[15]

Indirect CBDC

While hybrid proposals separate out responsibilities between private businesses—FinTech firms, tech companies or banks–and the public sector, asset issuance and network governance ultimately remain in the hands of the central bank. Indirect CBDC goes a step further.

Researchers at the IMF recently coined the term 'synthetic CBDC' (sCBDC) to describe a model in which a non-central bank entity, such as a commercial bank, can issue a stablecoin backed by central bank reserves.[16] Importantly, the asset held by retail participants in this model is actually a liability of the private sector intermediary. This could be a modern technical solution for an existing concept of narrow banking.[17]

[8] Yogita Khatri (CoinDesk), "Tether Says Its USDT Stablecoin May Not Be Backed By Fiat Alone", 12 May 2019.
[9] George Calle and Diana Barrero Zalles, "Will Businesses Ever Use Stablecoins?", R3, 26 March 2019.
[10] Ian Allison (CoinDesk), "Wells Fargo to Pilot Dollar-Linked Stablecoin for Internal Settlement", 17 September 2019.
[11] Press Release: "J.P. Morgan Creates Digital Coin for Payments", J.P. Morgan, 14 February 2019.
[12] Raphael Auer and Rainer Boehme, "The Technology of Retail Central Bank Digital Currency", Bank for International Settlements, 01 March 2020.
[13] Other similar 'layered' proposals include New Payments Platform in Australia, Payments Canada's Modernization initiative, along with Pay.UK's New Payments Architecture Program (source: Bank of England).
[14] "Central Bank Digital Currency: opportunities, challenges and design", Bank of England, 12 March 2020.
[15] Etienne Jinze (Binance Research), ""First Look: China's Central Bank Digital Currency", 28 August 2019.
[16] Tobias Adrian and Tommaso Griffoli, "The Rise of Digital Money", International Monetary Fund, 15 July 2019.
[17] A narrow bank is a strictly deposit taking bank with a reserve account at the central bank that is restricted from making loans, reducing credit risk to near zero.

Direct CBDC

Additionally, Sveriges Riksbank has announced a pilot for a digital version of its currency for retail use, dubbed the e-krona. The central bank has proposed that the central bank could offer access to its currency in two ways–through a 'value model' (akin to tokenized CBDC described above) and via central bank accounts.[18] The Swedish central bank describes the e-krona as a complement to physical cash.

Implementations will likely differ based on region to fit in with existing infrastructure.

It is important to remember that end consumers are not the only intended user of retail CBDC. In some currency zones, access to the central bank is tiered - that is, not all financial services actors are wholesale participants. Additionally, large corporates and some financial entities run treasury departments, which would benefit from atomic transactions. Finally, businesses and supply chains are complex, and access to a tokenized CBDC could enable a more flexible set of payments services. Learnings from non-CBDC exercises can help inform these nuances in a given currency zone. The development of faster payments is certainly relevant. Additionally, R3's report on stablecoins studies the structures of popular payment systems in the US, applying each to the various types of transactions they could facilitate. ACH (Automated Clearing House), for example, is a pull payment method[19], which would be highly relevant for blockchain applications where, say, a smart contract initiates payment upon confirmation of delivery of a good.[20]

Innovative research: adding privacy overlays to tokenized money

The European System of Central Banks (ESCB) developed a PoC for retail CBDC. The proof of concept drawn up by the ESCB demonstrates that it is possible to construct a simplified CBDC payment system that allows users some degree of privacy for lower-value transactions, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks.[21]

Exploring anonymity in central bank digital currencies

> "That proof of concept boasts several novel features developed by the ESCB's EUROchain research network (with the support of Accenture and R3) using distributed ledger technology (DLT). It provides a digitalization solution for AML/CFT compliance procedures whereby a user's identity and transaction history cannot be seen by the central bank or intermediaries other than that chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional checks are delegated to an AML authority. This is achieved using "anonymity vouchers", which allow users to anonymously transfer a limited amount of CBDC over a defined period of time.

[18] "E-krona project, report 2", Sveriges Riksbank.

[19] Push transactions mean that the payment is initiated by the sender. Think of how when a friend puts cash in your hand, they are pushing ownership of the money to you. On the other hand, pull transactions are initiated by the recipient. Think of depositing a check, where ownership is dependent on you telling your bank to pull money from the senders account into yours.

[20] Calle and Zalles, 2019.

[21] "Exploring Anonymity in Central Bank Digital Currency", European Central Bank, December 2019.

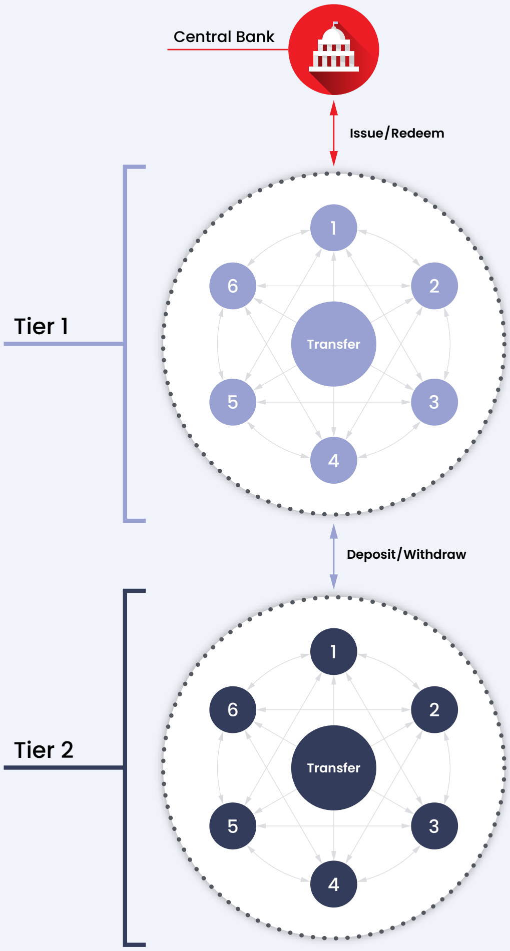
4 Generalized implementation options for CBDC

This section will outline two broad CBDC implementations to demonstrate a few methods for interacting with central bank money. Both models have three different types of participants; central banks, financial institutions with access to central bank's balance sheets and retail institutions without access to the central bank's balance sheets.

1. A two-tier system where every participant has access to the distributed ledger.
2. A two-tiered system where not all the participants have access to the ledger and therefore rely on API access with institutions who have ledger access.

These models can be used to form the basis of the wholesale and retail use cases described in the sections above.

Image 1: Two tier token system



This model is broken down into three different types of participants:

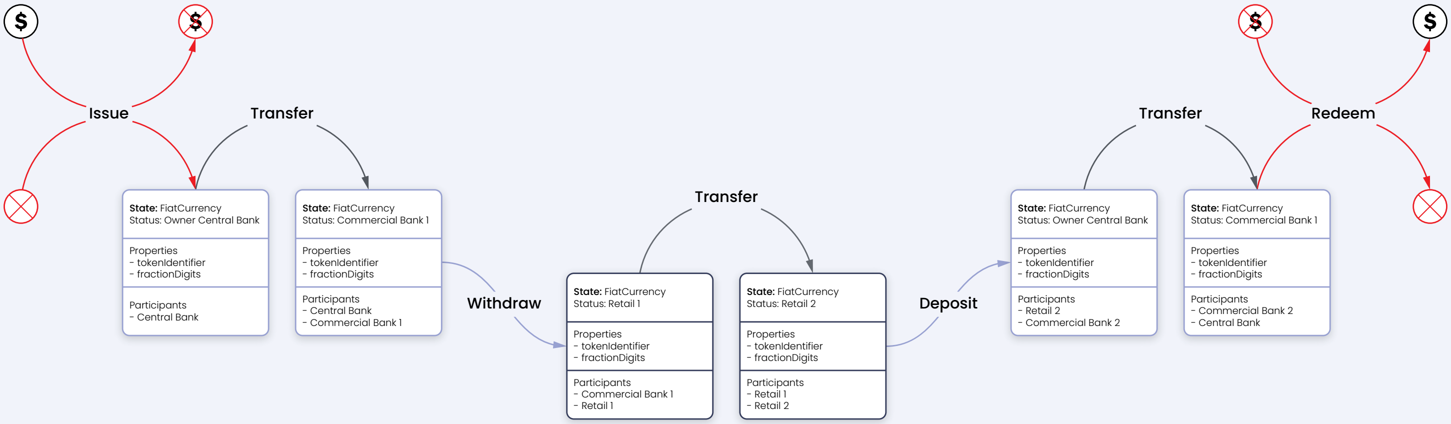
1. **Tier 0**: Institutions that can issue, redeem and transfer tokens. In most models this will represent central banks
2. **Tier 1**: Privileged institutions that can interact with tier 0 and hold and transfer tokens themselves. In most implementations this will represent wholesale financial institutions
3. **Tier 2**: Institutions that can interact with tier 1 and hold and transfer tokens between themselves. In most implementations this will represent retail user - such as FinTechs, corporates and individuals – or wholesale members of another currency zone.

Two-tier system with direct ledger access

We can demonstrate a CBDC as a sequence of state changes as depicted in the diagram below:

1. Collateralization of fiat currency against the issued CBDC as a bearer asset
2. Wholesale transfer moves the CBDC from the central bank to participant 1
3. Withdraw, representing the movement of the CBDC from the wholesale ecosystem to the retail ecosystem
4. CBDC transfers to from one retail holder to another
5. Retail user deposited the CBDC back into the wholesale system
6. Wholesale transfers back the CBDC to the central bank
7. The central banks redeems the CBDC against the original fiat funds

Image 2: Ledger recordings of potential transactions



Tokenized CBDC presents the opportunity to extend access central bank money. Here are a few examples of how the two-tier model can be used in situations where every participant has direct ledger access:

1. **Retail CBDC (hybrid)**: The central bank is the issuer and redeemer. Tier one participants are the current wholesale participants and tier two are domestic retail participants, which could be FinTechs, corporates or individuals. This would enable access to digital central bank liabilities at the retail level.
2. **Wholesale CBDC (cross-border settlement)**: The central bank is the issuer and redeemer. Tier one participants are the current domestic wholesale participants and tier two are foreign wholesale institutions. This would enable cross border wholesale payments (PvP) and foreign securities settlement (DvP).
3. **Wholesale CBDC (liquidity swap lines[22])**: Two or more central banks join each other's tier 1. This would enable a central bank or a set of central banks to have issuance and redemption privileges with a foreign central bank, potentially allowing it to issue foreign CBDC to its wholesale network.

[22] Central banks currently offer swap lines to provide a foreign central bank access to its money, helping the originating central bank provide liquidity for its currency in overseas markets.

Of course, all of these examples have open governance questions that central banks will be responsible to answer. For example, what are the privacy controls around payments? Will CBDC be anonymous like cash, or would there be some level of reporting for large transactions? What are the network boundaries for the CBDC? These are policy questions, not technology questions. What is important is that a tokenized CBDC gives the central bank the capability to implement the solution that enables the question.

Extending access to non-ledger participants through APIs

Not all participants will have access or want to be the custodian of their own CBDC. To enable this we introduce the notion of API accounts. API accounts are a mechanism for a node to act on behalf of other users who can communicate with the node through an API.

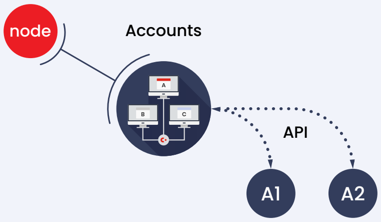
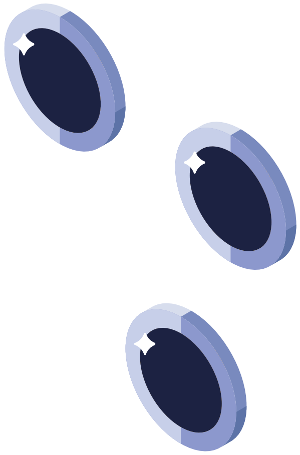


Image 3: Account based access to a node

In practice, any node—a participant on the network—manages an account for every user it represents. This is similar to bank accounts that we use today. Diagram 3 shows how an API account can extend access to off-ledger participants. Diagram 4 shows how API accounts can be added at any tier of the two-tier architecture introduced earlier in this section. Each tier can extend their functionality to members that currently don't have access.



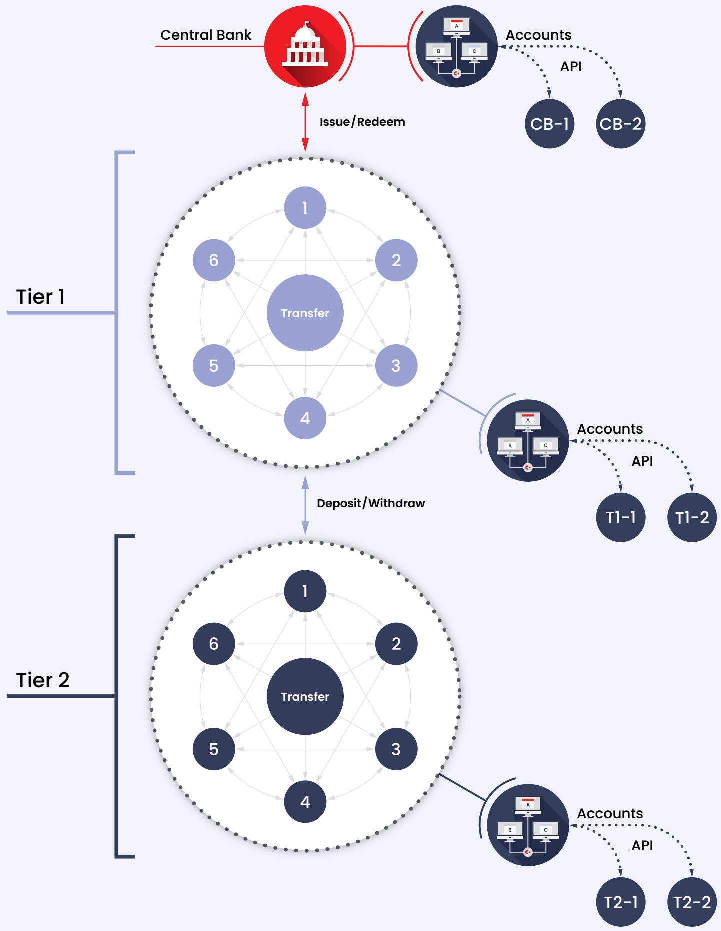


Image 4: Account based access to CBDC

When applied to the two-tier model, API accounts extend the potential implementation options for a CBDC:

1. **Retail CBDC (indirect)**: This model can be relevant for a narrow bank that collateralizes end users' accounts with tokens, giving small business or individual deposit account holders access to CBDC
2. **Wholesale or retail CBDC (direct)**: The central bank could simply extend account access to additional participants. This idea was proposed in 2015 via a staff report from the Federal Reserve Bank of New York that suggested the creation of a new offering called Segregated Balance Accounts (SBA). SBAs would allow a bank to set up an account at its Federal Reserve Bank using funds from the broader money market.[23]

These are only a few of the ways central banks can extend the use and utility of money using a CBDC. These examples can be combined in ways to produce more combinations that fit the requirements of each economic region. With so many possibilities for CBDC the mere distinction between wholesale and retail may blur.

[23] Rodney Garratt, Antoine Martin, James McAndrews and Ed Nosal, "Segregated Balance Accounts", Federal Reserve Bank of New York Staff Reports, August 2015.

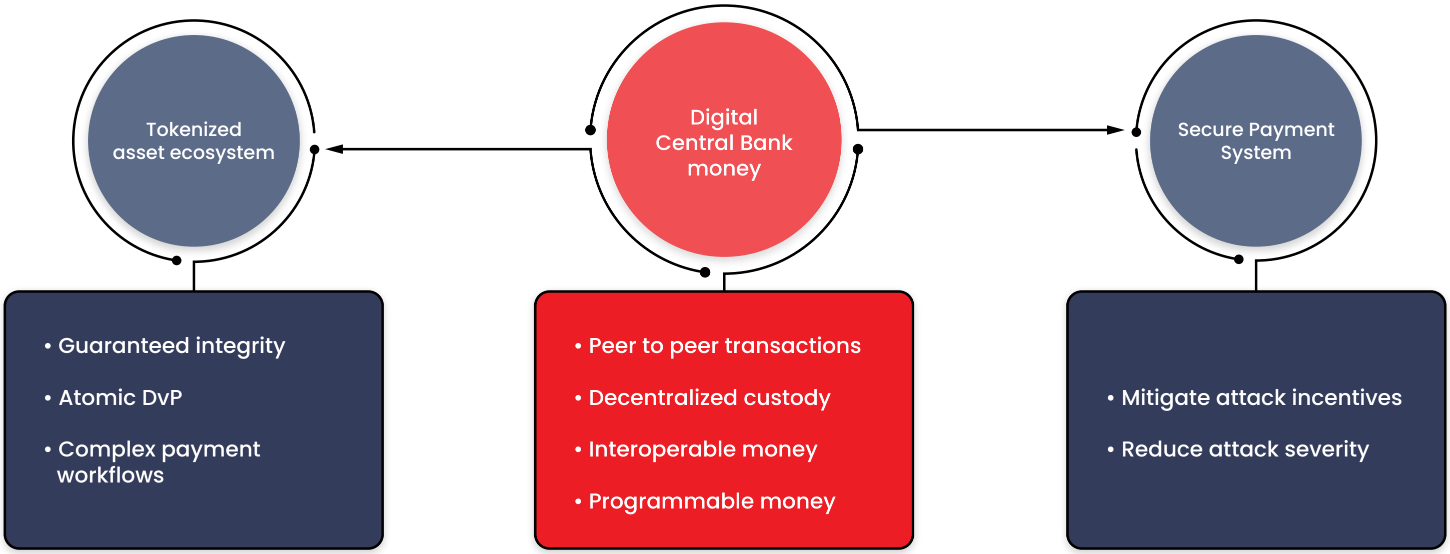
5 The case for CBDC on Corda

The merits of a blockchain-based CBDC solution

The previous sections focused on new capabilities unlocked by CBDC, while pointing towards potential paths forward. In almost every example, the tokenization of the currency as a bearer asset is necessary to the solution. This is a paradigm shift from the existing model of only account-based transfer of value.

There are three main components that demonstrate the value of a blockchain based CBDC implementation. First, distributed custody and peer to peer transfers are necessary for any CBDC solution. Second, a desirable attribute of CBDC is the integration with a larger tokenized ecosystem. Finally, improved security and resilience by removing honey pots of data and centralized weak points should be top of mind for any critical system. All of these are natural attributes of blockchain based systems.

Image 5: The benefits of a blockchain based CBDC



Blockchain enables the digital storage and transfer of value

The primary value blockchain enables is the digital storage and transfer of value. Transactions can be peer to peer, allowing for individual participants to custody their own money or assets.

Blockchain achieves this by solving the double spend problem through a decentralized consensus process. The double spend problem can be summarized as "how can a system prevent the double spend of an asset?" If this question cannot be answered, the scarcity of the asset cannot be guaranteed, and as a result, the asset would have no value.

Blockchain enables interoperability between different asset types through smart contracts (programable money)

Money recorded as tokens on blockchains can help to create efficient ecosystems when other assets are also recorded as tokens. With money and assets recorded as tokens, parties can create transactions that effect more than one change simultaneously.

In the purchase of an asset, this could mean the simultaneous delivery of an asset in exchange for its payment ("delivery versus payment"), or it could be the simultaneous payment of a dividend alongside marking the asset as ex-dividend - hugely reducing the uncertainties around dividend dates. With multiple currencies recorded as tokens, foreign exchange may take place without an escrow party or counterparty risk, in a single "payment vs payment" transaction.

A financial asset, whether it is money or a security, changes status throughout its lifetime. Perhaps it is transferred from one owner to another. Perhaps a quarterly dividend or coupon gets paid. Perhaps an external event happens, trigging a payout. We can think of these status changes as lifecycle events or the evolution of the asset. In a blockchain ecosystem, providing that the change is permitted by the asset's governing smart contract, any actor can evolve the asset. And can do so without paying a third party to do it on their behalf. This programmability enables a healthy ecosystem to emerge, where parties compete to provide the best service.[24]

Blockchain ensures global integrity of the system in which CBDC exists

The financial services ecosystem is complex, with multiple parties each keeping track of assets they own, assets they are owed, and assets they hold for other people. The global state of the ecosystem changes multiple times every second of the day, and its integrity is defined how accurately all participants record their business. If a single entity makes an accounting error, this can impact the entire system. Without blockchain, collective integrity has been hard and expensive, and sometimes simply impossible to validate.

For example, a company may issue 1,000 shares. Today, we have to trust that all parties who interact with the shares (custodians, transfer agents, traders, buyers, sellers, etc) record their transactions accurately and consistently. If the system has high integrity, an overall snapshot at any time will show exactly 1,000 shares. Yet, as we have seen in some cases,[25] parties may collectively record that there are more, or fewer, than the expected number of shares.

Recording assets, or indeed any agreement, as tokens guarantees the overall integrity of a system with multiple participants. This is because all parties must conform to a shared definition of what the asset is, and the business logic governing how it can evolve.

Using blockchain technology, we can record these assets on a definitive blockchain of record, and the smart contract code on the blockchain will guarantee that there is global integrity. We do not need to pin our reliance on specific third parties to behave as promised. Instead, overall integrity of the entire system can be guaranteed by the technology instead of being guaranteed by specific actors who may have motivation to deviate from the strict business agreements: stated more simply, there will always be 1,000 shares.

[24] Antony Lewis (Bits on Blocks)," Banking When the Bank is Shut – Token Maximalism", 2 October 2018.

[25] Matt Levine (Bloomberg), "Dole Foods Had Too Many Shares", 17 February 2017.

Blockchain reduces the overall system risk of a CBDC system

Finally, blockchain based CBDC provides a security improvement over centralized payments systems. This benefit is seen in two ways. There is no honey pot: since money exists as tokens held at by the participants, there is no centralized honey pot to be targeted, which reduces the incentive for an attack. There is no centralized point of failure: since the data is replicated across the participants of each transaction and each participant is running their own independent node, there is no single critical point of attack that can take down the network.

The drawbacks of some blockchains…

While blockchain is helpful tool for CBDC, modern payments systems have requirements that many blockchains fail to meet. Below are three attributes that are broadly applicable to any central bank sponsored payment regime.[26]

- **Data Privacy:** public blockchains globally broadcast sensitive information
- **Identity:** public blockchains enable the participation anonymous identities
- **Scalability:** blockchains tend to be slower than centralized systems
- **Probabilistic Settlement:** transactions on blockchains that use Proof of Work or Proof of Stake consensus models settle probabilistically and can ultimately be walked back

…and how Corda overcomes them

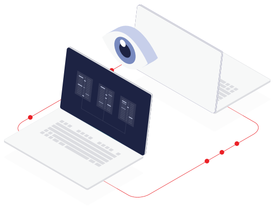
When considering the functional requirements of modern payment systems, the drawbacks inherent with other blockchains do not apply to Corda.

The Corda blockchain protocol is a product of rigorous requirement gathering from regulated enterprises. Corda creates a private permissioned environment where data is shared directly only between the counterparties of each transaction. This produces an environment that adheres to regulatory standards, promotes user identity, protects privacy, and enables appropriate firms to implement governance processes. Additionally, Corda's data distribution model along with its deterministic consensus protocol allow the network to scale to tens of thousands of transactions per second. As a result, the system looks and feels much like the production grade financial networks we use today.

Corda's point-to-point design is unique in that data is only shared with relevant parties.

What is a relevant party to a transaction? In Corda, relevant parties are defined in the contract code: the programmatic rules that define and govern a specific digital asset (what it is and how it can evolve). Relevant parties include the sender and recipient, but may also include a transfer agent, the issuer, an AML identity, a regulatory node, and so on.

[26] Depending on their goals, each central bank also has its own functional requirements, but it is outside of the scope of this paper to review technology distinctions across different features demanded by different organizations.

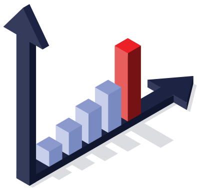


Data privacy

One set back of public blockchains is that in order to reach consensus, data relevant to every transaction needs to be distributed to everyone else on the ledger. With Corda this is not the case. Corda shares data only between the counterparties of transaction, therefore ensuring that any party's data does not reside with an entity that party has not transacted with. Additionally, even the communication protocol itself is entirely invisible to the other members of the blockchain. This protects not only the actual transaction details, but also prevents outsiders from knowing that the transaction is even happening in the first place.

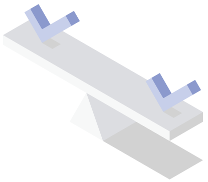
Identity

Corda is a private ledger. This means that in order to participate in a Corda based, solution each entity must be granted access to do so. One requirement to be granted access is the ability to attest to a legal identity. This creates a scenario when everyone can be certain that their counterparty is who they claim to be.



Scalability

There are a few factors that enable Corda to scale up to throughputs that can't be achieved in other protocols. Corda uses the unspent transaction output model (UTXO)–the consequence of this is that transactions that don't need to be sequential can very easily be paralyzed increasing the overall throughput of the system. Additionally, consensus bottlenecks are reduced due to Corda's peer-to-peer data distribution and the ability to add as many notaries as needed to each network.



Settlement finality

Blockchains that rely on proof of work or proof of stake consensus models are subject to a probabilistic settlement mechanism. What this implies is that when a transaction is submitted to be finalized, it is in the hands of something that may or may not happen. This also makes it hard to time bound each transaction. Additionally, this introduces issues around immutability since chains can be forked if a large enough group of the validating nodes are able to do so.

Corda's consensus model guarantees that assets have deterministic settlement finality. This is achieved with Corda because the mechanics of the consensus protocol are based on two things. **Validation** and **uniqueness.**

The process of the validation is handled by the counterparties of the transaction. In this process the counterparties all independently validate that the transaction adheres to the shared business rules within the governing contract code.

The second process, uniqueness is done by a notary or notary pool. The notary is in charge of attesting to the uniqueness of each transaction on the ledger. Together both these produce the final deterministic consensus which creates an immutable data point on the ledger.

Bank of Canada: Project Jasper Phase 1 and 2

Date: March 2016+
Use/Status: Project Jasper was a Canadian experiment with DLT for domestic interbank payments.
Technologies: Corda, Ethereum (private network)
Participants: R3, Bank of Canada, Payments Canada, Canadian banks
Findings:

- DLT platforms that employ a proof-of-work consensus protocol do not deliver the necessary settlement finality and low operational risk expected of core settlement systems.
- A distributed ledger system that employed an alternative consensus model on the basis of a notary node that could deliver improvements in regard to settlement finality, scalability and privacy.

6 Moving forward

We imagine a new architecture for money in the near future where central banks issue digital currency to wholesale or retail participants. This architecture is enabled by blockchain as a system of record and relies on central banks' diligence in providing robust governance frameworks for these new assets.

Wholesale participants can continue to have a direct relationship with the central bank and transact in central bank money with the additional benefits of atomic transactions, programmable money and improved complex payments scenarios. Non-wholesale will likely take advantage of CBDC through one of a few potential models. Some countries aim to provide full access wallets to the general population. Others envision end users interacting with central bank money through intermediary institutions. Proposals vary in their technical architecture, with interesting research around mixing the use of blockchain-enabled tokens and traditional account access.

The key to any viable CBDC will be in activating the comparative advantages of the diverse payments value chain, spanning liquidity providers, network operators, application providers, and end user wallet builders. Central banks will play a key role in orchestrating this ecosystem, and because of the infrastructure around them, have a tremendous opportunity to offer purchasing power.

As we think about expanding the scope of access to central bank money, it is hard to ignore parallel revolutions in the formation of a tokenized financial ecosystem. While the primary function of CBDC, at least as discussed in this paper, is to facilitate payment, its structure is often a tokenized asset. Blockchain systems have enabled a wide range of tokenized assets, and more recently on Corda we are seeing an emergence of tokens–such as a tokenized bond, equity or fractionalized piece of real estate–which could settle against CBDC.

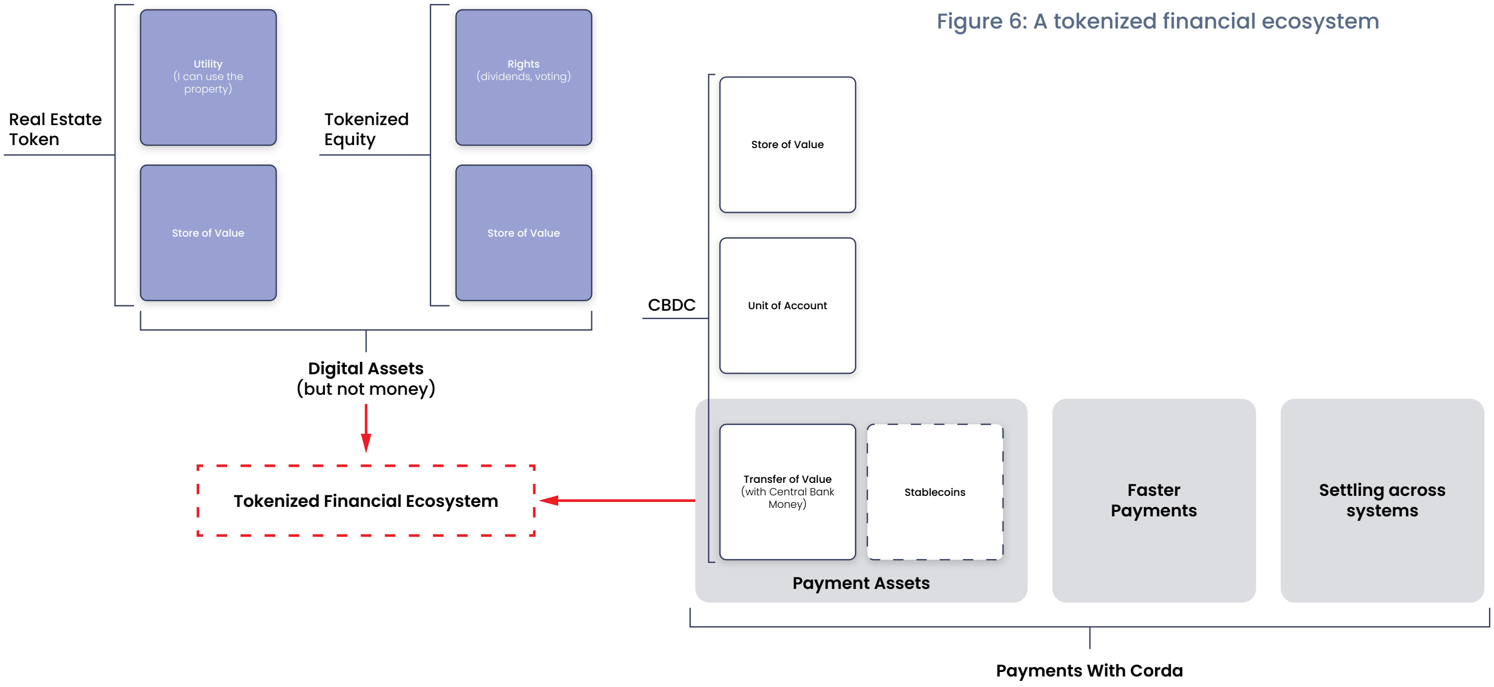


Figure 6: A tokenized financial ecosystem

Meanwhile, other areas of payments are undergoing significant innovations. Tokenized payment assets are certainly special because they enable easy access to tokenized financial market, enable peer to peer transactions and allow for decentralized custody. However, a sole focus on these neglects other opportunities to modernize systems, including other initiatives over which the public sector has control or influence. For example, right now there is significant momentum behind the build of faster payments systems. Additionally, there are opportunities to connect systems, using blockchain to jointly recognize obligations.

Widespread access to CBDC will be a key for central banks to fulfil their mandate of offering modern payments solutions. Additionally, it will catalyze connectivity between the general public, corporations and the financial industry with parallel innovations currently being built out by firms leveraging blockchain in non-payments related areas. Taken together, CBDC presents an opportunity for central banks to provide settlement solutions within a tokenized financial market infrastructure and meet general payment needs for a digital economy.

Sources

Papers

Morten Bech and Bart Hobijn, “Technology Diffusion within Central Banking: The Case of Real-Time-Gross Settlement”, Federal Reserve Bank of New York, September 2006.

Rodney Garratt, Antoine Martin, James McAndrews and Ed Nosal, “Segregated Balance Accounts”, Federal Reserve Bank of New York Staff Reports, August 2015.

Adam Furgal, Rodney Garratt, Zhiling Guo, Dave Hudson, "A Proposal for a Decentralized Liquidity Savings Mechanism with Side Payments", R3, 11 June 2018.

George Calle and Diana Barrero Zalles, “Will Businesses Ever Use Stablecoins?”, R3, 26 March 2019.

Tobias Adrian and Tommaso Griffoli, “The Rise of Digital Money”, International Monetary Fund, 15 July 2019.

"Exploring Anonymity in Central Bank Digital Currency", European Central Bank, December 2019.

“Flavors of Fast Report 2019”, FIS, 2019.

Raphael Auer and Rainer Boehme, “The Technology of Retail Central Bank Digital Currency”, Bank for International Settlements, 01 March 2020.

Morten Bech and Jenny Hancock, "Innovations in Payments", Bank for International Settlements, 01 March 2020.

“Central Bank Digital Currency: opportunities, challenges and design”, Bank of England, 12 March 2020.

Press releases

Press Release: "J.P. Morgan Creates Digital Coin for Payments", J.P. Morgan, 14 February 2019.

Project reports

“Inthanon-LionRock: leveraging distributed ledger technology to increase the efficiency of cross-border payments”, Bank of Thailand and Hong Kong Monetary Authority, January 2020.

"E-krona project, report 2”, Sveriges Riksbank.

Articles

Matt Levine (Bloomberg), "Dole Foods Had Too Many Shares", 17 February 2017.

Antony Lewis (Bits on Blocks),” Banking When the Bank is Shut – Token Maximalism”, 2 October 2018.

Yogita Khatri (CoinDesk), "Tether Says Its USDT Stablecoin May Not Be Backed By Fiat Alone", 12 May 2019.

Etienne Jinze (Binance Research), “”First Look: China’s Central Bank Digital Currency”, 28 August 2019.

Ian Allison (CoinDesk), "Wells Fargo to Pilot Dollar-Linked Stablecoin for Internal Settlement", 17 September 2019.

Continue the conversation

r3.com | corda.net

@inside_r3 | @cordablockchain

r3.com/blog | corda.net/blog

linkedin.com/company/r3cev-llc/

R3 Contributors

George Calle, Market Intelligence Lead
george.calle@r3.com

Daniel Eidan, Solution Architect
daniel.eidan@r3.com

About R3

R3 is an enterprise blockchain software firm working with a broad ecosystem of more than 350 participants across multiple industries from both the private and public sectors to develop on Corda, its open-source blockchain platform, and Corda Enterprise, a commercial version of Corda for enterprise usage.

The Corda platform is already being used in industries from financial services to healthcare, shipping, insurance and more. It records, manages and executes institutions' financial agreements in perfect synchrony with their peers, creating a world of frictionless commerce. Learn more at **r3.com** and **corda.net**.

New York
11 West 42nd Street,
8th Floor New York,
NY 10036

London
2 London Wall
Place, London
EC2Y 5AU

Singapore
18 Robinson Road,
Level 14-02,
Singapore 048547

São Paulo
Av. Angélica, 2529 -
Bela Vista, 6th Floor
São Paulo - SP,
01227-200, Brazil

Hong Kong
40-44 Bonham Strand,
7F Sheung Wan,
Hong Kong

Dublin
50 Richmond St. South,
Saint Kevin's, Dublin,
D02 FK02