CONSENSYS

CONSENSYS WHITE PAPER

Central banks and the future of digital money

An overview and proposal for central bank digital currency on the Ethereum blockchain

Prepared by ConsenSys AG
January, 2020

Authors: Matthieu Bouchaud, Tom Lyons, Matthieu Saint Olive, Ken Timsit
Contributors: Shailee Adinolfi, Benjamin Calmejane, Guillaume Dechaux, Faustine Fleuret, Vanessa Grellet, Joyce Lai, Monica Singer

WHITE PAPER

Foreword

Davos, 20 January, 2020

As the World Economic Forum meets in Davos for the 50th time, it does so against the backdrop of a sea change in the mechanics of money.

The rise of cryptocurrencies and blockchain technology over the last decade has brought about new possibilities in the issuance and use of money as well as exciting new forms of digital assets and markets. At the same time a rapidly evolving geopolitical, economic and social environment has created new expectations and new requirements for secure, reliable, easy-to-use, globally available digital payments and means of exchange.

Among the most significant innovations we are witnessing today are stablecoins, or privately issued cryptocurrencies pegged to a stable asset, which today have a market cap over $5B USD, as well as the parallel phenomenon of central bank-issued digital currencies, commonly referred to as CBDC, that are the subject of this paper.

According to the Bank of International Settlements, over 70% of central banks are looking at issuing a digital currency on a blockchain. We think this is a development to be applauded.

CBDCs can offer a range of advantages. They can play a central role in advancing the digital assets revolution in a regulated, lower-risk and – crucially – accessible way, helping make financial markets more efficient and available to all global citizens. CBDC can give the central banks more effective, future-oriented tools to allow them to implement monetary policy in

more direct and innovative ways and keep pace with technological change. CBDCs could also simplify and reduce the cost of cross-border remittances, while forming the basis for more efficient, more secure interbank payments networks. The list goes on.

Below we provide both an overview of CBDC and a concrete example of how a CBDC might be implemented on the Ethereum blockchain. We believe that Ethereum is the best-suited blockchain network for the kind of maximally secure, global-scale, interoperable settlement platforms that CBDCs require. But we are well aware that there are many other possibilities.

What is important is that central banks have come to realise the extent of the transformations that are already happening in digital currencies, and that they see the importance of embracing a significant role in bringing about this change. We hope this paper provides a useful and thought-provoking example of one promising approach.

Joseph Lubin, Founder and CEO of ConsenSys, Co-Founder of Ethereum

WHITE PAPER

Table of Contents

WHITE PAPER

Executive summary

Over the past year we have seen a number of groundbreaking announcements from central banks around the world exploring the issuance of central bank digital currencies (CBDC). In this paper we provide an overview of the potential and risks of CBDC, as well as an example of how a CBDC could be designed and built on the Ethereum blockchain. The intention is to give the reader not just a good background to this important topic, but also – by means of a concrete proposal – a practical look at what the implementation of a CBDC might entail.

Blockchain-based CBDC, which represents a new technology for the issuance of central bank money at the wholesale and retail level, offers a number of potential advantages for central banks. It could be a strong catalyst for financial services innovation by providing a viable, large-scale payments system for tokenised assets markets – offering a risk-free, widely accessible alternative to privately-issued stablecoins, like Facebook's Libra, which serve a similar purpose but could expose users to credit and/or liquidity risk.

Widespread use of CBDC instead of private payment tokens could also help central banks retain sovereignty over monetary policy in tokenised assets markets, an important consideration should such markets come to represent significant portions of the economy. Other benefits include potentially new regulatory monitoring and enforcement tools, cheaper cross-border remittances, improvements to the interbank payments infrastructure and innovation in retail markets. CBDC could also be a superior replacement to physical cash, helping alleviate some of the risks and costs associated with banknotes. Depending on how it is designed, a CBDC could support financial inclusion by providing wide-scale access to risk-free reserves.

There are risks as well – particularly in retail CBDC (that is, tokenised central bank money accessible to the general public). For this reason, we propose that central banks issue CBDC on a large-scale, private, permissioned, Ethereum-based network in which central-bank appointed intermediaries act as nodes and service providers. In the proposed setup, the central bank would issue the currency as well as authorise and onboard intermediaries, but only intermediaries would distribute CBDC directly to the public. Because the integrity of the system is embedded in the technology, the number and type of intermediary service providers on this platform would however be much larger and broader than is the case with the distribution of central bank money today.

Such a setup recommends itself on many grounds. As the issuer of the digital currency, central banks would have direct control of the money supply, while users of the currency would not be exposed to the risks of private currencies. It would provide the basis for a large-scale, evolving and easily adaptable infrastructure offering a continuously expanding number of shared services to various stakeholders. End users would benefit from a much more open, vibrant, competitive and above all innovative environment than today, with secure and user-friendly access to the benefits of tokenised assets markets.

For reasons we lay out in the paper, we believe that Ethereum is one of the best technologies available today to meet the technical requirements for such a CBDC. But there are other possible solutions as well. What is important is that central banks have come to realise the importance of CBDC as an innovative tool, and that they continue to learn about and experiment with it.

WHITE PAPER

1. Introduction

From China to Sweden, Singapore to South Africa, over the past year we have seen a number of groundbreaking announcements from central banks around the world exploring the issuance of central bank digital currencies (CBDC).

The idea of digital money issued directly by a central bank is not new. The 1990s and 2000s saw a period of interest as well, particularly for retail uses among the general public, though for various reasons central banks ultimately decided not to pursue the projects.

Much has changed since then, both in the global economy and in the world of technology. The main catalyst for today's renewed interest in CBDC has been the advent of blockchain technology. And while explorations to date have been more ad hoc than holistic, with proofs of concept here and there to investigate specific aspects of the problem, the trend is clear.

In this paper we provide an overview of the history and current state of CBDC as well as an example of how a CBDC could be designed and built on the Ethereum blockchain. Our intention is to give the reader an overview of the potential advantages and the challenges in a CBDC as well as, through a concrete proposal for a specific approach, to move the debate beyond the theoretical.[1]

CRYPTOCURRENCIES, STABLECOINS AND THE EVOLUTION OF DIGITAL MONEY

A blockchain-based CBDC is a type of crypto asset. To understand the resurgence of CBDC today it is necessary to take a short look at the history of crypto assets in general.

The first crypto asset was Bitcoin. A "decentralised electronic cash system," Bitcoin billed itself as a new form of money whose main characteristics were that it

1 Note: While blockchain is not necessary to issue a CBDC, it offers many advantages, and the majority of CBDC projects under contemplation today are based on blockchain. For the purposes of this paper, therefore, we will use the term CBDC to refer solely to blockchain-based CBDC.

was fully digital, lived on a blockchain, and was independent of any government or private institution. Quickly dubbed a cryptocurrency[2], it was followed by an explosion in similar blockchain-based cryptocurrencies known as altcoins. In 2014 the Ethereum blockchain launched adding new capabilities, in particular full programmability on a blockchain allowing the creation of "smart contracts." With this it became possible to represent almost any asset, not just money, on a blockchain by means of a unique digital token (hence the term "tokenisation").

What makes crypto assets interesting is not the fact that they are digital representations of assets. Most assets today already exist in digital form as entries in computer databases. Rather it is the fact that they are digital assets represented on a distributed ledger that is a) shared in a network and b) that acts as a single source of truth about the assets and their ownership independent of any organisation or third-party authority.

Such decentralised, communally maintained ledgers have a number of advantages over the centralised ledgers that are used in the financial system today. Chief among these is that asset transfers on distributed ledgers do not require reconciliation between different databases – an extremely complex and costly process. Markets based on tokenised assets have a lot of promise, including – depending on the asset and use case – faster, cheaper and more secure infrastructure than in traditional markets, higher levels of automation, lower levels of risk and lower barriers to entry.

Despite this great promise, almost all crypto asset projects to date have run into a similar problem: the ability to execute payments in the real world of fiat currencies. Originally it was thought that cryptocurrencies like bitcoin or ether would be able to provide the means of payment in crypto asset markets and act as a bridge to the fiat world. But cryptocurrencies have proven to be extremely volatile, and cryptocurrency networks slow, cumbersome and complex

2 Cryptocurrencies are a subset of crypto assets.

for users. Today they are generally considered unsuitable as a means of payment.

The initial response to this problem in the blockchain community was stablecoins – cryptocurrencies that are either pegged to fiat currencies or that maintain a stable value by some other means.[3]

The first stablecoins began appearing in 2017, with one of the most well-known early projects being Tether. These were generally focused on solving the payment problem for blockchain-based platforms specifically. As people began to understand the value of stablecoins for tokenised asset markets, we have seen a second generation of stablecoin projects by private and public entities, often as part of consortia and with the participation of technology providers. These include Facebook's Libra, Fnality (formerly USC), Binance coin, JP Morgan's JPM Coin, Terra, USD Coin, the Gemini dollar and China's DC/EP project.

Of these, perhaps the most widely publicised has been Libra, and it serves as a good example of the promise but also the issues surrounding such projects. The Libra cryptocurrency will be stabilised by a basket of currencies and other assets[4], and potentially other means. While hailed as a way to help the billions of unbanked in the world, Libra has also raised concerns among central bankers, regulators and governments about infringements on monetary policy and risks to financial stability.[5]

While we see many benefits to stablecoins issued by private companies, the discussion around Libra highlights their limits as well. By leveraging blockchain technology for CBDC, central banks may be able to address some of these issues and so help realise some of the key benefits stablecoins can offer. In the rest of this paper, we look specifically at CBDC.

INTRODUCING CENTRAL BANK DIGITAL CURRENCIES

In modern societies there are two main types of fiat money. Central bank money is legal tender created and backed by a central bank. It represents a claim against the central bank and – with the crucial exception of cash in the form of banknotes and coins – is mainly used for wholesale payments. Commercial bank money is created by commercial banks when they issue credit, either through loans or credit lines. Most of the fiat money in the world is commercial bank money, and it is widely used as a retail means of payment,(with retail here meaning paymnt between non-financial institutions, corporates or individuals).

CBDC represents a new technology and approach for the issuance of central bank money, and can be characterised by the following:

- **Digital assets.** CBDC is a digital asset, meaning that it is accounted for in a single ledger (distributed or not) that acts as the single source of truth.

3 There are many different stablecoins in circulation today, using many different methodologies. A discussion of the types of stablecoins is beyond the scope of this paper however. We direct the reader to Stablecoins: The Complete Guide.

4 Libra "will be backed by a collection of low-volatility assets, such as bank deposits and short-term government securities in currencies from stable and reputable central banks." Libra White Paper, Section 04: The Libra Currency and Reserve.

5 Libra Crypto Is 'Undoubtedly' a Wakeup Call for Central Banks, Says ECB Exec, CoinDesk, 26 September, 2019.

- **Central bank-backed.** CBDC represents a claim against the central bank, just as banknotes do.
- **Central bank controlled.** The supply of CBDC is fully controlled and determined by the central bank.

We distinguish between two types of CBDC:

- **Wholesale CBDC.** CBDC that would be used to facilitate payments between banks and other entities that have accounts at the central bank itself.
- **Retail CBDC.** CBDC used for retail payments, for example between individuals and businesses, and akin to digital bank notes.

Blockchain technology could be used to support both types of CBDC. For example, it could be used as an alternative approach to existing wholesale central bank systems, either real-time gross settlement systems such as CHAPS, Target 2, Fedwire, or deferred net settlement systems like BACS, EURO1, TIPS, ACH. It could also be used to create platforms for the distribution of retail CBDC on a broad scale, and with it true, government-backed electronic cash.

According to the BIS, today some 70% of central banks are looking at CBDC, with the majority of them considering blockchain as the underlying technology.[6] While many of these banks have expressed interest in both wholesale and retail use cases, most of the admittedly few actual experiments or pilots carried out to date have focused on wholesale. These include Project Ubin[7] by the Monetary Authority of Singapore, Project Khokha by the South African Reserve Bank[8], China's DC/EB[9], and Project Stella[10], a joint research project by the ECB and the Bank of Japan.

Despite the current focus on wholesale, many industry observers think there is high potential for both wholesale and retail CBDC, and that central banks will consider both.

6 Proceeding with caution – a survey on central bank digital currency, BIS Papers 101, January 2019.
7 Project Ubin Phase 2, Accenture, November 2017.
8 Project Khokha: Blockchain Case Study for Central Banking in South Africa, ConsenSys Case Study.
9 China's digital renminbi could increase commercial bank competition, Ledger Insights, January 2020.
10 Project Stella: the ECB and the Bank of Japan release joint report on distributed ledger technology (Phase 3), Bank of Japan, 4 June 2019.

WHITE PAPER

2. Benefits of digital currencies for central banks and the economy

While we have yet to see CBDC projects in production and so have no empirical evidence of their impact, many believe CBDC can offer a number of significant benefits for central banks and the wider financial system. These include the following.

FOSTERING THE DIGITAL ASSETS REVOLUTION

Digital assets in general are set to disrupt today's capital markets, offering among other things cheap issuance and distribution, massively increased efficiency and flexibility due to programmability, instant delivery versus payment, and automated lifecycle management.

As tokenised asset markets are created there will be a need for tokenised payments for the immediate settlement of transactions. CBDC could be the key ingredient in introducing a viable, broad-based blockchain-based payments system that could enable a large-scale, decentralised clearing house and asset register and in turn allow digital assets to reach their potential.

If central banks do not issue their own digital currency, the markets will move to private payment tokens. This would expose users to various risks. There is credit risk: if private issuers fail, holders of the currency would lose all their money. Privately issued tokens may also not be accessible to all, leading to financial exclusion. A CBDC would represent a risk-free, widely accessible alternative.

It could have other benefits too. It could help bring massive efficiencies and cost savings to the financial system. Studies have placed the cost of clearing and settling securities in G7 countries at over USD 50 billion per year, mostly due to the resources needed to transfer the assets and reconcile accounts.[1] By replacing various middlemen and providing for increased automation, a decentralised clearinghouse based on a distributed ledger could be a far cheaper and, through reduced complexity, a likely more secure system.

1 Speech by Mr Ben Broadbent, Deputy Governor for Monetary Policy of the Bank of England, at the London School of Economics, London, 2 March 2016.

An international equivalent for tokenised national currencies could also reduce risk in foreign exchange transactions by allowing for payment-versus-payment settlement approaches. That could have benefits for governments, but also for millions upon millions of businesses and individuals.

Central banks might also find CBDC to be superior to physical cash. In some countries the creation and distribution of banknotes is expensive and can be a major catalyst for unlawful activity. In many parts of the world it is also difficult for citizens to access physical cash because they live far from bank branches and ATMs. CBDC could be distributed easily on mobile phones, which would help address these problems.[2]

Retail CBDC could also be a way to offer individuals access to digital and risk-free reserves, something that is only available to major financial institutions at the moment. This could be a major advantage in the many parts of the world bank where deposits are not insured and where depositors risk losing all if a bank becomes insolvent. As this is generally not an issue with a central bank, CBDC does not carry this risk.

FUTURE-ORIENTED MONETARY POLICY AND REGULATORY TOOLS

As noted, if central banks do not issue their own digital currency, then privately issued payment tokens – which for all intents and purposes are akin to digital cash – will be the only choice for payments. In some developing countries we are already seeing a significant decrease in the use and acceptance of banknotes in favor of digital solutions. If, as many believe, such solutions become very large and broad-based, they can potentially represent significant, systemically relevant portions of the economy.

If central banks do not have their own digital currency as a basis for payments in these markets, then they risk losing some of their ability to carry out their monetary policy and

2 Projects such as mPesa have shown that the mobile phone is an excellent distribution mechanism for digital forms of money in developing countries.

regulatory mandates. CBDC would mitigate this risk by giving central banks direct influence over all or a portion of the money supply in digital markets.

CBDC could also give central banks new tools for expanding and reducing the supply of money. It could make it easier to employ innovative retail-oriented interventions, for example, direct distribution of money to individuals (as opposed to the indirect methods typically used by governments today, like tax breaks). It could help central banks fight against financial and social exclusion for individuals and enterprises that do not have access to commercial bank created money, for instance due to reasons of cost or availability. If the retail CBDC bears interest, either positive or negative, it could strengthen their ability to pass through policy interest rates to money and lending markets as well as directly to individuals. Finally, if structured in a way that allows the CBDC to be traced, it could be useful in more efficient sanctions and AML enforcement contexts.

CHEAPER CROSS-BORDER REMITTANCES

Today, cross-border payment transactions, whether for businesses or individuals, are very expensive. This is generally a function of the state of the technology when the infrastructures for cross-border payments were developed, which at the time did not allow for direct transfer without intermediaries. In the current financial system, a typical cross-border payment involves transfers through several different correspondent banks, with the attendant cost of transacting and reconciliation as well as significant wait times. For individuals – in particular migrant workers sending remittances back home, one of the largest sources of financial inflows to developing countries – there is the added cost of the dense network of physical outlets at both the sending and receiving end.

If we imagine a world where both the origin currency and the destination currency are based on CBDCs, it is quite easy to imagine money transfer systems that are almost entirely automated and use cryptographic techniques to permit interoperability between different systems and distributed ledgers. Many financial actors can then connect to these ledgers and compete to offer the best price and service to customers, driving costs down and reducing delays. With the prevalence of mobile phones among all sections of the population, including in developing countries, such a system would also obviate the need for physical distribution outlets, further driving down costs.

IMPROVING THE SETTLEMENT OF INTERBANK PAYMENTS

Today the settlement of interbank transactions using central bank money is increasingly carried out on Real-Time Gross Settlement (RTGS) systems. These have the advantage of settling payments on an individual order basis between counterparties, instead of netting payments

at the end of the day.[3] The downside to these systems is that they rely on batch processing overnight and require collateral to cover the outstanding positions. These systems therefore do not completely eliminate settlement risk. Many RTGS systems today also rely on antiquated technology, including mainframes, older programming languages like Cobol, or messaging platforms like SWIFT, and as a result, have a certain amount of operational risk.

With CBDC, interbank payments would be much more akin to the transfer of digital cash (albeit in very large amounts), and would be true real-time payments between counterparties with no settlement risk and greatly reduced operational risk. We can also expect CBDC-based systems to be more secure and performant than current approaches.

ACCELERATING INNOVATION IN RETAIL MARKETS

Even though real-time money transfers can be made quite cheaply and in quasi real-time by centralised settlement platforms like SEPA, it does not mean that all consumers and businesses have access to real-time and low cost remittances.

In fact, many financial institutions charge their customers for real-time money transfers at rates well above the cost that they incur. While some of this revenue is necessary to fund their operations, it could be considered unfair that end users are not able to take advantage of the technological improvements driven by central banks. Additionally, in some developing countries, particularly in South East Asia, the fact that intra bank payments are free and inter bank money transfers are not free or not real-time, has resulted in massive competitive advantage for the largest bank networks, which have disproportionate access to consumer deposits, which diminishes competition in the retail and SME banking sectors.

In this context, the creation of central bank-sponsored digital currency, freely and quickly transferable between users, can be a way for regulators to set new market standards, encouraging retail financial institutions to improve their value proposition to consumers and SMEs. This could include extended operating hours, potentially 24/7, richer data in payment messages and transparency on processing status, higher interoperability between platforms and further supporting the development of programmable money, one of the great promises of blockchain.

3 Real-Time Gross Settlement (RTGS), Investopedia.

WHITE PAPER

3. Requirements for successful implementation of CBDC

While there are many benefits to CBDCs, before they can be introduced many challenges will need to be tackled and risks will need to be addressed. There are also a number of key design decisions that will need to be taken, some of which will have far-reaching consequences in terms of how the CBDC is used and its potential impact. In this section we outline some of the requirements and issues that central banks will want to keep in mind.

WHAT KIND OF CBDC

First and foremost, central banks will need to make a fundamental decision about who will have access to the CBDC. The basic choice will be between a retail or wholesale CBDC, or both. The answer will depend on the central bank's goals for the CBDC. For instance, wholesale CBDC can support financial innovation and add efficiencies and lower cost to interbank payments. Retail CBDC can be a way for central banks to provide risk-free, easy to use digital cash to the general public.[1] The central bank will also want to decide to what extent it sees the CBDC as a tool for monetary policy, and in particular whether the CBDC should be interest-bearing.

DISTRIBUTION

While central banks will be the issuers of CBDCs, they will have to decide on how they will be circulated. Here there are a wide variety of choices, running from reliance on banks and select institutions to distribute CBDC, as is done today with central bank money, to using CBDC as an opportunity to increase the number of intermediaries with access to central bank money (which is what we propose below), to distributing CBDC directly to the public, something which could easily be done with a blockchain-based CBDC platform.

SOUND GOVERNANCE

Another crucial issue is governance. While decentralised systems offer many advantages, a broad-based decentralised platform with no responsible entity can be

1 For more see Central Bank Digital Currency: One, Two or None?, Christian Pfister, Banque de France Working Paper, October 2019.

problematic. Lack of structured governance could hamper decision making both on the technical and design level, making it hard for the platform to evolve. Lack of clear ownership would raise many difficult legal and regulatory questions, for example around liability if things go wrong.[2] There would therefore be a need for a controlled and regulated infrastructure with clear governance structures in terms of design, development, maintenance, funding, upgrades and the like.

PRIVACY VERSUS TRANSPARENCY

It will technically be possible to design CBDCs with various mixes of anonymity versus traceability of transactions. Central banks will have to decide on the appropriate balance between privacy and transparency. While each bank will draw its own conclusions, one promising option is to provide high privacy for small transactions by retail users, similar to cash today, while programming in high traceability for larger transactions, whether by individuals or corporations. This would allow for the implementation of KYC/AML procedures on those transactions.

TOKEN-BASED OR ACCOUNT-BASED

Another important design decision is whether the system should be token-based or account-based. In a token-based system, the CBDC is created as a token with a specific denomination. The transfer of a token from one party to another does not require reconciling two databases, but is rather the near-immediate transfer of ownership, very much like handing over banknotes from one person to another.

In an account-based system, the central bank would hold accounts for users of the CBDC, and would handle the debit and credits between users itself. Currently central banks offer accounts for financial institutions, some non-bank financial intermediaries, and in certain cases, retail customers. In this approach, central banks would have to hold accounts for all users of

2 Legal and regulatory framework of blockchains and smart contracts, EU Blockchain Observatory and Forum, September 2019.

the currency, meaning exponentially more accounts to manage.

We recommend a tokenised model on several grounds. It would for instance enable business models based on asset tokenisation, and so be the basis for significant innovation. Second, it would free the central banks from the duties of large-scale account keeping and reconciliation, as well as the attendant reputational risks should things go wrong or service quality be poor.

PERFORMANT AND OPERATIONALLY ROBUST

To achieve significant adoption, the service will need to be performant and provide a good user experience. That means it needs to be operational 24/7, be highly reliable (with no or very few failed transactions), and be fast, with near-immediate transaction speeds.

Assuming 100 million citizens carrying out one transaction per day, that implies an infrastructure with throughput rates in the thousands of transactions per second. No blockchain technology at the moment can deliver such rates at the base protocol layer, but with a mix of protocol additions as well as ongoing improvements to the base technology, we expect that this will be possible in the future. To meet user needs, the platform should also allow offline transactions.

The system should also be robust, with the capacity to continue operations even if a certain percentage of nodes are down. It should also be easy for new or disconnected nodes to come online and quickly sync with the network. It will also need a highly available and reliable backup capacity. The system will need to be safe and efficient, maintaining the integrity of its payment, clearing and settlement arrangements under all conditions, and offering both expeditious transaction finality as well as controlled reversibility of transactions when necessary.

Finally, the system will have to be well protected against cyber and other operational risks through a mix of appropriate systems, policies, procedures and controls. It should also be highly interoperable with existing and future systems, able to integrate easily into new contexts and adapt to new needs as they arise.

LEGALLY SOUND

A broad-based CBDC platform will need to be legally sound as well. That means ensuring that the CBDC enjoys protections under existing legislation including payment law, contract law, settlement finality provisions, insolvency law and conflicts of law regimes in their local jurisdictions.

As a new approach to money, CBDC may well require adjustments to regulations to take into account its new properties. There are other new legal questions as well. For example, as opposed to physical cash, it would be possible to restrict the usage of CBDC to only allow its use by citizens or residents of a certain country. Central banks, policy makers and the courts will be tasked with finding appropriate use for such capabilities and responses to such issues.

UNDERSTAND THE RISKS

While we have outlined many potential benefits of CBDC above, we are fully aware that there are risks as well. Considering the far-reaching innovation potential of CBDC, and in particular retail CBDC, before implementing them, central banks will want to conduct comprehensive analyses of their potential impact.

For example, one issue raised by retail CBDC is the potential negative impact on commercial bank deposits as people withdraw funds from commercial banks in favor of central bank money. This could weaken banks, forcing them to either increase the interest they pay on deposits to attract customers, or raise interest rates on loans to maintain adequate funding. In times of crisis, outflows could increase dramatically, leading to large-scale bank runs. This would cause the central bank balance sheet to balloon, and would oblige it to support the commercial banks, which in turn would mean expanding the balance sheet and exposing them to credit risk of the financial institutions they are supporting.

There are other risks as well, and central banks will want to understand the opportunities and risks of their approach ahead of time.[3]

3 For an overview see Central Bank Digital Currencies: 4 Questions and Answers, IMF Blog, 12 December, 2019.

WHITE PAPER

4. Proposed architecture for Ethereum-based central bank money

In this section we propose an architecture for a CBDC implementation on the Ethereum blockchain.

AN OPEN, INTEROPERABLE, PROVIDER-BASED SYSTEM

We propose that central banks issue CBDC on a large-scale, private, permissioned, Ethereum-based network in which central-bank appointed intermediaries act as nodes.

These intermediaries would work together on a single platform as providers of the currency, as well as compete to offer innovative services to citizens and businesses. The number and type of intermediary service providers would be much larger and broader than is the case with central bank money today, incorporating financial and non-financial institutions, but the system would not entail direct distribution of CBDC to the public.

Such a setup has many advantages.

First, using a permissioned blockchain, central banks would retain control over the onboarding and distribution of the CBDC to the intermediaries they choose, and would therefore maintain oversight and control, allowing them to act as wardens of the ecosystem without having to provide or manage the services themselves.

Second, since the tokenised CBDC that underlies the system is issued by the central bank and not the intermediaries, it is the CBDC and not the intermediary's balance sheet that is on the line. In the event that an intermediary goes into liquidation, it will not put the record of ownership of the digital currency at risk as the digital currency is in the e-wallet of the customer and in the blockchain ledger of the central bank.

Third, it would provide the basis for a large-scale, evolving and easily adaptable infrastructure offering a continuously expanding number of shared services to various stakeholders. Because the stability and integrity of the system is embedded in the technology, the technical and prudential requirements to be an intermediary would be much lower than those required to be a

bank or e-money provider. End users would benefit from a much more open, vibrant and competitive environment than today, while intermediaries will become more and more like utilities.

Fourth, it would allow for standardised identifiers and identity mechanisms as well as mutualised control mechanisms, for example for KYC/AML, which could simplify and reduce the cost of compliance for all stakeholders, while likely improving their effectiveness.

Fifth, the system would be easy and secure for end users, as it would allow for service providers to offer key management and custodial services, as well as compete to develop user friendly wallets and related services.

Finally, as an Ethereum-based platform, it would be easily interoperable with the public Ethereum network as well as other blockchain networks, allowing for broad, far-reaching use cases in many different contexts, including in settlement networks in other jurisdictions.

TECHNICAL REQUIREMENTS FOR OUR PROPOSED ARCHITECTURE

The system described above implies the following list of requirements:

- **Full control of the money supply by central banks.** The central bank is the only entity allowed to issue CBDC units and remove them from circulation.
- **Quasi-real-time asset transfer at negligible cost.** Transaction times should be fast, with transfers occurring at or near real-time, and at a sub-one tenth of a cent (<0.1 EUR) cost.
- **High transaction throughput.** The system should offer several thousands to several tens of thousands of transactions per second on the network.
- **Large number of network participants.** The system should support several hundred to several tens of thousands of approved intermediaries as network participants, which is the likely number

of financial and non-financial institutions and intermediaries that we can expect for a large-scale CBDC in an area like the eurozone.

- **Privacy of consumer data and transactions.** In our view, central banks should not have a comprehensive view on individual wallets and associated IDs below a certain transaction value threshold when KYC/AML requirements would kick in (see below).
- **Confidentiality of business data.** The system should also support confidentiality of critical business data of the intermediaries on the network. While the central bank would maintain a view of all large transactions, individual network participants would not be able to see the volumes or individual transactions of their competitors.
- **Compliance with KYC/AML and related regulations.** The system supports the implementation of KYC/AML and related regulations by providing traceability and monitoring capabilities to the relevant authorities. As mentioned above, we believe this should only be possible above a certain threshold.
- **Asset recovery.** The system should allow for the reversing of transactions under legally acceptable conditions, as well as the ability for end users to recover lost or misplaced funds.
- **Acceptable environmental impact.** The system should be able to run at acceptable energy usage levels so as not to have a negative environmental impact.

WHY ETHEREUM FOR CBDC

Ethereum is a decentralised, open source and distributed computing platform that was launched in 2015 as a more versatile version of the Bitcoin blockchain.

Today public Ethereum is the second-largest blockchain platform by market capitalisation, behind Bitcoin, and Ethereum has by far the largest developer community of any blockchain protocol. While public Ethereum is permissionless, meaning open to all, Ethereum has permissioned variants capable of offering enterprise grade security and performance. We believe that private, permissioned Ethereum would offer the best possible platform for the CBDC requirements specified above.

Ethereum is by nature well suited to the creation of tokens. Central banks could easily design and implement tokens that can be widely circulated yet whose issuance and destruction remain firmly under their control. As these tokens live natively on the network, they do not depend on a single issuer who establishes point-to-point private communication channels with each participant.

Ethereum offers robust permissioning capabilities that would allow central banks to easily authorise and deauthorise network participants, allowing them to maintain control over who is on the network and what activities they are authorised to carry out. Private Ethereum networks using proof-of-

authority (PoA) consensus can offer quasi-real-time asset transfers at negligible cost.

While no blockchain has the technology to support the required transaction throughput levels today, Ethereum is well placed to be able to do so in the near future. The switch to proof-of-authority at the protocol level (Level 1) and the introduction of a number of Level 2 solutions, like state channels, plus ongoing R&D efforts in the Ethereum community, will make these performance levels possible. The large number of developers on Ethereum means these R&D efforts are not only robust, but also multifaceted.

As the global user base of public Ethereum shows, the protocol is well suited for large-scale platforms. Ethereum can also easily handle the privacy and confidentiality requirements of a CBDC, through a mix of public and private smart contracts complemented by cryptographic techniques such as zero-knowledge proofs, homormorphic encryption and secure multi-party computation or newer technologies like rollups.

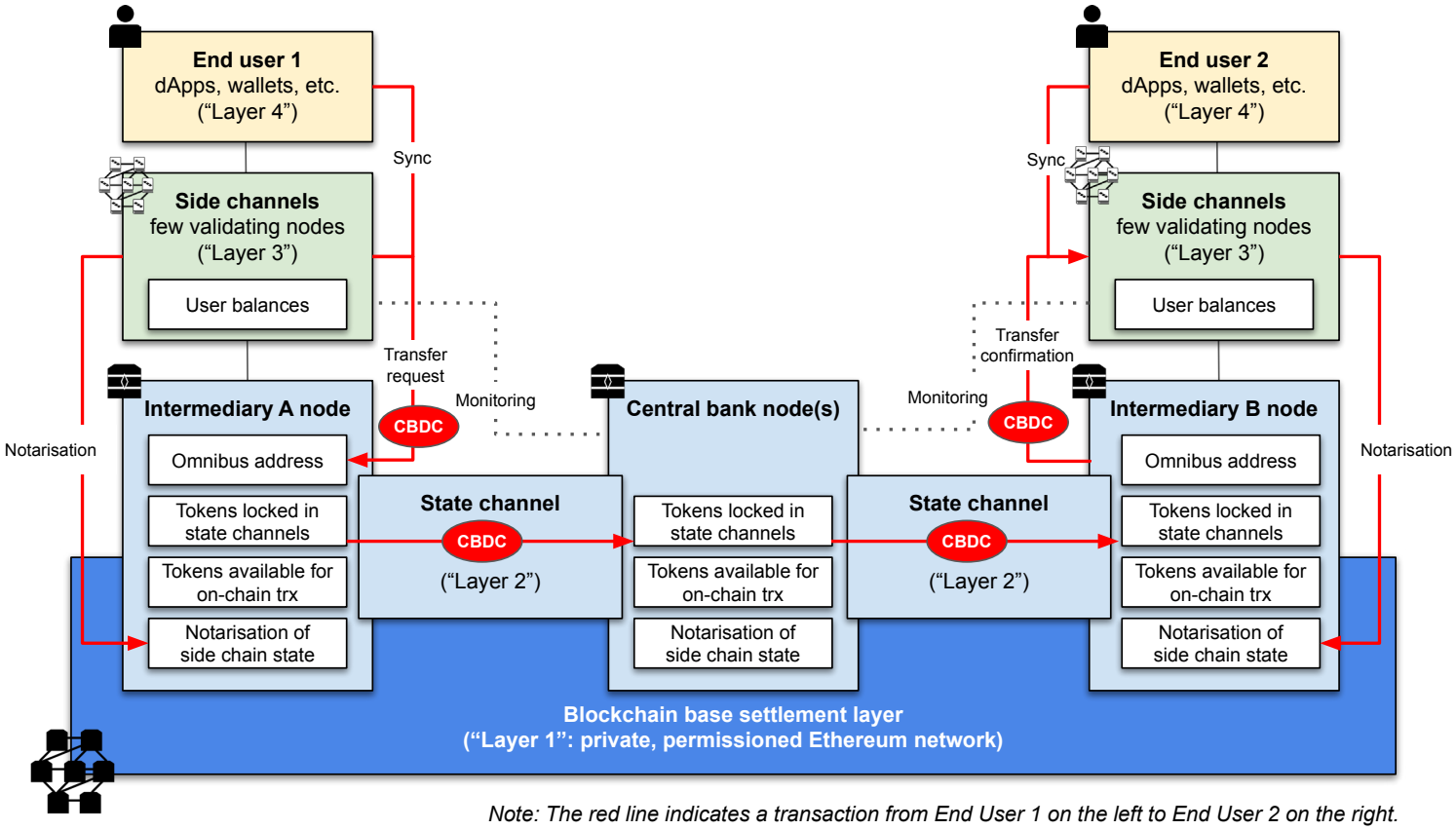
Tokens are powered by smart contracts, which are software applications that live in a distributed fashion in the network. These smart contracts can be programmed rules and business logic that are automatically enforced by the network and can restrict CBDC transfers in any way deemed suitable by the central bank and the regulator. This could make it possible to for instance "hard wire" KYC/AML procedures into the tokens themselves, greatly simplifying and improving the effectiveness of regulatory compliance mechanisms. Tokens could also be pre-programmed with rules that determine exactly under what conditions a transfer can be reversed or assets recovered.

Last but by no means least, proof-of-authority (PoA) consensus on Ethereum is not energy intensive and would support a large-scale network at low energy cost and environmental impact.

TECHNICAL SCHEMATIC

The graphic on page 25 provides a schematic overview of our proposed architecture. It is divided into the following layers:

- **Layer 1/Base settlement layer (dark blue).** There is one base settlement layer on a permissioned Ethereum blockchain.
- **Layer 2 (light blue).** The next layer is comprised of a network of state channels between intermediaries that would enable fast payments.
- **Layer 3 (green).** In this layer each intermediary operates its own side chain, where the central bank or regulator is a participant and can ensure that the supply of money remains consistent with the supply of CBDC allocated to the intermediary in the base settlement layer
- **Layer 4 (tan).** At the top we find many different end user interfaces, offered by banks, telecom operators, mobile phone manufacturers, fintechs and other providers, each in competition with each other and with their own special functionalities, in order to provide the best possible end user experience via competition between these private providers.



Note: The red line indicates a transaction from End User 1 on the left to End User 2 on the right.
Source: ConsenSys

WHITE PAPER

5. Conclusion

There is growing debate surrounding the future of cash in the digital world, and this is posing new challenges to authorities and central banks around the globe. This debate is taking place against a backdrop of doubts about financial stability that were raised by the 2008 financial crisis, of the rise of (private) cryptocurrencies, the development of new digital payment methods, and the entry of large technology companies into the payments arena.

Most countries today are analysing the potential of CBDC, seeing it as a means for governments to maintain their role as issuers and stewards of national currencies and economies. Yet the introduction of a CBDC would itself mean major changes to the existing monetary system and would raise a number of fundamental economic, monetary policy and legal questions. It is no wonder that there is heated debate on the subject in both banking and academic circles.

There are certainly risks involved in issuing a CBDC, as we have touched on above, and central banks will have to weigh these carefully. But they will need equally to evaluate the risks of not issuing CBDC, or doing so too slowly. Without a CBDC, the future of digital money would be largely if not wholly in private hands, leaving businesses and individuals exposed to the risks of private issuers or lack of access to digital tokens in certain markets.

Similarly, being an early mover in the CBDC space could bring significant benefits to a currency, while being behind the curve compared to other jurisdictions could be costly. ECB President Christine Lagarde has said as much with regards to Europe's central bank.[1] Ideally, central banks should be working together to agree on CBDC standards that would allow them to interoperate across borders.

1 ECB should be 'ahead of the curve' on digital currency: Lagarde, Reuters, 12 December, 2019.

In this paper we have tried to both provide some background to the topic and its importance, as well as a concrete proposal as to how to implement a CBDC. While the introduction of a CBDC will involve more than a narrow, technical evaluation of the efficiency of a payments system, it is sometimes by jumping in and trying it out that policy makers and central bankers can get the best sense of both the big picture and the nuts and bolts of CBDC.

At ConsenSys, we strongly believe that Ethereum is one of the only technologies available today that has the potential to answer the technical requirements for such CBDC over the short and mid term. We have also gained a great deal of experience in a short time working with central banks and others on the topic, and thinking about the related issues, both big and small. We are happy to share our experience and expertise and encourage any interested party to reach out to us.

TO CONTACT THE AUTHORS:

matthieu.bouchaud@consensys.net
matthieu.saintolive@consensys.net
monica.singer@consensys.net
ken.timsit@consensys.net

CONSENSYS