CONSENSYS

CBDC IMPLEMENTATION FAQ

20 Key Questions from Central Banks Answered

Central banks around the world are awakened to digital national currencies. Find out which specific questions they are asking our experts.

By ConsenSys

Questions from Central Banks

Overview

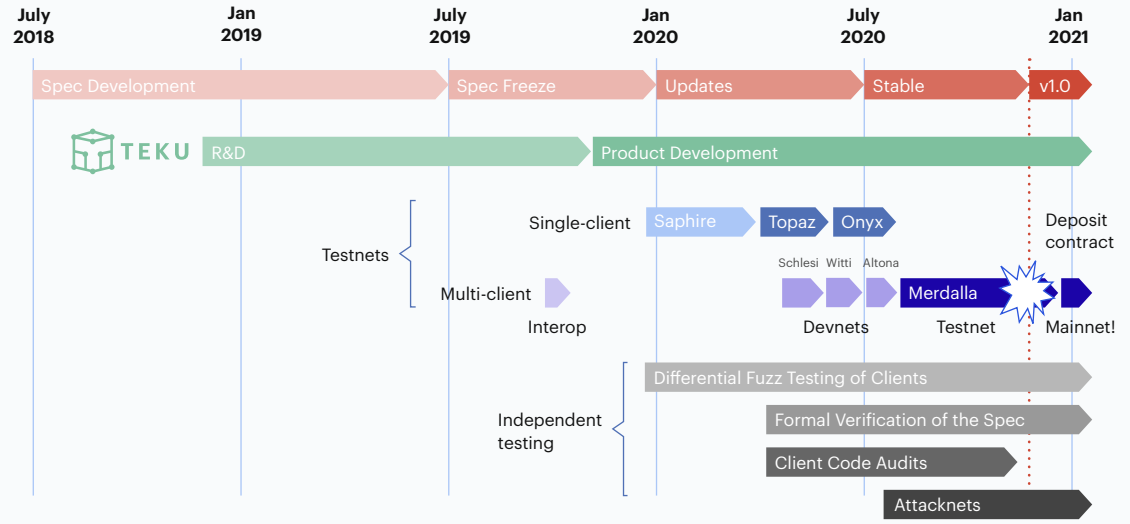
As an increasing number of nations begin to investigate the integration of CBDCs, Matthieu Saint Olive, our CBDC and stablecoin lead expert sat down with representatives from a prominent central bank to answer a range of questions around implementing an Ethereum-based CBDC.

Here's what they covered.

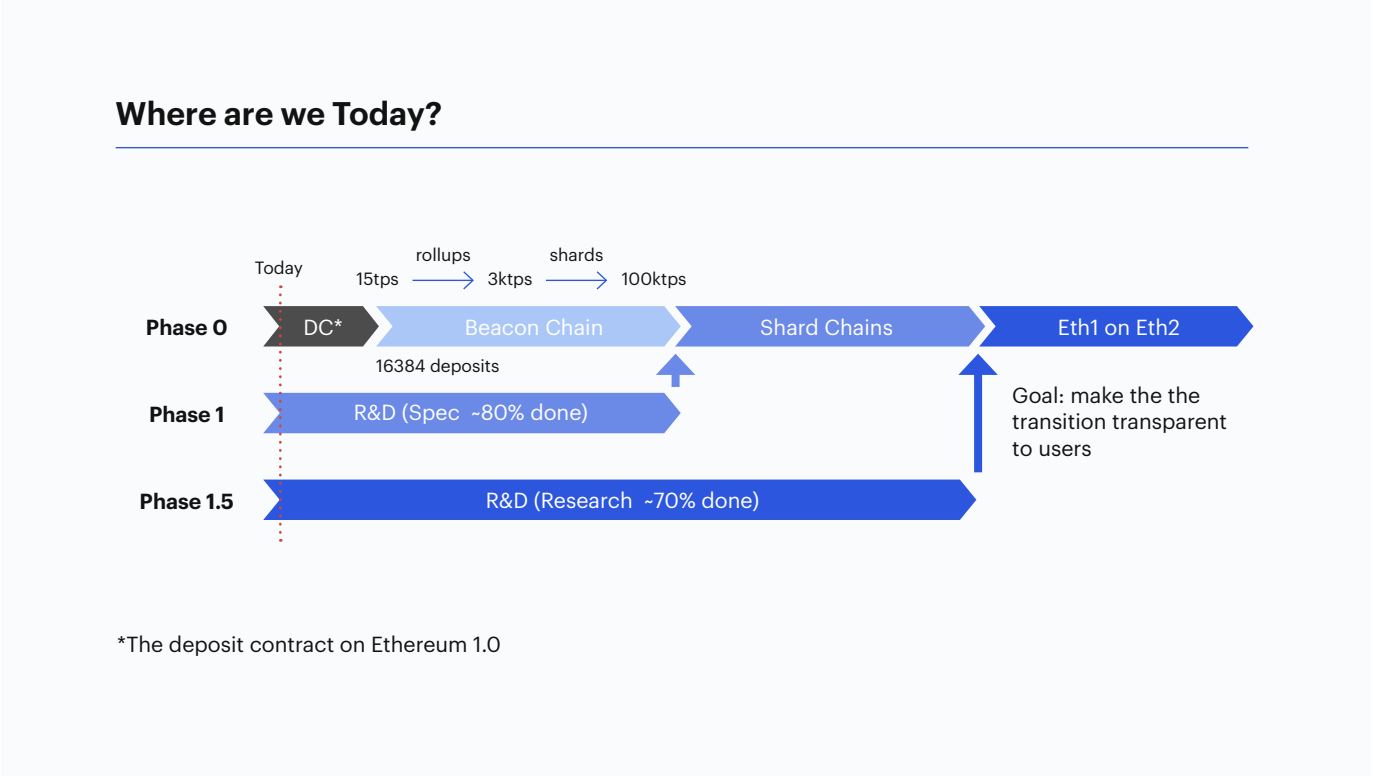
What is the strategy regarding adopting ETH 2.0?

ConsenSys is directly involved in ETH2, which ambitions to address the two significant challenges of the Ethereum public blockchain: scalability and sustainability. This will be solved thanks to a combination of factors, including the migration to the proof of stake consensus protocol, the use of rollups, and the use of sharding. This migration has been prepared for years and more precisely since July 2018, as illustrated below.

Where are we Today?



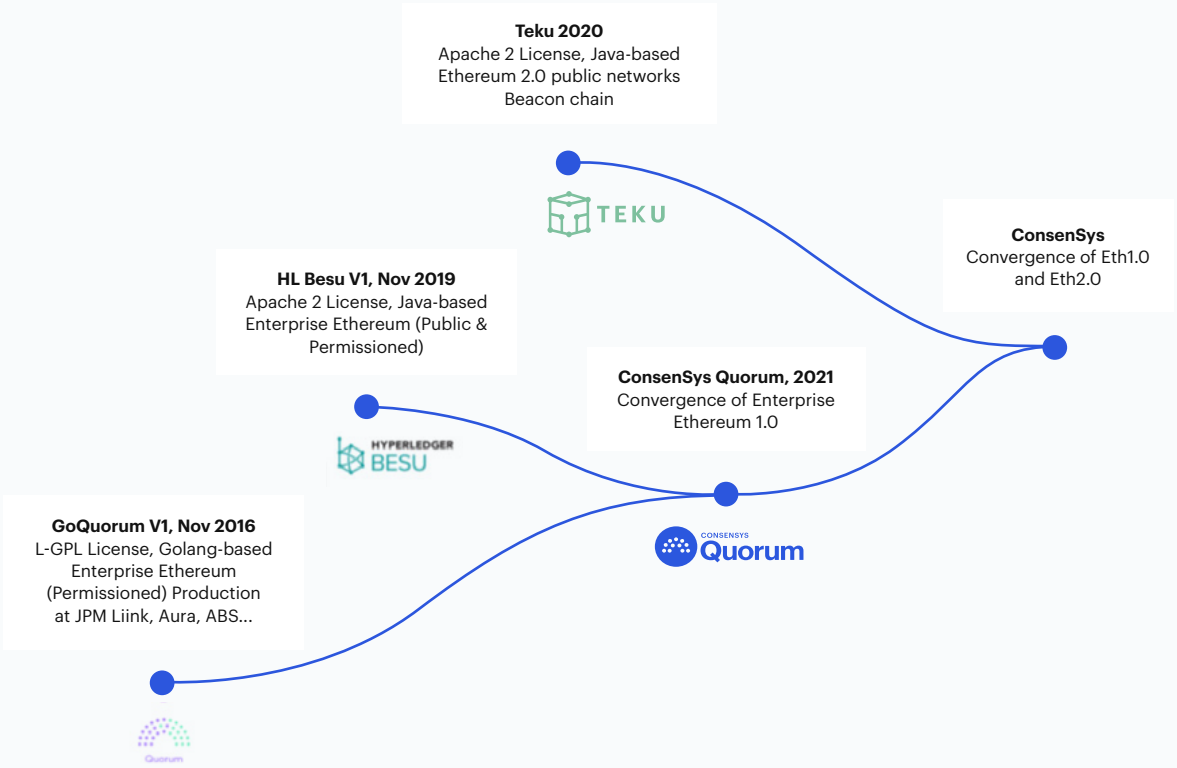
The plan for the future is the following:



ConsenSys is building an ETH2 client "Teku" and a staking service "Codefi Staking," which is already used in production. We are building the rollup software that will serve both ETH2 and our CBDC offering on both public and permissioned networks.
Below are some key points on the relation between ETH2 and CBDC:

- We expect most central banks to choose to run a permissioned Ethereum network for their CBDC and not the public Ethereum Mainnet. The migration of Ethereum Mainnet to ETH2 will not impact those platforms at all
- If a Central Bank were to issue a CBDC on Ethereum Mainnet, the transaction to ETH2 would be seamless. It is a priority for the teams leading this migration, including ConsenSys, to make it as seamless as possible for the millions of users of Ethereum Mainnet
- ConsenSys will continue to maintain all enterprise Ethereum platforms, whether they were built before or after the Mainnet migration to ETH2, as illustrated below.

Long term convergence of Enterprise Ethereum with Ethereum 2.0



Can you compare ETH-based solutions against the newest generation protocols, like Polkadot?

Teams in the ecosystem have launched hundreds of protocols since 2014, and all claim to be better than Ethereum, having solved its scalability challenge (e.g., EOS) or smart contract security (e.g., Tezos), etc. However, Ethereum counts by far the highest number of users and developers.

This community activity is a very valuable asset that leads to the creation and adoption of:

- Infrastructure solutions such as alternative protocol clients, development tools, and open-source libraries (e.g., Open Zeppelin)
- Standards such as the ERC20
- Overlay solutions such as wallets, tokenization management software, layer 2, and privacy solutions.

Hundreds of thousands of developers are working to make Ethereum better and easier to use. If any new solution emerges, it will be offered on Ethereum because the entire developer ecosystem participates in the development. This large and vibrant ecosystem also almost eliminates vendor lock-in.

If an ERC20 token is used for a digital national currency, what would be the role of the underlying ETH?

The role of ETH depends on the deployment model.

Suppose a Central Bank were to issue a CBDC on a private and permissioned Quorum network. In that case, the underlying ETH is not needed because we use a permissioned network and do not need to prevent the node validators from flooding the network because they are regulated. ETH would have no value, and individuals won't need it to use their digital currency wallet. In the short term, we would likely start out with setting the gas price to 0, allowing all nodes, which are known and regulated entities, to send transactions at will.

In some permissioned platforms, we introduce a gas price (and consequently use the underlying ETH) to preserve the platform from DDoS attacks or configure transaction fees. However, the ETH with being different from the ether crypto assets will have no value outside of the private network.

If a Central Bank were to issue a digital currency on the public Ethereum network "Mainnet," then users will need ETH to process their digital currency transactions. On the public blockchain, ETH is used to compensate the network validators and consequently secure the network.

Would the digital national currency need to be bought with the ERC20 token and used to settle transactions? Do you contemplate using gas and ETH in a similar way as in the ETH mainnet?

On a permissioned network, ERC20 would not be used. Individuals will solely acquire and use the national digital coin. On the public network "Mainnet," ETH is used for all on-chain transactions, including settling transactions, interacting with ERC20, and rollup smart contracts functions.

How would the nodes pass these costs (gas fees) to end-users if their access is restricted to Layer 2?

We believe that using digital currency should be free for end-users such as individuals because it is free today whatever means of payment (cash, credit card, Revolut). This will be highly beneficial for corporations, particularly SMEs, to accept digital payments without paying a commission to a credit card provider or other payment service provider.

Though, running a node of a national digital coin platform will have a cost for the participating financial institutions, which may include hosting, maintenance and license. The supporting Blockchain Services Infrastructure could share feedback with the central bank on the costs of using Hyperledger BESU (i.e., ConsenSys Quorum.)

To cover this cost, the financial institutions will find ways to benefit from their network participation, which may include offering paying overlay services to customers. This will accelerate the emergence of innovative payment solutions. We could also imagine using the underlying ETH to measure nodes' activity and finance them accordingly.

Which Layer 2 solution do you imagine fits best for CBDC?

At ConsenSys, we've tried almost all layer 2 solutions and decided to invest in rollups as it appears to be the best layer 2 solution, based on the community and our own benchmarks. Our rollup software is being integrated with our "out of the box" CBDC solution.

Though, multiple layer 2 solutions can be deployed in the CBDC platform. Network participants will be able to deploy their own smart contracts and use them. This is also what we observe on the public Ethereum network "Mainnet," with a mix of custodial solutions (e.g., exchanges), rollup solutions (loopring, optimist, Aztec), state channel solutions (e.g., SKALE).

Note: the reason we believe less in state channel solutions such as Raiden is that, with these solutions, it is required to lock high amounts of funds to enable an efficient payment network. Also, the exits are long and dangerous because participants must always listen to the chain in case someone tries to exit the state channel funds with a fake receipt. The last drawback is that there is no data availability on-chain using State Channels: everything is happening off-chain, and the chain is only used for net settlement.

For technical information on rollups, you can refer to
this recent paper written by Vitalik Buterin.

Will end-users only have access to the Layer 2?

In our proposed approach:

- Regulated entities run validator nodes. Validator nodes are running the Quorum client and consequently participate in the consensus mechanism.
- Validator nodes are also running the rollup software as "rollup operators." By running this software and the Quorum client (and some other middlewares and software), nodes will expose functionalities to the end-users, such as creating an account, querying balance, and transferring money in a secure and censorship-resistant way. Rollup operators can not lie on user balances because the state is updated every block. Rollup operators can not censor user-specific transactions and can not use the money on others' behalf, thanks to cryptographic operations on Merkle trees.
- Validator nodes can offer intermediated access to the network to its customers so that they can read and use the shared infrastructure via APIs. We observe similar intermediation on public blockchains, where several major crypto companies and developers use services such as Infura to interact with the Ethereum Mainnet without dealing with the constraints of running their own nodes.

Having said that, we could also allow anyone to run a node on the platform. Such nodes would likely not participate in the consensus but still directly access the ledger and the platform.

Do your projections accommodate the possibility that end-users do not use your key vault or third-party key vaults?

Yes, it is very much possible, and we believe it is essential. Our solution offers a native key custody solution and some integrations to make it easier to use, but we believe that all users (incl. Individuals, financial institutions, corporates, and the central bank) should be able to choose the custody of their choice. This is one of the key principles that drive the development of the ConsenSys wallet solution: Metamask, a non-custodial wallet.

If users can not custody their own key, they get stuck in a closed system. However, self-custodied keys offer users the possibility to use their money with all wallets. Keys just need to be exported. It would also allow users to not rely on an institution to custody their funds. People may start to custody their hardware or paper wallets "under the mattress" just as they do with cash.

Have you already experimented with the practical feasibility of this approach or is R&D still needed to validate this claim?

For layer 1 transactions, an ERC20 smart contract can be configured with transaction or balance thresholds. We have not implemented this specific logic in production, but it is just a few lines of code, and we have deployed some very similar functionalities for various clients. It is very straightforward to add rules to the smart contract to configure that a balance or a transaction can not exceed a certain amount. Trying to execute a transaction that doesn't comply with the smart contract rules would simply fail. What's important is to define what should be the user experience of this transaction failure. Such rules can be dynamically updated in the smart contract if properly built, allowing all payment operators to automatically comply with the new rules configured in the smart contract.

However, retail transactions are expected to happen in the rollup because Layer 1 can only process a few hundreds of transactions per second. We expect the Layer 1 transactions to be only used by financial institutions to acquire and distribute the digital currencies to their customers and possibly use it for their own business (e.g., for interbank transfers).

For layer 2 transactions, the user balances and state of the transactions are kept off-chain. Only the state (root hash) of the off-chain database and the raw transactions are stored on-chain. Checking the rules will happen off-chain and be led by the rollup operator (i.e., the validator nodes). The rollup operator receives the end-user transactions and processes them off-chain. The rollup software can be configured to verify the threshold rules when it processes the transactions off-chain. If a rollup operator tentatively submits a transaction that violates a rule, this transaction will be discarded by the other nodes or the ZK smart contract provider because invalid. The rules could be configured either in the software itself or as a smart contract that is used as input by the rollup software.

What countermeasures will be put in place regarding cyber-security aspects? For instance, limiting the expressivity (e.g., Turing-completeness) of the smart contract's language?

The Ethereum protocol itself has never experienced any security breach. Only the smart contracts and overlay solutions built on it have been hacked, mainly because improperly developed. This is pretty common with the emergence of new technologies.

To mitigate this development risk, ConsenSys relies on three pillars for all projects:

- Codefi Orchestrate is a middleware that manages the transaction lifecycle. It makes blockchain easy to use by abstracting complexity and makes the integration point with the blockchain completely safe.
- ConsenSys Diligence is a smart contract audit team specialized in Ethereum. It is recognized as one of the most skilled teams within the Ethereum ecosystem.
- ConsenSys systematically uses MythX: it is a security analysis software dedicated to smart contracts. MythX automatically runs the smart contract against sophisticated security rules like reentry attacks.

Having said that, we could also allow anyone to run a node on the platform. Such nodes would likely not participate in the consensus but still directly access the ledger and the platform.

Ethereum's current transaction throughput is around 15 TPS. What steps are being taken to allow for tens of thousands of TPS?

We believe this scalability topic is a crucial one, and we would be happy to schedule a one-hour workshop to walk you through our approach in detail with a demo. It is true that the Ethereum public network "Mainnet" processes around 15 transactions per second. However, with rollups, one public Ethereum transaction can be used to process thousands of retail transactions. Some solutions are already deployed on the Mainnet, such as Loopring, Optimism, Aztec. Ethereum permissioned networks are by default more scalable than the Mainnet because they use a different consensus algorithm. By default, a permissioned network can process a few hundreds of TPS.

As of today, our rollup software allows 10,000+ TPS for ERC20 transfers on a permissioned network. But this level of scalability cannot yet be achieved for all transaction types. The "programmability" and "composability" of rollups to interact with other smart contracts are still in the piloting phase. We expect it to be doable in the next 12 months.

In the meantime, programmability can be implemented via our proposed t wo-tiered architecture:

- The wholesale network (i.e., layer 1) can process all kinds of transactions, up to 300 TPS (e.g., threshold rules, DvP, PvP, security tokenization, bond tokenization…)
- The rollup layer (i.e., layer 2) is used specifically for central bank digital currency transfers, up to 10,000 TPS

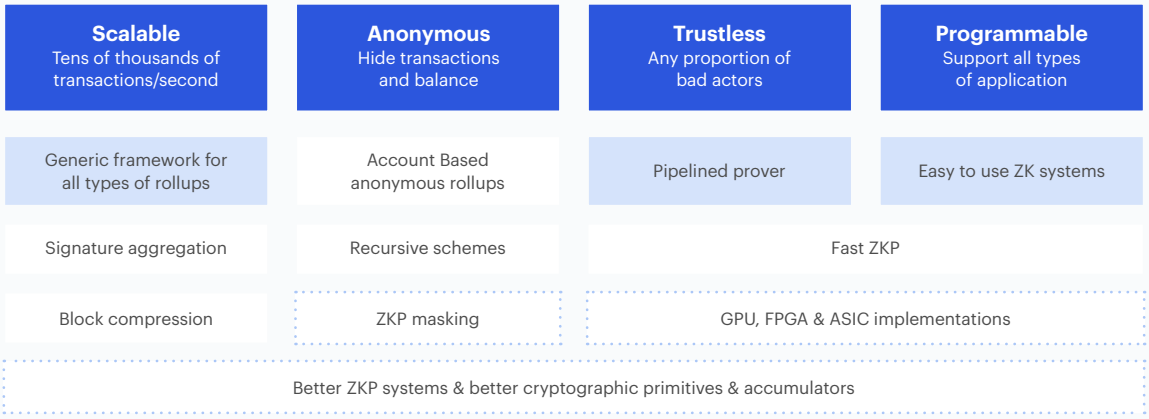
In our last performance testing, we reached 14,000 TPS on a four-node permissioned Quorum platform distributed across the US. The test was performed with 50M accounts. We would be happy to test again with 100M accounts if you are interested. From a Quorum point of view, the number of accounts does not change anything. The only impact is on the rollup operator because of the memory used and Merkle branches to calculate.

Several optimization options could allow us to grow those numbers further, e.g., whether raw transaction signatures should be recorded on-chain or not.

Every user transaction is formed of the following:

From	To	Value	Nonce	Signature	
32 bits	32 bits	48 bits	32 bits	512 bits	= 656 bits

Because the signature is very heavy (~85% of the weight of the transaction), removing the signature from the chain would make the TPS grow significantly. In some business cases, it makes sense to remove it, and there are also many ideas to improve the rollup technology. Below a quick overview of the improvement area:



Would swapping the PoW consensus with PoA consensus be enough to support the high TPS needed for a CDBC?

Indeed, permissioned Ethereum platforms can reach a few hundreds of TPS. This is the throughput available on platforms such as JPM Coin, EBSI, Blockchain, Komgo, Aura, and more. This is why we recommend using rollups as the Layer 2 solutions to grow the platform throughput capabilities to tens of thousands of TPS.

Would an Ethereum-based CBDC rely mainly on smart contracts implementing "payment channels" or rollups?

We plan to use rollups instead of payment channels. With rollups, all transactions are settled on the blockchain. The main difference is that the retail transactions (e.g., Alice sends 10 CBDC to Bob) are not processed on-chain but by an off-chain software. The blockchain is used for what it is best – to reach consensus on the current state of the retail account off-chain database and retail raw transactions.

Rollups as already used in production, for example, for Decentralized Exchanges with Loopring and payments with Aztec.

What consensus mechanism would an Ethereum-based CBDC use?

IBFT2.0.
The key driver of IBFT is to guarantee immediate finality. Finality means that once a transaction is included in a block added to the blockchain, it is guaranteed to always be part of the blockchain. That is, there are no forks or chain reorganizations. If bad actors can fork a blockchain, it is no longer secure.

The super-majority modification changes the number of nodes required to reach quorum. This change addresses the issue of Byzantine nodes being able to reach consensus with two distinct sets of validators by requiring a super-majority. For example, with 5 validators, IBFT 2.0 requires 4 validators, rather than 3, to reach agreement on a block for the block to be added to the blockchain. With this change, a Byzantine validator cannot get two sets of honest validators to reach agreement on different blocks. Read IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks and Another day, another consensus algorithm. Why IBFT 2.0? for more information.

How are transactions being recorded on a single ledger? We understand bearer as 'settled between payer and payee.' How is that possible if each party must record their transaction in a ledger accessed through a bank node?

We understand bearer instruments as the ability to move the assets because the owner has a proof of ownership which is not related to his identity. Whoever is in possession of the private keys is consequently presumed to be the owner of the asset and is entitled to use it.

The fact that a transaction is settled on the ledger by validator nodes is censorship-resistant.

This is similar to public Ethereum "Mainnet," where most users do not run their own nodes and rely on private services such as Infura. As an illustration, Metamask, which is the most adopted crypto wallet in the world with 1M+ monthly active users, uses Infura APIs for all the on-chain transactions. Metamask does not manage an Ethereum node itself.

Complementarily, it could be possible for a payer and a payee to settle transactions directly peer to peer, particularly for transactions in zones that do not have Internet network coverage. Several solutions are emerging on the market, but ConsenSys is not working on such a solution. In theory, those solutions could be easily plugged into the platform we are recommending. A wallet provider could lock the funds registered on the shared ledger and provide a convenient solution that makes it speandable offline. When the payer or the payee gets back access to the Internet, the transaction stored offline (e.g., on the mobile application) can be processed on the shared ledger.

How do you see Quorum evolve in the Ethereum 2.0 roadmap? Is there a risk that Enterprise Ethereum and public Ethereum would go separate ways?

There are no risks. ConsenSys is the leading Enterprise Ethereum client software provider (ConsenSys Quorum = Hyperledger BESU + Quorum), and we are actively working on Ethereum 2.0, for example, with Teku.

ConsenSys teams involved in ETH1 and ETH2 are closely working together.

How many mining nodes would you envision? Would it be possible to control who runs these nodes centrally?

When going to production, we envision a network with 10 to 100 nodes. Those nodes would be operated by the central bank and selected financial institutions. As of today, growing the network beyond 100 nodes would impact performances (incl. TPS and transaction finality time).

However, more stakeholders will access the infrastructure without running a node via API gateways. This is similar to what we observe on the Mainnet, where 100,000 crypto-companies and developers use Infura to use Ethereum in their applications.

Rules can be configured. It is possible to mandate a single stakeholder (e.g., the central bank) to define who can participate in the network or a vote or something else.

Is your CBDC idea available only for wholesale intermediaries (Banks, PSPs) or also retail users? Is direct access to the ledger possible for end-users? Can users deploy smart contracts and exchange transactions?

CBDC will be available to the general public.

A Central Bank can decide whether or not the general public can directly read the ledger.

- In public networks (e.g., Ethereum Mainnet), anyone can run a node and read the ledger with block explorers such as Etherscan.
- In most permissioned networks (e.g., Komgo, CBDC pilots), the ledger can only be read by permissioned stakeholders. Those stakeholders then offer overlay solutions to their customers to allow them to see their holdings, transfer money, etc.

Our reference architecture supposes that only licensed entities can run nodes and can consequently deploy smart contracts. The nodes can also deploy smart contracts on behalf of others.

It is also feasible to allow the general public to access the permissioned blockchain directly if needed. Note that if they participate in the consensus, it will impact the performances (similar to the public network) because all participants will have to process all transactions.

Adoption is vital for the success of Central Bank Digital Currencies, but adoption is contingent upon the cost born by citizens and banks. How much would it cost for Banks and PSPs to transit to an environment based on this technology?

Building a digital currency platform would be significantly cheaper and faster than it was to build RTGS platforms. Blockchain is the technology that allows using the Internet not only to share information but also to transfer value. This was the first ambition of Bitcoin, as illustrated by the white paper title "Bitcoin: a peer-to-peer electronic cash system." A blockchain protocol is designed for transferring value, which was not the case of the database technologies used for RTGS platforms. The price will depend on the platform design (e.g., features, throughput, etc.)

It will be quite simple for financial institutions to use this platform and not costly. ConsenSys Quorum is an open-source software, consequently free to use.

The costs that may occur are mainly:

- Hosting for the node and the software in performant machines
- Some service/maintenance teams monitor and run the platform 24/7
- Licenses for the software(s) sitting on top of the blockchain to manage users, screens, workflows to craft and sign transactions, keeping the private key secure, etc. The software will be the same for all licensed entities running the network (banks, the central bank, and large PSP), helping mutualize costs. A central bank could decide to build that software from scratch or leverage existing solutions or use a mix of both.

Many financial institutions are already using ConsenSys Quorum (including JP Morgan, Société Générale, BNPP, Deutsche Boerse, Santander, etc.) Institutions that want to reduce the burden of running their own node will rely on intermediated solutions similar to Infura.

If the central bank is the trusted instance, why should we consider moving to a decentralized platform?

Ethereum is a protocol that can be used for both public and permissioned networks. ConsenSys is leading Enterprise Ethereum on permissioned networks with ConsenSys Quorum.

In any case, the trust in the central bank is the reason why we would configure the platform only to authorize the central bank to create and destroy a Central Bank Digital Currency. A central bank may also want more admin capabilities such as blacklisting wallets. All systems need various roles and responsibilities. The benefit of using blockchain is that any change made in the shared infrastructure automatically notifies all other participants. This allows all stakeholders to behave according to a shared, single source of truth for all the above information, with an immutable ledger. As the rules are embedded into the protocol and cannot be avoided, this will remove the need for audits and reconciliations.

Do you see a future for "central custodial wallets" like the Ledger Vault, where keys are stored centrally but under the control of the client?

Yes, decentralization can be introduced without necessarily having full self-sovereignty. We imagine a model where most users will have their keys custodied by intermediaries whose offerings will take multiple forms (including hardware and software wallet, custodial and non-custodial.)

The settlement of all transactions is done on the shared ledger, which introduces decentralization to keep the transactions history, manage the settlement, and keep balances.

With end-users only able to engage with digital national currency through licensed banks, isn't this more or less what the current banking system is doing, only without a cash option?

Our proposition to solely allow regulated institutions to read and write in the ledger can be challenged and expanded.

This hypothesis's rationale is that a central bank would need a final and environmentally sound consensus algorithm, which is why we recommend using IBFT 2. Known and regulated financial institutions should run this consensus algorithm. This is an interbank layer that can be used as a public good, similarly to public blockchain infrastructure. Regulated financial institutions are the validator nodes: they make sure that all transactions follow the protocol and, in particular, prevent double-spending.

For simplicity, we suggested that only the validator nodes can read the blockchain ledger, participate in consensus and run software that uses it. However, it is absolutely feasible to configure the digital currency platform as a public and permissioned network, similar to some testnets (e.g., Rinkeby, Ropsten). In that case, only regulated financial institutions can run validator nodes, but anyone can participate in the consensus and read the ledger. This decision is up to the central bank.

In both cases, we expect some nodes to provide API access to the blockchain to allow their customers to develop applications with the digital currency. This service will be similar to Infura, and Infura could be used for a digital currency platform as a service.

In both cases, each individual wallet balance and transactions are recorded on the shared ledger, and the digital currency is a direct liability to the central bank. The validator nodes are responsible for processing and securing the ledger, but do not control the underlying assets' ownership. The end-user manages the custody of its assets through the custody of the private key, either by himself or by relying on a trusted 3rd party. This is similar to the public blockchain, where miners are responsible for the consensus, but each individual is the owner of its assets and the only one who can use it because he is the sole owner of the private key that must be used to operate the underlying assets.

We believe that the benefits of this infrastructure compared to existing banking infrastructures are the following:

- The shared infrastructure can embed rules (programmability), including the central bank administrative rights.
- The shared infrastructure removes dependencies that emerge with open banking APIs and enable seamless on-chain composability.
- All transactions are settled in real-time, removing the reconciliation needs for the banks.
- It is possible to self-custody the private keys, and consequently, the underlying assets, for example, "under the mattress."
- The ledger is immutable, which will improve financial integrity and trust.
- The infrastructure is decentralized and does not have a single point of failure. Which means that even if some banks node are not working (including the central bank node), individuals will still be able to use their funds

Many financial institutions are already using ConsenSys Quorum (including JP Morgan, Société Générale, BNPP, Deutsche Boerse, Santander, etc.) Institutions that want to reduce the burden of running their own node will rely on intermediated solutions similar to Infura.

Why DLT / ConsenSys Quorum for CBDC?

Brand assets	Efficiency gains (retail time & final tx, no reconciliation needs); allows wholesale txs
Resiliency & security	No single point of failure; cryptographic schemes; powers large scale platforms
Traceability	Ledger immutability for financial integrity & trust; targeted monetary policies
Interoperability	Standard way of representing assets; wallet and platform interoperability
Programmability	Smart contracts to automate business processes (eg., interest rates)
Composability	Tokenized assets can be composed as lego blocks to foster innovation
Privacy	Tiered privacy capabilities, privacy groups, Zero Knowledge Proofs
Scalability	High transaction throughput with "layer 2" solutions (current: 10,000+ TPS)
Large ecosystem	Wide variety of tools and solutions available; drastically reduce vendor lock-in
Compliance	Protocol based compliance for AML-CTF; ledger analysis & reporting tools

What if the wallet's keys are lost? Can a PSP recover the money held by the wallet?

It depends.

For custodial wallets, i.e., a private service provider custodies the private key on behalf of its user and allows its customers to use their funds by proving their identity with a login and a password:

- Logins and passwords can be recovered because the intermediary knows the identity of the holder. If a user loses his private key, he will prove his identity to the service provider and be able to recover them and consequently recover his money.

For non-custodial wallets, i.e., the user is custodying its private keys themselves (e.g., with a hardware wallet or paper wallet or else):

- Losing private keys might be similar to losing a physical wallet and the cash that's in it. Funds are lost.
- Backup seed phrases are a combination of 12 words that are used to regenerate private keys. An individual can store his seed phrase in multiple places, e.g., on a piece of paper stored in a physical vault or "under the mattress" or on a password manager or somewhere else.
- We observe the emergence of new solutions such as the Argent smart contract wallet, allowing users to configure recovery contacts who can together generate a new private key and enable them to recover their funds.

Also, independently of the wallet used, it could be possible for the central bank to be able to freeze specific wallet funds with an on-chain "blacklist" and then re-issue the funds to the owner on a new wallet. ConsenSys could build this kind of recovery protocol for an interested central bank.