CONSENSYS

CONSENSYS GUIDES

Libra: Understanding Facebook's Cryptocurrency

Written by Coogan Brennan, Technical Trainer at ConsenSys Academy

CONSENSYS **ACADEMY**

Interested in learning the essentials?

Regular price: $99
Save 35% with our pre-launch sale!
Price for you: $65!

http://consensys.academy/essentials

USE COUPON CODE BE_35_OFF_LIBRA

Interested in blockchain development?

Regular price: $295
Save 20% with our pre-launch sale!
Price for you: $236!

http://consensys.academy/ondemand

USE COUPON CODE BDP_20_OFF_LIBRA

CONTENTS

Intro

Regardless of what you think about Facebook, its announcement of Libra immediately created an enormous, captive audience for the larger ideas of blockchain. Not only do they have 2 billion users, but Facebook also influences people's everyday lives in a way no other company has before (other than maybe Google). As leaders in this space, we at ConsenSys believe it's incumbent on us to use our expertise and experience in the field to help bring that expertise and experience into the public discussion.

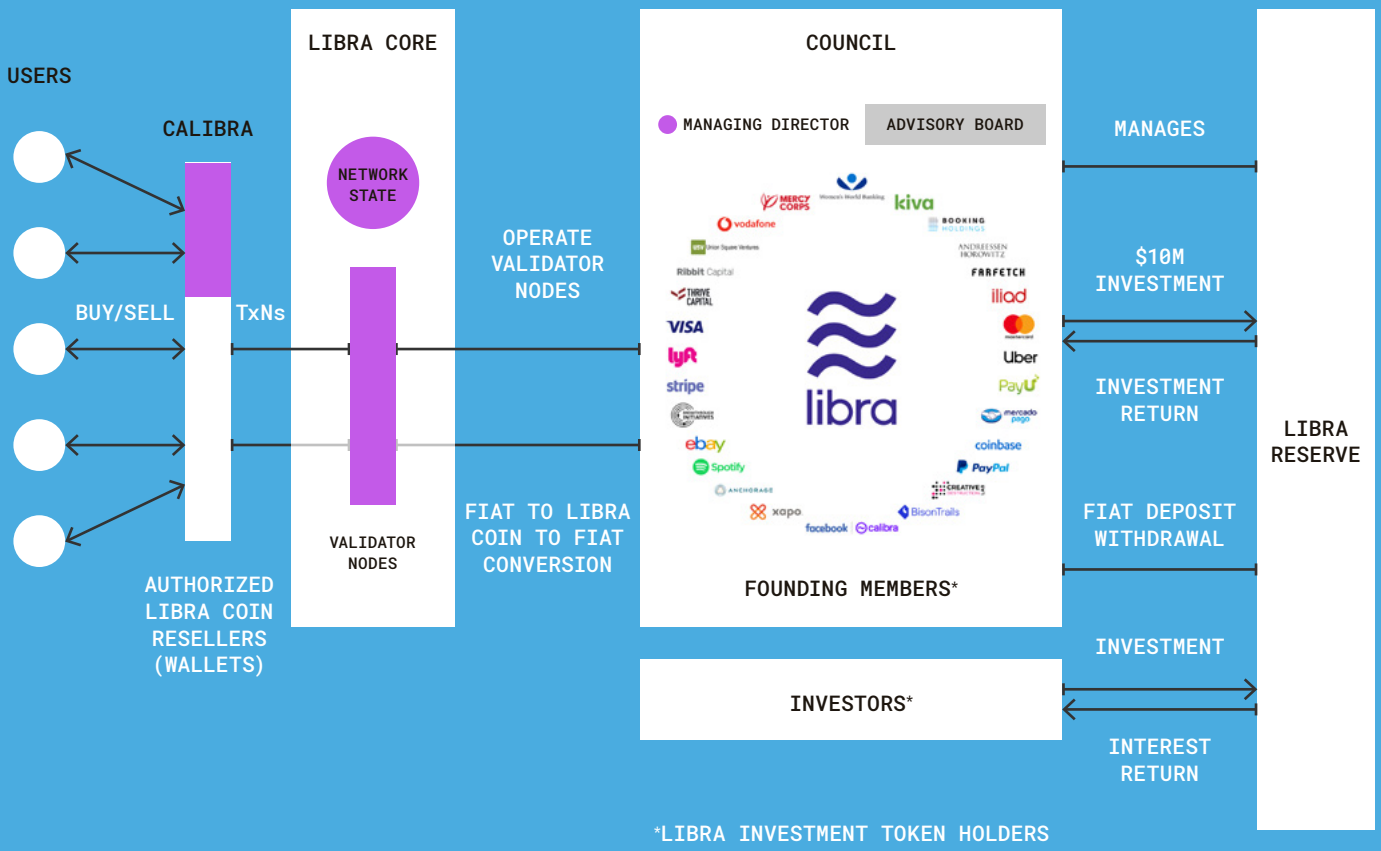
We also think there's a very real opportunity for ConsenSys and the greater Ethereum community to help inform Libra's continued development.

Libra has made lots of claims for what it would like to do in the future, but they're also in some ways asking the world to accept Libra now. It's a tough needle to thread and we've decided to focus on what they've proposed as their Minimum Viable Product (MVP).

We will try to limit the speculation as much as possible, and we will make it very clear when we're speculating or basing a statement on a non-Libra resource.

Note that we won't be discussing how a permissionless Proof of Stake network would work, and we won't discuss too much about the social impact allocation of Libra Coin. We're getting down to brass tax—what's been proposed in the technical documentation and public statements from Facebook, Libra, and Calibra.

Libra Ecosystem Map



The Libra Association

The Libra Association is the overarching organizational body that has three main functions:

1. GOVERNANCE

Manage the "Founding Members", as the association's partners are called. This has been in the news the most because it involves not just Facebook, but 27 other businesses, including Visa, MasterCard, and PayPal. However, there has been reporting by Nathaniel Popper in the New York Times that the agreements signed are non-binding and no money has changed hands yet.

2. MANAGEMENT OF THE LIBRA RESERVE

This is the reserve that is backing Libra Coin which is causing people to call it a "stablecoin," which is a blockchain term. These resources come from the $10m membership fee validators are required to pay OR from fiat consumers use to "buy into" the Libra ecosystem.

3. MANAGEMENT OF LIBRA CORE

This can be a bit confusing, but Libra Core is the software implementation of the Libra Protocol. Everyone who participates in the Libra blockchain must interact with the Libra Core software. The Libra Association acts as a gatekeeper to the Libra Core software screening any updates and making sure it doesn't violate the Founding Members' Terms of Service.

Think of The Libra Association as a big business organization, having to deal with international regulation and the Reserve.

“The Libra Network borrows a lot from Ethereum and other blockchain projects”

Libra Network

Libra Network is the permissioned, consortium blockchain network proposed by Facebook. For security and regulatory reasons, all traffic in the network is directed through a group of validators nodes, which will initially be comprised of the Founding Members. They are all running Libra Core and using the $10m membership fee as a “stake” in the network to maintain its safety and security. The Libra Network borrows a lot from Ethereum and other blockchain projects, which is discussed later in the technical section of the guide.

Calibra

Calibra is Facebook’s digital wallet platform, which will be the “on and off ramp” for consumers to submit transactions to the Libra Network. There are not many technical details that have been revealed by Calibra or Facebook about Calibra, except that it will be embedded in all of Facebook’s digital products and therefore available to all Facebook customers. Point of Sale, consumer-level questions still need to be further addressed and has not been the immediate focus of the informational hearings.

Libra Association and Libra Reserve

While almost all of the Libra Project is a proposal, the Libra Association and its management of the Libra Reserve is particularly speculative. In the first few lines of the documentation outlining the Libra Association, it says:

"This proposal [The Libra Association whitepaper] will serve as a basis for discussion among the association's members, leading to the modification of its charter and formulation of its bylaws" ["Libra Association," "Overview: the Association & Council"]

This means that the details outlined in the Libra Association white paper itself will need to be debated and voted on by the Council members, most likely requiring a two-thirds supermajority of all stakeholders (the Founding Members outlined in the previous section).

STABLECOIN & LIBRA RESERVE

- Price stability a concern
- 1:1 asset backed, initially from investors
- "Basket of Fiat Currencies"
- Libra Coin backed by Reserve assets
- Outstanding Questions
- Creation…

One of the current challenges for businesses trying to use cryptocurrency is the fluctuation in secondary market price, such as in USD or Yen. The blockchain communities have come up with a general term for a solution to this problem: stablecoins. These are coins that are either a) regulated by an algorithm to maintain a certain price (such as DAI, the MakerDAO token) or b) 1:1 asset backing (such as GeminiUSD). Facebook has decided to use the latter to create stability in Libra.

The Libra Association collects $10 million from each member, bundles all that up and puts it into something called the Libra Reserve. "Libra Reserve is managed by the [Libra] association with the goal of value preservation" [Libra Association 1.C]. Meaning they want to invest that capital into something that will be relatively stable over time and not dependent on one government.

So, here's the investment strategy:

"The actual assets will be a collection of low-volatility assets, including bank deposits and government securities in currencies from stable and reputable central banks. [T]he association will only invest in debt from stable governments with low default probability that are unlikely to experience high inflation. […] In terms of liquidity, the association plans to rely on short-dated securities issued by these governments, that are all traded in liquid markets that regularly accommodate daily trading volume in the tens or even hundreds of billions. This allows the size of the reserve to be easily adjusted as the number of Libra in circulation expands or contracts."

Creation of Libra Coin

The organization will use the funds parked in a group of stable banks (essentially, a basket of bonds) which will then theoretically maintain a relatively stable price over time. So there's a stable price mechanism, and Libra Coins will be minted against the Libra Reserve, against those assets.

Allocation of Libra Coin will happen two ways:

The first way, which people may be somewhat familiar with, is allotting Libra Coins to Founding Members based on their $10m buy-in or membership fee. The Founding Members will then turn around and "stake" those coins in the Libra Network (which we'll talk about later), essentially guaranteeing the safety of the network at the risk of losing this investment.

The second way—which people aren't as familiar with—is through the currency that individual consumers use to buy into the network.

New Libra Coins will be minted for users as a 1:1 equivalent for "fiat and transfer of that fiat to the reserve."

This hasn't been discussed as much but is a crucial element of the network and one that brings up a lot of outstanding questions.

It also leads us to our last feature we'll discuss in the Libra Reserve: **Authorized Resellers**

In the Libra Reserve white paper, it says:

"Users will not directly interface with the reserve. Rather, to support higher efficiency, there will be authorized resellers who will be the only entities authorized by the association to transact large amounts of fiat and Libra in and out of the reserve."

To partition off KYC / AML and local regulations, Libra creates a barrier between the Libra Reserve and customers by creating a class of network participants called "Authorized Resellers". In an episode with Laura Shin on her podcast Unconfirmed, Libra's Head of Communication and Policy suggested Libra would push down local regulation, and adherence to the Authorized Resellers with Libra Reserve would typically deal with international AML laws that are currently in place for international financial institutions.

So, the authorized resellers will be digital wallets that act as the on- and off-ramps for customers. They will take local currency from users of their digital wallet and provide Libra Coin in return. In some sort of transaction, those authorized resellers will either purchase a large amount of Libra Coin in their local currency, or somehow obtain a large amount of Libra Coin which they then distribute to their users.

Libra Reserve Outstanding Questions

Libra proposes to help the unbanked. However, the Libra Reserve, which will back the Libra Coin, can only grant Libra Coin to a new user if it accepts that user's fiat in return. What currency can someone who is unbanked use to buy into the system? How can you serve unbanked populations when you need to take their local currency and somehow convert it to a stable note?

If someone in the US wires remittances to their family in the Philippines, can the family withdraw that into a local currency? Or do they have to stay on the Libra Network using Libra Coin?

What sort of Silicon Valley investor will invest to see the kinds of "stable returns" the Reserve needs to maintain?

The Chinese Social Credit Score has been used to create a list of individuals who are not allowed to take a certain trainline or purchase certain products due to the behavior deemed bad by the State. If Calibra becomes a dominant mode of payment, could Facebook use a social credit score to "ban" people from using their financial services?

Countries with small economies or large unbanked populations typically have tight currency restrictions to prevent the concentration of its currency in the hands of organizations outside of its country. If the authorized resellers must give money to Facebook, how can that happen in a large way without violating those currency restrictions?

There are obviously many logistical, financial, and ethical questions that require further elaboration and detail before the execution of Libra.

Regulatory Response from Central Banks

- Federal Reserve
- Bank of International Settlements
- **Positive(-ish):** Mark Carney and Bank of England
- **Less Positive:** G7

- Federal Reserve: Powell says Fed is looking into Facebook's Libra cryptocurrency, flags 'serious concerns'
- Financial Times reported: "Agustín Carstens, who heads the Bank of International Settlements, known as the central bankers' bank, told the Financial Times that the organization supported the efforts of the world's central banks in creating digital versions of state currencies. "Many central banks are working on it; we are working on it, supporting them," Mr Carstens said."
- Financial Times: "Central bank plans to create digital currencies receive backing" (June 30th, 2019)
- Relatively positive from Mark Carney said it could substantially lower costs and increase financial inclusion, but needs regulation. In a separate decision, Bank of England also announced it will be the first central bank with plans to open up access to its balance sheet to new payment providers including firms and users of payment services.

Regulatory Response from Governments

- Facebook has said that it won't launch its digital wallet service in India, citing regulatory restrictions. https://www.coindesk.com/facebook-says-it-wont-launch-crypto-in-india-due-to-regulatory-issues
- China is launching their own cryptocurrency: South China Morning Post: "Facebook's Libra forcing China to step up plans for its own cryptocurrency, says central bank official" (July 8th, 2019)
- "Germany's Finance Ministry, in an internal paper, said the government should work on ways to prevent Libra from becoming a full alternative to the Euro, according to a senior government official" — WSJ

U.S Regulatory Response

- National Security Concerns
- Privacy and Data Concerns
- Wallet Interoperability Discussion

What we'd expect.

"Facebook has been successful at creating a magnifying glass rather than a mirror- concentrating focus on most divisive issues and manipulating emotions. Now you want to get involved with people's bank accounts and monetary policy— how can we fathom trusting this entity to do this responsibly?"

The U.S hearings about Libra have so far been informational in nature. Many politicians stated their desire to foster innovation and growth while remaining hesitant at Facebooks potential oversight and control within The Libra Association. There will likely be many more information sessions and congressional hearings about Libra, Facebook, and the various still unanswered questions.

Technical Part

SIMILARITIES TO ETHEREUM 1.X

- Libra Core written in Rust
- Authenticated database based on Merkle trees
- Storage bloat concerns
- Node discovery methods
- Gas Metering
- Transactions...

We'll now move on to the more technical aspects of Libra. Frequently, the Libra whitepaper mentions aspects the **Ethereum 1.x** community is also dealing with, for example:

- It mentions Rust has been researched by many blockchain projects due to its speed and security.
- They address the issue of storage and discuss rent in terms of regulating network memory.
- Their peer discovery and gossip methods look similar to DEVP2P, Ethereum's current network protocol.
- They use gas metering to guard against Turing-complete errors or DoS errors.
- Here's an image of a transaction in the proposed Libra network:

3.2 Transaction Structure

A transaction is a signed message containing the following data:

- **Sender address:** The account address of the transaction sender. The VM reads the sequence number, authentication key, and balance from the `LibraAccount.T` resource stored under this address.
- **Sender public key:** The public key that corresponds to the private key used to sign the transaction. The hash of this public key must match the authentication key stored under the sender's `LibraAccount.T` resource.
- **Program:** A Move bytecode transaction script to execute, an optional list of inputs to the script, and an optional list of Move bytecode modules to publish.
- **Gas price:** The number of Libra coins that the sender is willing to pay per unit of gas in order to execute this transaction.
- **Maximum gas amount:** The maximum number of gas units that the transaction is allowed to consume before halting.
- **Sequence number:** An unsigned integer that must be equal to the sequence number from the sender's `LibraAccount.T` resource. After this transaction executes, the sequence number is incremented by one. Since only one transaction can be committed for a given sequence number, transactions cannot be replayed.

This is so similar to an Ethereum transaction! However, in Ethereum address and public key are combined protocols. Another notable difference is the "program" field, which in Ethereum is the data field and holds smart contract deployment code, function parameters, etc.

SIMILARITIES TO ETHEREUM 2.0

- Rotating Leader Proof-of-Stake / Slashing
- Randomness
- libp2p
- BLS12-381 Signature
- Future?

They also mention aspects similar to what Ethereum 2.0 has confirmed as part of the new ecosystem. This includes:

- The Rotating Leader PoS consensus is similar to what has been proposed for Ethereum 2.0. Libra discusses slashing as a disincentive mechanism for misbehaving validator nodes.
- "Both networks are looking at ways to minimize influence for leader selection by proposing different schemes dealing with pseudo or biasable randomness."
- Libra says its network protocol is "inspired" by libp2p, something that Ethereum 2.0 has also recently decided to use:
- Libp2p. "The network layer is designed to be general-purpose and draws inspiration from the libp2p project." [LibraBFT white paper] Section 6
- In the Libra Core repository, they have a folder called "Nextgen crypto" which has the BLS12-381 curve in it, the same one being used for Ethereum 2.0.

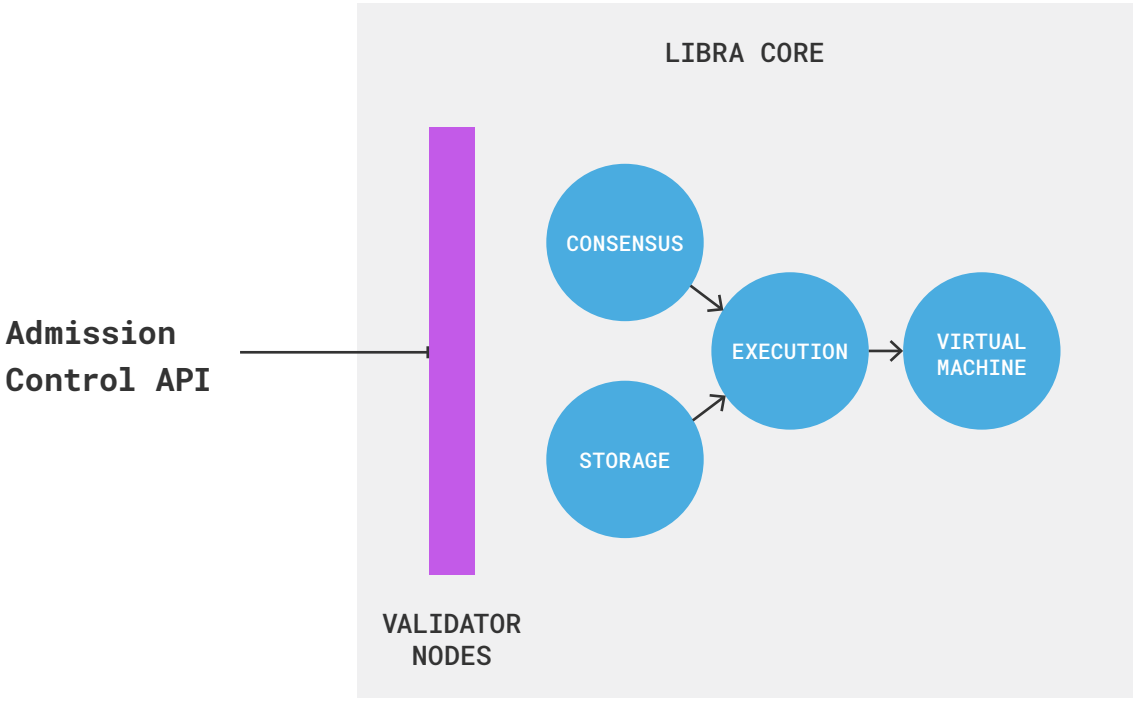
> *Founding Members of the Libra Association are both the gatekeepers and maintainers of information about the Libra blockchain."*

LibraBFT

The Founding Members of the Libra Association are bought into the network with $10m. In the Libra Network, they become known as Validator Nodes, meaning they are both the gatekeepers and maintainers of information about the Libra blockchain. As validators, they obey certain rules, which we call consensus. That consensus model is called LibraBFT.

LibraBFT is a leader-led consensus model by vote, meaning that the Founding Members will take turns authorizing the transactions that are coming into the network. It uses cryptographic features that blockchain people will be familiar with such as digital signatures, hash functions, and public-private key encryption.

LIBRA VALIDATOR EXECUTION



All calls to the network go through a single API, a single endpoint, called Admission Control. Non-validators have two types of calls they can do: query and submit transaction.

It's a strict control on the network traffic, meaning that the demand on the Validators will be high. It's a more centralized model, which is a trade-off Libra is willing to make for speed and security.

This is not unusual for a blockchain network that is a consortium, but it is definitely different from Ethereum or Bitcoin, where theoretically, anyone can submit a transaction or run a mining node. There are challenges with this as well.

The point here is that there's a single API endpoint available to users from validators and they act as a shield of sorts into the inner sanctum of the network.

And what's going on in that inner sanctum? Well, if you look to the right of the diagram, you can see the processing of the network is happening in a few, separate stages. This gives it increased capacity: the documentation specifies there are no CPU limits on transactions.

Move Programming Language

This separation of consensus, execution, and storage is an interesting aspect that brings us to our last technical feature of the network. Remember, Libra has a limited number of actors, all of whom are tightly regulated in their own industries and want to be able to share data in a standardized and trustless way. This will be important as we discuss the blockchain programming language Facebook has proposed, Move.

Ethereum also has only "one" language understood by the Ethereum VM and that is EVM bytecode. Solidity, Vyper, LLL, etc all just compile to it. Libra operates the same way and only has Move bytecode. As Libra matures, it's likely we'll see other languages that compile to Move bytecode. For now, we just have Move IR which uses Rust-like syntax.

Move uses something called a First-Class Resource which programmatically introduces the idea of ownership to their network, but only for certain variables that you want to maintain strict security on. For example, a Libra Coin is a First-Class Resource within the network, but the integer representing the address that coin is going to is not.

First Class Resources take variables that are normally secured with cryptography and constricting it even more with this typing to give it more security on a programmatic level.

Move is currently implemented in Rust-like syntax. In the same way that Solidity resembles Javascript, Move looks like Rust. Rust is studied by many blockchain researchers because it's very fast and Rust has a unique sense of ownership. According to Wikipedia, "Rust has an ownership system where all values have a unique owner."

"The key feature of Move is the ability to define custom resource types with semantics inspired by linear logic: a resource can never be copied or implicitly discarded, only moved between program storage locations." [ibid] Section 3.1: "First-Class Resources"

Another quote, this time from Calibra's tech lead on the Rust subreddit a few weeks ago:

"As a project where security is a primary focus, the type-safety and memory-safety of Rust were extremely appealing."

One of the bugs that comes up frequently in Ethereum (and cited as informing the Move language design) is smart contract programmers mishandling variables. Rust creates a certain level of safety by catching some of the common ways that people could accidentally send money somewhere they didn't want or accidently delete it.

Essentially, Rust (or rather, the Rust compiler), enforces ownership rules at runtime" which creates a lightweight verification tool to catch user errors and prevent certain bugs.

PEER-TO-PEER PAYMENT TRANSACTION SCRIPT

```
public main(payee: address, amount: u64) {
  let coin: 0x0.Currency.Coin = 0x0.Currency.withdraw_from_sender(copy(amount));
  0x0.Currency.deposit(copy(payee), move(coin));
}
```

Here's a quick example of that happening: notice move() is used here to send, not copy(). (Hence the name!)

I believe the reason the language is called Move is because move is an extremely important operation within the virtual machine of the blockchain, as it handles these so-called First-Class Resources specifically.

Smart Contracts are called modules in this network and written in Move. They are not going to accept third-party modules yet (no app store here) and you can see why once you understand the importance of the first-class resources: the modules themselves don't hold state but they do have the privilege of creating First Class Resources in the network. Those resources inherit those extra security features of unique ownership.

Libra Coin, their token, is represented as a "resource in the system," and is only assigned to one account at a time. It's represented that way in the system state. It's the only module currently in the system, which makes sense as Facebook and Libra are the main infrastructure supporters right now.

"The key feature of Move is the ability to define custom resource types with semantics inspired by linear logic: a resource can never be copied or implicitly discarded, only moved between program storage locations." [ibid] Section 3.1: "First-Class Resources"

Not to put too fine a point on it, but we can see here that the Validators, if they are MasterCard, for example, already have access to a large state of information – the assets of their customers. Move, tied into the permissioned network, grants a way to make that state more efficient technologically, particularly as data is passed around.

Conclusion

We've just scratched the surface here today. However, we do think we've given a good overview of the system, including some of the design decisions that Libra made.

Maximally, decentralized systems are the most secure, and Libra is not maximally decentralized. The more decentralized the system, the more secure it will be against malicious actors (hacking). The Libra consortium is only as decentralized as the number of validator nodes in the network, which today is made up of 29 of some of the world's largest enterprises and financial institutions, which only seems to further centralize power. In comparison, the Bitcoin and Ethereum blockchains have thousands of nodes maintaining the network across the globe. It's impossible to say whether Libra will succeed after such little time, but it will be an important narrative that increasingly brings blockchain technology into the mainstream world.

CONSENSYS **ACADEMY**

Interested in learning the essentials?

Regular price: $99
Save 35% with our pre-launch sale!
Price for you: $65!

http://consensys.academy/essentials

USE COUPON CODE BE_35_OFF_LIBRA

Interested in blockchain development?

Regular price: $295
Save 20% with our pre-launch sale!
Price for you: $236!

http://consensys.academy/ondemand

USE COUPON CODE BDP_20_OFF_LIBRA

CONSENSYS

The Libra consortium is only as decentralized as the number of validator nodes in the network, which today is made up of 29 of some of the world's largest enterprises and financial institutions, which only seems to further centralize power."