omisego

# OmiseGO Official Guide

# Contents



(Please note, this Guide is a work in progress. OMG is still in development, and some details cannot yet be included. The Guide will be revised regularly to include updates and additional details.)

# What is OmiseGO?

OmiseGO is a subsidiary of Omise, a leading online payment gateway service provider operating in Southeast Asia. The OmiseGO blockchain team has been involved in the Ethereum community from its very beginning—starting in 2015, Omise Blockchain Lab began research work focusing primarily on scalability. By the end of 2016, research had expanded into proof-of-stake (PoS) consensus design and in 2017, OmiseGO was created to achieve two goals:

1. Create the OMG Money Gateway as a scaling solution for Ethereum focused on enabling payments, trades, and other financial transactions in both crypto and fiat. OMG is a fully public, currency agnostic decentralized exchange (DEX) network which will be secured by Ethereum and built to scale infinitely using the Plasma architecture. The OMG Network will be able to interact with Bitcoin (or Bitcoin-like blockchains) and other blockchain platforms through clearinghouses in state channels or smart contracts, as well as with digital fiat platforms and economies through collateralized fiat tokens. This, in combination with virtually unlimited scalability, will enable the OMG Network to serve essentially all global transactions simultaneously.

2. Develop the OMG open-source, white label digital wallet Software Development Kit (SDK). The SDK will be free for anyone to use and will make it easy for those who need online asset exchange as part of their business to connect seamlessly to the OMG Network. The SDK allows wallet providers the flexibility to enhance, add, and customize payment solutions for many use cases.

OMG is the answer to a fundamental coordination problem amongst payment processors, gateways and financial institutions. By enabling decentralized exchange at high volume and low cost, OMG provides a next-generation value transfer service operating across currencies and asset types, and across national borders and corporate ledgers.

Through the OMG network, anyone will be able to conduct real-time, peer-to-peer financial transactions, including but not limited to payments, remittances, payroll deposit, B2B commerce, supply-chain finance, loyalty program activity, asset management, and other on-demand services in a completely decentralized and inexpensive way, and including highly performant and fully decentralized trading.

OMG offers mainstream end-customers an introduction to the many benefits of blockchain technology—the wallet SDK will make it easy to create dapps that let the end user take advantage of Ethereum's immense potential without having to leave their comfort zone.

Omise will use the OMG network as the platform for their own payments processing needs, but **neither Omise nor OmiseGO will own or control the network.**

## Why do we need OMG?

Ultimately, blockchain solves one problem—*the* problem: **coordination**.

The central paradox of human society is that we need to conduct transactions on a mass scale to accomplish our ends, but are simultaneously unwilling to trust anyone outside our immediate circle.

Throughout history, societies have tried to circumvent this problem by constructing various ever-more-elaborate mechanisms, all of which still rely on trust at some level: governments, banks, clearinghouses, arbitrators and the legal system are all institutions that we have little choice but to trust with our money, our identities, our histories and our futures. There is no guarantee that they will be competent enough to secure those things adequately; no guarantee that they will act honestly or responsibly; no guarantee that the rules of the game will not change without warning; and taken to the extreme, no guarantee that these institutions will continue to exist at all.

Applying this to the current financial system, assets such as currencies are locked up in a messy web of indirect ownership and delayed settlement. Transferring assets from one party to another often requires point-to-point interaction between multiple intermediaries, and reconciliation of duplicated ledgers held by multiple parties. Even between these parties there is a lack of trust, leading to a proliferation of convoluted systems designed to protect financial institutions from each other and themselves—and paid for by the consumer.

Blockchains allow us to create a single shared ledger, or an interoperable network of provably coordinated ledgers, on which ownership and status of an asset can be immutably recorded. We aim to create such a ledger on a global scale, by constructing a lightweight and highly scalable and secure blockchain which directly integrates with the Ethereum blockchain and Ethereum smart contracts.

## Why did a for-profit company choose to invest in building a public network that they will not own?

Logically Omise, as a payments provider trying to keep ahead of the market, needs to support *any* popular digital wallet platform that may emerge. Omise's customers must be confident that their end-customers' needs are met, no matter what payment method they have chosen.

Omise recognizes the need for infrastructure that nobody owns. While ostensibly, Omise *could* develop a centralized infrastructure for digital wallet interchange similar to existing card processors and clearinghouses, there is difficulty reaching sufficient stakeholder agreement for switching to a system around a single company.

Similar to open source software, there is significantly more incentive alignment around developing an open, decentralized system whereby participants can have assurance that they are not obligated to trust a single vendor. Our research projects as Omise Blockchain Lab, which ran from 2015 to 2017, indicate strongly that this path will bring greater adoption to this platform.

## How was OmiseGO Launched?

We had planned a token sale to raise funds through the sale of OMG tokens. However, a token presale offered to the earliest OmiseGO community (with no preferential pricing for anybody) received such high interest that the goal amount of $25 million was raised just through that - without having to run an on-chain sale (even though far more would have been raised if we had chosen to do so.)

We wanted as many people as possible to be able to participate, without taking more money than we thought we needed. We thought we needed $25 million to create and launch the network, and we felt that taking more than that would be irresponsible. We wanted people to buy in because they believed in the long-term vision, so we intentionally did no marketing or promotion, including not offering discounts to incentivize people to buy more tokens.

**OMG token: allocation**

Total supply created = 140,245,398.245132780789239631
https://etherscan.io/token/OmiseGO

During the crowdsale period (“OMG token creation period”), up to a total of USD $25 million (Maximal Launch Quantity) equivalent of OMG were to be created by the smart contract, all equal value and functionality, but divided by the smart contract into different pools, for both public and private distribution:

Public:

I. Sale [65.1% of OMG issued]

II. Airdrop [5% of OMG issued]
5% of the total amount of OMG tokens created were designated for an Airdrop, both to encourage wider adoption of decentralized network operation and as a thank you to the Ethereum community to raise awareness and keep community incentives aligned. In September 2017, these OMG tokens were automatically distributed to addresses which held more than 0.1 ETH as of block 3988888 on 7th July. Over 450,000 addresses received OMG tokens (approximately 0.075 OMG per 1 ETH). **There are no more airdrops planned (do not believe scams that advertise a future OMG airdrop and require the recipient to take action).**

Private:

III. OmiseGO reserve [20% of OMG issued]
Directly released by the smart contract to OmiseGO for future costs and uses including use for network validation as part of the development and execution of the project. These OMG are locked through a smart contract function and may not be transacted by OmiseGO for a period of 1 year, starting from the end of the creation period.

IV. Team [9.9% of OMG issued]
Reserved for team members and key contributors who worked to develop the ideas, supporting structures, and actual implementations of the OMG Project. Locked for 1 year.

## OMG basics

OMG consists of several layers:

1. **White-label Wallet Software Development Kit (SDK)**
The SDK provides standardized features to so-called digital wallet service providers. We will add more and more to this top layer as a "standard base" for others to build applications upon. While we must start somewhere, it is our ultimate goal to simplify the creation of new digital wallets to the point where they require little to no developer support.

2. **Decentralized Exchange (DEX)**
The DEX is a scalable and secure Proof-of-Stake blockchain on which any form of digital asset can be traded. All transaction orders will be managed on the DEX chain and validated by OMG stakers (as part of the Proof-of-Stake, or PoS, consensus), who collectively and dynamically determine the fees that are necessary to keep the network running, similar to how Ethereum or Bitcoin miners currently determine this (but without the energy waste and other objections to Proof-of-Work mining). The exchange will also be able to provide interoperability for all Ethereum tokens and for any Bitcoin (or Bitcoin-like) blockchain for fully on-chain cross-chain exchange.

3. **Scalability Network Mechanism**
Above all else, OMG is a scaling solution for Ethereum finance. OMG was designed for the Plasma architecture, which structures blockchain computation into MapReduce functions and uses a combination of proof-of-stake token bonding, fraud proofs to reduce the costs of computation, a withdrawal design to efficiently counter network attacks, and the network security provided by Ethereum as the root chain to safely enable unprecedented transaction and on-chain exchange processing speed and scale.

4. **Decentralized Cash In/Out Layer**
The OmiseGO digital wallet SDK allows integration with debit and credit cards for top-up and cash-out options, via ATMs or over-the counter. Our goal with cash in and

cash out touch points is to create a network of banking, hardware, and retail partners where users can deposit and withdraw their cash. The cash becomes tokenized on to their wallet application of choice, and is immediately exchangeable for other tokenized currencies and assets via the OmiseGO blockchain.

## Key Concepts

**Decentralized Network**

In a decentralized network, data is not stored or administrated by a private server. Instead, the blockchain is redundantly stored and monitored by many nodes, distributed amongst a web of individual machines with different owners that perform continuous consensus on the validity of changes to its state. If this sounds like you're being asked to trust a bunch of strangers to behave honestly, it's actually quite the opposite: there are mechanisms in place to reward nodes which align themselves with network consensus, and penalize those which do not. (See the Proof of Stake section for more on OMG's specific enforcement mechanisms)

Centralized networks require trust in a central party, which will maybe - even probably - act responsibly. However, centralized systems are necessarily opaque and gated, and centralized databases are vulnerable to attack because they present a single point of entry for bad actors looking to steal or manipulate that data. In contrast, decentralized networks are transparent in that every state and every state change (i.e. every balance and every transaction) is stored on a shared ledger which can be viewed by anyone, or are obscured in a way that makes voluntary provable traceability possible where necessary, so there is no need to trust the word of a central authority.

**Proof of Stake (PoS)**

Unlike Proof of Work (PoW), in which a miner or validator has to expend an enormous amount of computing power in order to mine a block, Proof of Stake (PoS) requires a validator to "stake" their tokens in order to validate: essentially, put their tokens in a security deposit. If they validate actively and honestly they are rewarded; if they behave dishonestly they lose tokens. Both systems are designed to make faulty behavior cost more than it's worth:

The brute computational strength needed to mine a block in a PoW system represents both a substantial investment in hardware and a great deal of energy consumed. The first miner to demonstrate correct PoW on a mined block receives a block reward as well as transaction fees associated with that block. That investment is a sunk cost regardless of the outcome; miners who misbehave (e.g. submitting incorrect proofs) will expend resources and see no returns, while honest ones have a chance of collecting block rewards that make them their money back and then some.

In PoS, we skip all the hardware and burned energy. Validators just put their investment (in the form of tokens) directly into the system, get rewarded in the form of transaction fees for non-faulty behavior and are penalized by the protocol for faulty behavior. That penalty can take the form of either hard slashing (loss of all staked tokens) or soft slashing (loss of returns). OMG will use soft slashing in its initial Honte implementation.

Returns are distributed in proportion to the number of tokens staked. However, PoS still represents a more equitable system in that returns are directly proportional to your stake. In PoW, the more computing power you have, the cheaper it is to add more - and since computing power is what earns you mining rewards, this leads to people with lots of money collecting disproportionately larger returns. In PoS, a dollar is a dollar no matter how many of them you have.

**OMG token function**

The OMG token is first and foremost a staking token. By holding OMG tokens, users gain the right to take an active role by running validator nodes on OMG's Proof of Stake network, using their tokens as a security deposit. Returns may be paid out in any currency, including but not limited to OMG. Read more on staking OMG here and here.

OMG will be a conduit for bringing value to Ethereum mainnet, because the value of OMG will be backed by the value of the amounts transacted on the OMG network; both external, real-world money, and crypto-money that is being pushed through the network's decentralized exchange (including the other applications, businesses, and token projects that are outsourcing their DEX requirements to it).

As the OMG platform and underlying network develops and evolves over time, so does the nature and role of the OMG token.

**Scalability with Plasma**

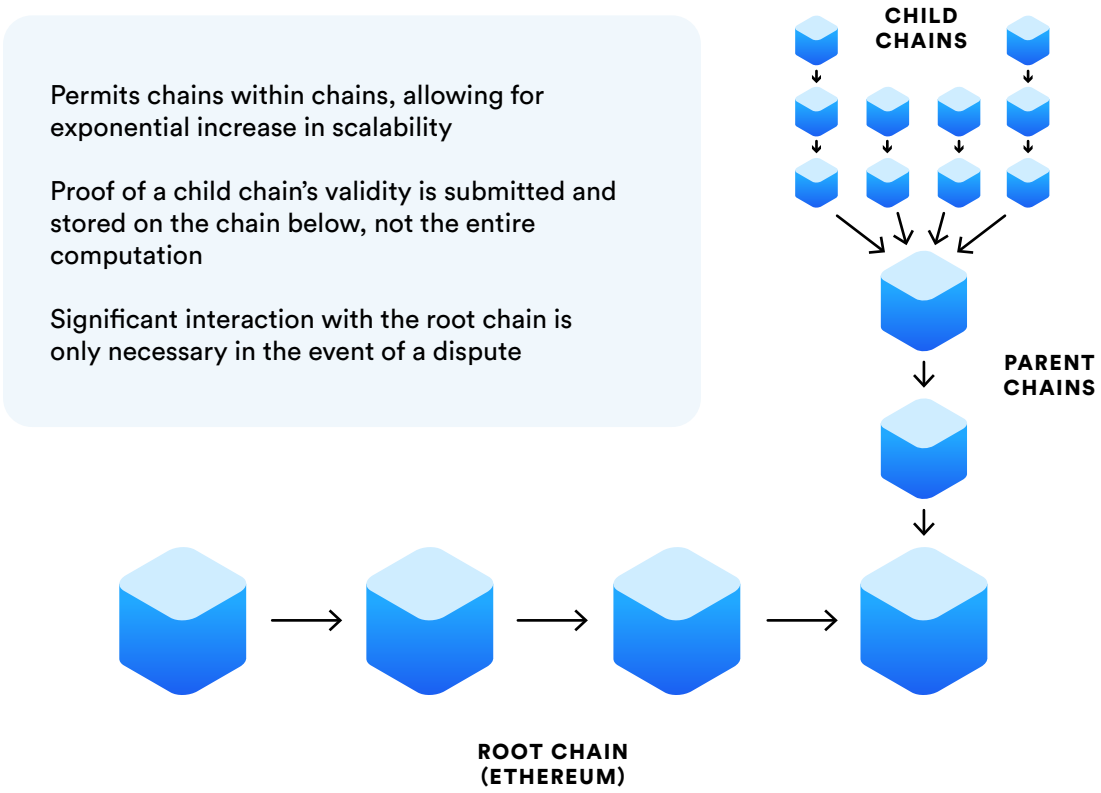
Plasma is a framework for scalable decentralized applications, conceived by Lightning Network creator Joseph Poon and Ethereum creator Vitalik Buterin. We will provide a brief overview here; the full whitepaper can be found at http://plasma.io/.

OMG is being built as a scaling solution for decentralized finance on Ethereum, using the Plasma architecture. Plasma structures blockchain computation into MapReduce functions and uses a combination of proof-of-stake token bonding, fraud proofs to reduce the costs of computation, a withdrawal design to efficiently counter network attacks, and the network security provided by Ethereum as the root chain to safely enable unprecedented transaction and on-chain exchange processing speed and scale.

This is achieved by allowing many "child chains" to run on top of the main blockchain, each interacting with the root chain with its own customized set of smart contracts. Computation

happens primarily within these child chains, and only state proofs (tiny data packets, essentially snapshots of the balances within the child chain) are committed to and enforced by the root chain. This means that transactions can be processed instantly off-chain, but are ultimately stored on and enforced by the Ethereum root chain.

## Plasma: The Basics




As an ultimate safeguard, Plasma also employs an exit mechanism which allows account holders who identify suspicious behavior within a child chain to withdraw to the root chain, reverting all accounts on the child chain to the last root chain-finalized state.

We have a team actively working on building a release-ready Minimum Viable Plasma implementation. You can read more about our progress on the MVP here.

### Hazards of Centralization

On a global scale, centralization in monetary systems create and perpetuate inequality: a tiny minority of people act as gatekeepers to the vast majority of the world's wealth. Wealth buys power, power begets wealth, and resources are siphoned into a black hole from which they rarely return: the richest 1% of people own more wealth than the rest of the planet combined and this disparity is only increasing.

Our current financial institutions don't just enable this hoarding of wealth (whether intentionally or inadvertently), they also control the channels by which ordinary people can hold and move money, and impose regressive fee structures which make it very expensive to be poor. Many banks now impose fees on accounts that do not maintain a high enough balance - literally charging customers for not having enough money.

Even for the consumer who can maintain a healthy account balance, avoid crushing debt and manage to establish a comfortable financial position, privatized systems are motivated by profit first before customers' needs. They charge a lot to use, are kind of unpleasant, and are resistant to improvements that don't first improve conditions for owners. No 'interoperability' between networks means customers must juggle many accounts, wallets and payment systems, often paying high fees to transfer money or assets between networks.

On OMG's decentralized network, transaction fees will directly reflect the actual cost of validation, not the whims of a third party. Fees serve as an incentive to validators to enforce consensus across the network, rather than funneling to a central self-enriching authority. The cost of using the network is no more or less than the cost of maintaining it.

The OMG network is also optimized for interoperability: providers can allow their customers to send and receive payments not only inside their own channels, but also cross-channel. The OMG network allows for seamless interchange between wallets, while the OMG blockchain keeps a universal ledger of every wallet's current balance.

As long as everyday users have no other option, financial institutions have no incentive to change (and to be fair, these institutions haven't really had a better alternative either). With blockchain technology, we can now do better. Existing institutions that adopt this technology will be able to serve their users better, decrease fraud risk and improve efficiency. Institutions that do not may find themselves out-competed by the adopters.

OMG will use centralized mechanisms only ever as a transitional stage, with an understanding that decentralized mechanisms will replace them, along with the open-source culture of a public development progress. **At no time will Omise or OmiseGO charge rent on the network or impose mandatory fees on network users other than those earned in the same way as anyone else - as validators on the network.**

**Unbanking the Banked**

Billions of people across the world are unbanked, meaning they don't have access to traditional banking infrastructure such as cards, loans, etc and primarily use fiat cash for everything from getting paid to buying groceries.

Much of the discussion has been around "banking the unbanked", bringing the unbanked into traditional financial systems via mobile finance tools. We think the truly exciting opportunities digitized finance opens up are quite the opposite. It opens up the possibility of a decentralized

financial system where being “banked” is not a requirement for world citizenship and financial freedom is not a privilege of the wealthy but a basic right available to anyone.

We are building infrastructure that will provide unprecedented financial access and sovereignty to people that is unmatched by banks today. The design permits user custody of funds, which decentralizes some of the functionality of banks, but not all, while simultaneously increasing usability. Banks still have roles to play, and many of them are interested in using the OMG network for their asset exchange needs. We hope to also help them increase the quality of the services they can provide to people who are their voluntary customers.

## Who will use the network?

There are many reasons why companies may wish to use OMG:

- To move money quickly, both domestically and internationally
- To gain a secure ledger for tracking assets across divisions of a large organization
- To adopt next-generation mobile banking solutions
- To enable central bank currencies to be issued digitally and improve the payments system within a given country
- To allow payments and remittances in any type of asset
- To create a loyalty points system for consortiums of brands
- To issue digital gift cards onto a network which can support multiple wallet vendors

We are working to create infrastructure that will be useful to anyone in the fintech space, with much more than Omise’s own needs in mind. We believe that this framework not only provides much-needed leadership in the fintech space, but also provides a framework for emerging business models around diverse stakeholder systems.

These mobile applications, which hold digital representations of fiat currencies and other digital assets (e.g. loyalty, game points, travel rewards), are seeing widespread adoption, but face significant barriers around coordination. By building a staking token and blockchain backed by the open Ethereum network - the most flexible, proven blockchain technology available - we are doing our part to resolve these coordination problems.

OMG’s core software will be made available for free, including the white-label digital wallet SDK, which means these businesses will be able to take advantage of everything the OMG network offers without permission from OmiseGO or anyone else. It’s a level playing field created for the benefit of users, not for the dominance of service providers.

We are confident that many businesses will see the benefit to their bottom line of increased interoperability and currency-agnostic asset transfer. We have already heard from many established and aspiring businesses who are interested in leveraging the network.

## What will OmiseGO do with themselves once the network is built?

Although Omise will use the network for their payments needs, neither Omise nor OmiseGO will own or control the network once it is deployed. It will be 100% public, owned by everyone.

Our long-term profit model will be a combination of validator fees through owning and staking some tokens ourselves, and the aforementioned anticipated growth of our payments business with network effects of the interchange network creating the long-term value. We may also provide consultancy services to companies to implement OMG blockchain services (not to be confused with charging fees to access the network, which is unilaterally not a thing).

## How does OMG provide for...

**Security?**

Centralized databases are highly susceptible to attack. Over and over again we have seen massive stores of sensitive data hacked, stolen, leaked and tampered with. It only takes one careless person to compromise the whole system. The owners of those databases get a slap on the wrist; the users whose data was leaked spend the rest of their lives in fear of having their money or identity stolen.

By employing asymmetric encryption via public and private keys, blockchains make it possible to conduct secure transactions without having to collect and store personal data in centralized databases. This is good for both the service provider and the user: private keys are more difficult to steal than physical cards, cannot be forged like an ID or written signature, and cannot be stolen en masse like account numbers or passwords since they are not stored in any database. So users don't get their identities stolen due to lax security systems, and service providers don't find themselves liable for fraudulent transactions.

**Scalability?**

OMG solves the security vs. performance (on-chain vs. off-chain) dilemma by performing all orderbook and execution functions on-chain, on a specialized chain. The Plasma architecture allows for transactions to occur in real time, while state proofs are committed to and enforced by the root chain, so the OMG network can scale infinitely while still being secured by the Ethereum root chain.

Currently Ethereum is processing about 15 transactions per second, but we are building the OMG network to be able to handle all the world's transactions simultaneously.

**Mainstream adoption?**

Today, decentralized finance and cryptocurrencies are still quite foreign to the mainstream. Taking advantage of the many opportunities Ethereum can offer still requires a fair amount of technical knowledge, well beyond the scope of the average consumer. OMG's white-label SDK is designed to be simple and friendly, allowing business users to create customer-facing wallet apps that utilize the OMG network without requiring a deep understanding of the underlying technology.

By creating the SDK, we are doing the legwork that will allow business users to plug into the network easily and build wallets that take advantage of Ethereum's vast potential without compelling any behavioral change on the part of the end customer. Providers can customize wallets, building in whatever functions they need and incorporating their own branding.

Users will be able to experience the freedom to transfer money in and out of whatever currencies they wish, including decentralized currencies such as ETH and BTC. The OMG network is intrinsically agnostic between fiat and decentralized money: as far as adoption and use go, the system is constructed so that the best currencies will win.

End-customers will not necessarily know that their service is powered by OMG, they will simply know that it works and that they get benefits passed down in terms of reduced costs, real-time transactions, and increased access and flexibility.

## Community & Communication

From the very beginning the community response to OMG has been incredible. We are grateful for your support, and optimistic that the enthusiasm around the project bodes well for the future of decentralized networks. Big thanks to token holders and stakers, who are the key to the network's function, security and growth; individuals and teams who have contributed to OMG; to the businesses who are eager to become early adopters; and to members of our various online communities who continuously challenge and encourage us.

Follow us on Twitter (omise_go) and Medium to keep up-to-date. Join us on Reddit and Rocket to ask community questions, chat and discuss.

## FAQ

We have provided answers here for the most common questions we receive via email; we can't personally respond to each and every request for basic information so please read before emailing with questions.