Overledger Network for Community

June 2020

QUANT

This paper aims to outline how Quant Overledger OS and Overledger Network can benefit the developer community.

Contributors:
Dr Luke Riley
Martin Hargreaves
Peter Marirosans
Gilbert Verdian

Quant Network is a technology provider, delivering enterprise-grade interoperability for the secure exchange of information and digital assets across any network, platform or protocol, at scale. Quant's Overledger, the world's first DLT operating system, complements and connects existing systems and DLTs, to drive innovative and efficient growth for companies, public entities, and regulatory bodies alike. Headquartered in London, UK, Quant is recognised as a Gartner Cool Vendor 2019 and is committed to unleashing the power of systems that are as connected as the world we live in.

For more information: www.quant.network

30th June 2020 - Version 1.0

Contents

Introduction

Quant Network is a pioneering technology company combining cybersecurity, industry and government experience to develop advanced technologies that automate trust. Overledger is the world's first blockchain operating system connecting the world's blockchains and networks.

Our vision is to build an ecosystem around Overledger, allowing for developers and Enterprise to innovate, create value and build game-changing multi-chain applications for users and their customers.

Overledger: An operating system for interconnected DLTs

Digital Ledger Technology (DLT) is emerging in many areas as an innovation which is well suited to solving specific problems in compliance and regulation, provenance of goods, trade networks, Internet of Things, commodity trading, energy, healthcare and many others areas. It is a better solution for certain classes of problems rather than being aligned to any particular market, and it's adoption is growing in almost all industry sectors.

Quant Overledger is an Enterprise Distributed Ledger Technology (DLT) operating system, that connects to many DLT and other Application Programming Interface (API) based systems. It exposes their combined functionality through a single API and allows coordinated transactions and business processes to happen across all the connected DLTs and API based systems.

Our vision is for the Overledger ecosystem to connect to all the DLTs, globally, that organisations need to do business, and present them in a single API, with a vibrant marketplace of applications and with the simplicity and ease of use of today's Internet – with the trust, privacy and security that only distributed ledger technology can provide.

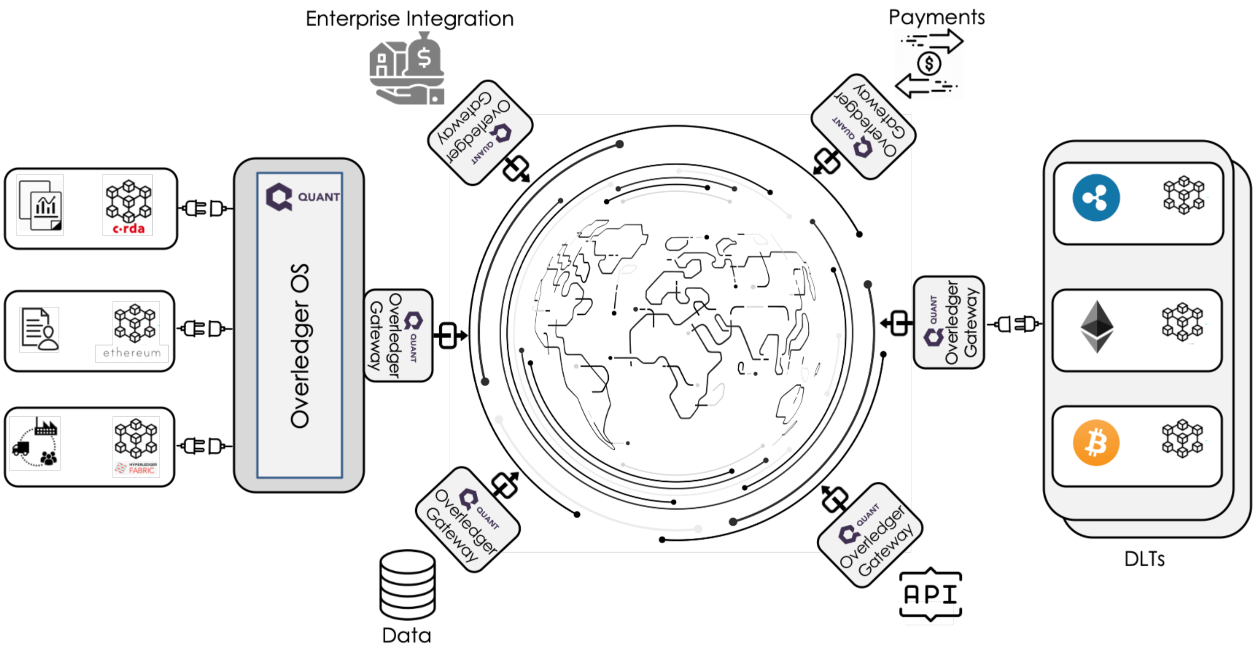

Figure 1. The Overledger Network Ecosystem

Security

Cybersecurity is our company's DNA. Our team have a rich heritage of working for Governments, banks and industry for over 20 years protecting organisations and people from security threats.

The pillars of security are Confidentiality, Integrity and Availability. As such, we have used our experience in running payment and financial infrastructure and critical national infrastructure for nations and embedded these principles into every aspect of Overledger.

To enforce confidentiality and integrity, QNT are used to validate with the option to **sign and encrypt** every transaction that flows through Overledger. Every enterprise client, developer, user and application (mApp) validates each transaction using their QNT linked to their mAppID and bpiKey.

- No transactions can flow through Overledger without being securely validated by QNT.
- No 3rd party can view or tamper with transactions and their contents, including Quant when signed and encrypted.

Developers

License fees

- Developers will be able to obtain an annual license to develop applications on Overledger through the purchase of QNT tokens equivalent to a fixed FIAT amount.
- The developer wallet will in turn be authorised to access the platform for the length of the license period (i.e. annual), as well as develop, sign and publish applications.
- Users can also hold a subscription license tied to their wallet and QNT for a period of time to access features of Overledger.
- The license/key will expire annually and thus must be renewed using only QNT.
- QNT are locked for the entire duration of their license and are out of circulation.
- If licenses are renewed at expiry, the QNT will continue to be locked for the new period of time and remain out of circulation. If the license is not renewed at expiry, the QNT is put back into circulation through the Treasury at market prices for other client use.

Consumption fees

- Payments for read and write to Overledger will also need to be made in QNT based on a FIAT value, for example if the monthly read and writes equate to $10/month, the equivalent will be paid to the Quant Treasury using QNT, however the price will be variable and adjusted to market supply and demand.

Add-on services

- Additional features and services can also be consumed as middleware. These features will be released with updates to Overledger as part of the roadmap.

Monetisation

- Developers may choose to monetise their applications and will have the options to use a payment processor to charge a subscription, a recurring price, a one-off price, or an in-app fee. This can be charged in FIAT or digital currencies.
- We are working on the monetisation options to incorporate into the Treasury, alternatively developers will be able to use their own providers.

Developer Accounts

All existing account from the old developer portal from 2018 have been migrated to the new Developer Portal. All accounts will be able to get API keys to start using immediately on Testnet and will receive a 500QNT allocation of Testnet QNT. For Mainnet connectivity, all accounts need upgrade by completing KYC checks in compliance to the appropriate AML policy. This process will be automated for the next release. If you require Mainnet before then, please log a support ticket with support@quant.network.

Enterprise

License fees

- Enterprises will be able to obtain an annual license to develop applications on Overledger. Enterprise license fees will be determined on the basis of:
  - number of users
  - number of employees
  - types and number of applications (internal, external, native applications or web-based etc)
  - volume of Overledger transactions

Platform fees

- In addition to the license fee and developer license approach, a platform fee calculated as a percentage of the license fee in QNT will be payable. However, QNT will be obtained and managed through the Treasury by Quant Network on behalf of the client at a given day's rate. The Treasury - Enterprise has been live with clients since April 2019.

Consumptions fees

- Similarly, payments for read and write to Overledger will also need to be made in QNT based on a FIAT value. For example, if the read and writes equate to $10/month, the equivalent in QNT will be paid, however, the conversion to QNT will be handled by the Treasury.
- As Enterprises will have larger volumes of usage, we will be introducing payment options for:
  - pay-as-you-go
  - pay in arrears
  - pay in advance (pre-pay)
  - unlimited usage
  - number of users

Add-on services

- We are releasing enterprise add-on services which provide additional features and services which can also be consumed as middleware. These will be released with updates to Overledger for Enterprise to utilise.

Overledger Gateways

To foster the wider ecosystem, we are expanding Overledger gateways to access multiple permissioned and permissionless blockchain networks, API sources, Data Sources and existing network interconnectivity.

Overledger gateways part of our strategy to optimise network latency providing enterprises, developers and users choice to access new data sources, markets and transactions. Gateways are hosted by anyone wishing to participate in the network. Partners and also Enterprises will host their own gateways within their corporate networks will be stakeholders of the Overledger Network.

Community Gateways

To help encourage the expansion of the Overledger Network, we are providing users the opportunity to host their own public Overledger gateways to drive volume and applications to multiple permissionless blockchains.

By hosting a gateway, stakeholders can earn a percentage of transactions that pass through their gateway. Stakeholders have the option to host different tiered gateways, composing of:

- Tier 1: Overledger gateway with connectivity to 3 or more blockchain nodes
- Tier 2: Overledger gateway with connectivity to a single blockchain node
- Tier 3: Overledger gateway with no blockchain nodes

The Overledger gateways will create a scalable p2p network that shares the transaction and volume between participants and choses the closest or largest node to transact with. Gateways that also host connectivity to blockchain nodes, will attract more transactions and volume as the local destination node is prioritised.

Initially, we're undergoing stress testing of the network and will be providing all gateway participants 500 Testnet QNT to run payment channels, send transactions, test the treasury and all the functionality of the network.

Upon completing the initial stress test, the full payment channels and flows will be opened up to the network for all participants.

Enterprise Hosted Gateways

The Overledger Network is also available to Enterprise clients who wish to host their own dedicated gateway to access the underlying blockchains.

The benefit to enterprise stakeholders is the ability to own and control a node hosted within the corporate perimeter and comply with technical and security governance and requirements. Overledger gateways allow for enterprise to interconnect internal permissioned blockchains such as Corda or Hyperledger Fabric with public permissionless blockchains such as Ethereum safely through your own enterprise gateway.

OVN: Gateway Operator Guide

Overledger Gateways allow participants to host Overledger Gateways on their own infrastructure.

Enterprise clients, can also host their own Overledger Gateway in conjunction with their Overledger OS instance to securely access the OVN and to bridge other internal permissioned DLT networks, access public permissionless networks or consume data sources that are available to participants through the OVN.

Detailed instructions: https://github.com/quantnetwork/overledger-network-gateway

How do you host an Overledger Gateway?

Overledger Gateways are downloadable from www.github.com/quantnetwork

You need to register as a gateway operator on https://developer.quant.network or https://quant.dev from June 30 to provide your ERC20 wallet and details to obtain your licence keys.

What is the Treasury and how does it work?

The community treasury's role is to handle QNT payments flowing from multi-chain applications (and their users) to Overledger and Overledger Network Gateways. The treasury organises these payments through layer 2 uni-directional payment channels.

Layer 2 payment channels, move the vast majority of payment transactions off the underlying blockchain, and uses the blockchain only to open channels, claim accumulated payments from a channel, resolve a dispute in a channel and close a channel. Processing payments using payment channels significantly cuts down on transaction fees and dramatically increases processing speed, while keeping intact the trustless nature of blockchain technology.

The treasury is organised into three sections: (1) smart contracts deployed on the Ethereum blockchain; (2) an off-chain web app; and (3) communication connections into the Overledger Network. Further to the payment channel smart contracts mentioned previously, additional smart contracts are used to encode the treasury's operational rules and to disincentivise faulty behaviour from any user or gateway.

All of the treasury smart contracts can be viewed in the Github project: https://github.com/quantnetwork/overledger-treasury-community/tree/master/Code/SmartContracts

To learn more about the treasury and how to interact with it, see: https://github.com/quantnetwork/overledger-treasury-community

How do licences and payments work

For a user or multi-chain app (MAPP) owner to join the Overledger Network, they will have to pay a licence fee locked in a payment channel for 12 months, as well as fund a payment channel from themselves to the treasury. The funds in the payment channel will remain locked for a set period of time, after which any remaining amount can be reclaimed by the user.

Whenever a user wants to request a function of the Overledger Network, a message will be sent to the network that includes the function information as well as the related payment. This payment will only be added to the channel by the treasury if a gateway processes the function before the designated timeout.

For a gateway to join the Overledger Network, gateway owners will the licence fee. On top of this licence fee, gateway owners will be able to lock up (stake) an increasing amount of QNT for a set period of time. The higher the fee locked up, the more priority this gateway will get on the network, in terms of function requests received. A gateway will earn a fee for every function request correctly processed before the response timeout limit. These fees will accumulate in a treasury to gateway payment channel, the total of which can be claimed whenever required.

Under normal conditions, a gateway's locked up fee will be returned to the gateway in full at the end of the lockup time period. Only if the gateway deviates from the Overledger Network communication protocol will some of the locked up fee not be returned – this will not occur, should the gateway operator run the gateway software provided by Quant Network.

Steps to use the test version of Overledger Network Payment Channels:

For the steps required to interact with the Overledger Network Treasury, see the following link: https://github.com/quantnetwork/overledger-treasury-community/blob/master/Code/README.md#interaction-steps

What can you do on the OVN?

The OVN is creating enabling an ecosystem of cross-chain transactions for participants, gateway operators and developers to create and transact value using digital assets.

Open Source Connector (OSC)

Working with many distributed ledgers can be a complicated task that puts an educational burden on a developer to understand specific details of many different technological implementations. Quant Network is continually working to make this process easier through the integration of standards both at the SDK and connector level.

Quant Network are a leader in distributed ledger technology standardisation. CEO Gilbert Verdian founded the Blockchain ISO Standard TC307 and now chairs the UK Standardisation Delegation for it . This dedication to standards is a foundational philosophy of Quant Network and work on these standards is a core driving point of innovation of our open source connector concept.

Now that the Overledger Network has launched, developers can start to provide their own connectors into distributed ledgers not currently provided by Quant Network.

To do so, developers will be working to strict connector interface definitions, which will be versioned and can iterate over time according to community feedback. Choosing what specific connector interface definition to use for a new distributed ledger will depend on its underlying properties. For instance, does the distributed ledger:

- have blocks?;
- organise its current state via the unspent transaction output model or the accounts based model?;
- allow smart contracts to be written in a Turing complete language?;
- and so on.

By following a strict interface standard, firstly the SDK will be easily interoperable with these new connectors, and will do so without adding further educational burden onto the SDK users. Secondly output can be compared for consistency between different Overledger gateways connecting to the same source, which will increase the reliability of the network as a whole.

Note that the advantage of open source connectors does not have to be limited to connecting only to new distributed ledgers. This model can be reused to connect to distributed databases, big data providers and any type of service a gateway wants to provide.

In conclusion, the integration of open source connectors to the Overledger Network will provide organic ecosystem growth. The increased variety of data sources and services will lead to more complex multiple chain apps being developed, which should in turn drive further connectors to be developed.

Multi-chain Smart Contracts – Treaty Contracts

As Overledger connects to multiple DLTs, it allows developers to start building *multi-chain applications* (MAPPs). Each MAPP contains one or multiple Treaty Contracts.

A Treaty Contract details the rules of interaction between the multiple DLTs, i.e. it contains the multi-distributed ledger logic. Treaty Contracts can be written in any language, instantiated and shared between multiple participants and run in one location or many locations at the same time.

If a Treaty Contract is run in a single location, we have no problem with data consistency and availability, as everything required is in that single location.

Alternatively, we many want to run a Treaty Contract in multiple locations (for reasons such as its users do not want to rely on a single instance of a Treaty Contract). In this case, there may be *n instances* of a single Treaty Contract.

To keep multiple instances of a single Treaty Contract in sync, the Treaty Contract code has to be *stateless.* Therefore ,all state variables of the MAPP have to be stored either on a distributed ledger, on a distributed database where the underlying data cannot be changed (e.g. IPFS) or privately in the MAPPs database.

We say that a Treaty Contract is *trustless* if it has the properties of:

[i] *verifiable correctness*: there is a method to check that the Treaty Contract instance stakeholders are running have the same code base; and

[ii] *eventual data consistency*: all verified instances of the same Treaty Contract will eventually return the same result for any specific function call with the same input (given no further changes to the underlying state variables).

Please contact us if you want further information on how to build a trustless Treaty Contract that can be run in multiple locations.

Distributed ledger infrastructure

Applications utilising distributed ledger technology currently have 3 infrastructure choices for their node deployment and utilisation:
1) Own nodes – Where the application owner runs their own node(s)
2) Single node service provider – Where the application owner has no personal nodes, instead all application transactions are routed through a single node service provider
3) Hybrid: single backup – Where the application owner runs their own nodes but a single node service provider is used as a backup

The Overledger Network provides two additional infrastructure choices:

4) Multiple node service providers – Where the application owner has no personal nodes, instead all application transactions are routed through multiple node service providers, with the results cross checked between service providers for consistency.

5) Hybrid: multiple backups - Where the application owner runs their own nodes but multiple node service providers are used as a backup.

These two additional infrastructure choices are ground-breaking. Where distributed ledger networks provide a method to establish trust between different parties running different nodes, the Overledger Network provides a method to establish trust between distributed ledger users not running a node and parties running nodes, providing a crucial missing piece in full end-to-end trust. This end-to-end trust is established using a game theoretic approach between the multiple node service providers (gateways) on the Overledger Network and is described in the community treasury white paper.

Note that Overledger Network's gateways provide read and write capability for the chains that they are connected to. Therefore, multi-chain apps can be designed to use make use of these capabilities treaty contracts to provide oracle*, fire-and-forget** or complex cross-chain smart contract logic.

The Overledger Network can additionally be integrated into distributed ledger applications already created as a fail-safe backup, for an ever-expanding number of distributed ledgers, should the application owner's nodes be overloaded or crash.

*Oracle in terms of the blockchain use of the phase, I.e. adding data onto a blockchain from another source.
**Fire-and-forget, I.e. picking up data from one distributed ledger and moving it onto another .

Overledger Bitcoin Wallet

In combination with our Overledger Network release, we have added new examples to our Javascript SDK Github.

The main new example in this SDK update is the Bitcoin wallet, to understand why it is beneficial, we firstly have to discuss how Bitcoin organises its current state via the unspent transaction outputs (UTXOs). Note that other distributed ledgers also use the UTXO current state model, such as Bitcoin Cash, ZCash and Corda.

A Bitcoin transaction is made up of transaction inputs and transaction outputs:

- **Transaction output:** A transaction in an UTXO based distributed ledger produces a collection of outputs. Each output has a script detailing the conditions required to spend the digital asset of this output (cryptocurrency coins in the case of Bitcoin). If the output has not yet been spent, we call it: **an unspent transaction output**.
- **Transaction input:** Each input contains a link to the previously unspent transaction output that is now being spent. Each input also contains evidence to prove the conditions of the output script have been satisfied.

The UTXO current state therefore is **a list of unspent transaction outputs**.

So, for a user to create a new Bitcoin transaction, the user has to track and reference unspent transaction outputs. This is what our wallet example automates.

To start the example, a user with a Bitcoin address must add the details on all related UTXOs of this address into the Bitcoin wallet's associated csv file. Next the Bitcoin wallet will choose which UTXOs to use for every new transaction. Additionally, the Bitcoin wallet will update the csv file to remove spent UTXOs and add UTXOs when they are generated.

Note that this Bitcoin wallet can be used as a basis for a wallet of different UXTO distributed ledgers. Whereas Ethereum and Ripple do not have the same issue of having to track unspent outputs these ledgers follow the accounts-based current state model, which requires no tracking of previous transactions.

New features and possibilities of the Overledger Network.

Multi-chain Oracles

Run cross-chain oracles to serve the Overledger and wider DLT ecosystem by creating MAPPs that can operate as oracles across networks aimed for enterprise, institutional and developer oracle needs.

API Marketplace

Once the network is established, we will enable a marketplace of different directories for developers and API owners to publish connectivity to these APIs through their gateways and acting as the processes for that API.

Data Marketplace

In the same method as above, gateway operators can publish the connectivity to datasets through their gateway and sell the access and the data, processed by their gateway.

Layer 2 Scaling

As QNT resides on Ethereum, we had to analyse the different options available for Ethereum scaling. Most of these options are nicely summarised by the following article: https://medium.com/matter-labs/evaluating-ethereum-l2-scaling-solutions-a-comparison-framework-b6b2f410f955?_branch_match_id=712263612681585392

Notice that uni-directional payment channels are not covered in that article as they are not applicable to every use case, but they are a good fit for the Overledger Network design.

Before we continue the discussion, we should make the distinction between the different categories of off-chain channels. Firstly, there are payment channels (for cryptocurrency/asset transfer) and secondly state channels (for any data agreements between the parties of the channel). Uni-directional payment channels are a special type of payment channel where the sender (developer) does not need to always be online. Bi-directional payment channels on the other hand require both parties of the channel to be online most of the time.

Now we can evaluate our bespoke uni-directional payment channel design in the style of the referenced article above.

Security

- What about the Liveness Assumption?: The treasury must watch the developer to treasury payment channel in order to claim funds before the channel's timeout. The gateway does not have to watch the treasury to gateway payment channel as our unique design allows the treasury to push through payments to the gateway if required.
- What about the Mass Exit Assumption?: Developers and Gateways can withdraw their funds from the payment channel after the defined expiration period (and not before)
- Can a Quorum of Validators Freeze Funds?: This is not possible as our payment channel funds are only locked according to the expiration time
- Can a Quorum of Validators can Confiscate Funds?: This is not possible, funds can only be moved through a channel if there is a signed transaction by the sender saying that this should occur.
- Are the Payment Channels Vulnerable to Hot Wallet Exploits?: Our payment channels have been designed to minimise this issue. Users of the channels have two addresses: (1) their QNT wallet address, which can be a cold wallet where all of the user's QNT could reside; and (2) their operator address, which can perform actions on the payment channel. Now if a user's operator address private key is obtained by a hacker, the hacker can only send funds through payment channel up to the QNT amount currently locked in the channel. This significantly minimises risk as firstly the hacker can only send QNT to one destination and secondly the hacker cannot access the sender's full QNT amount (which is safely secured in the QNT wallet address).
- Are the Payment Channels Vulnerable to Crypto-Economic Attacks?: The only relevant attack here is a compromise to the Treasury software operator. This is not an issue due to the collection of smart contracts that define the rules of the treasury's operation. A deviation from these rules will result in the Treasury's QNT deposit being deducted.
- Are there un-Tested Cryptographic Primitives Used?: No, the payment channels only rely on standard cryptographic primitives native to the Ethereum Virtual Machine (EVM)

Performance/Economics

- What is the Maximum Throughput on Eth 1 and Eth 2?: Payment channels have by far the highest maximum throughput compared to the other alternatives, which was one of the key reasons for choosing this design. This occurs as the majority of transactions do not occur on the blockchain. The maximum throughput is therefore limited only by the computational specification of the machines involved.

- How Capital Efficient are the Payment Channels?: The payment channels do require a lock up of QNT in order to be used. The more QNT locked up and the longer for, the cheaper QNT transaction will be. Note that longer and bigger QNT lockups would be beneficial for the QNT market price.
- Is there an On Chain Transaction to Open an Account?: Yes. This only has to occur once, even if a user's payment channel has expired and the same user wants to reopen it (as long as the same operator address is used).
- What is the Cost of a Transaction in a Payment Channel?: This is very low. The cost will be lower, the longer the QNT is locked up for and the more transactions that are sent off chain. Note that payment channels do require less on chain transactions compared to scaling alternatives such as rollups

Usability

- What is the Withdrawal Time from a Payment Channel?: After your payment channel is expired, you can withdraw your funds immediately
- How Final are Transactions sent to a Payment Channel?: On chain transactions sent to a payment channel are immediately final once added to the blockchain (but it is recommended to wait at least 6 confirmations due to proof-of-work consensus)
- Can Light Nodes Verify Payment Channels?: Light nodes can verify any on chain interaction with a payment channel

- Will the Treasury Instantly Confirm Off Chain Payment Channel Transaction?: Yes the treasury will confirm or reject a payment channel message instantly

We’re allowing:

- Developers to build and publish multi-chain apps to run and publish on OVN. We’re starting with Testnet and Mainnet connectivity.
- OVN will have a marketplace to power the ecosystem
- Gateway Operators will be able to download and connect to the OVN, registering on the new developer portal, get licences
- Payments and payment channels will be turned on after a couple of months of initial stress testing
- We’re looking at providing each developer and/or gateway operator will receive Testnet QNT to start using the OVN from day one and help in the scaling for all participants.
- Later, gateway operators will be able to integrate DLT nodes and other data sources and other APIs to publish to the network – E.g. Data to sell, IOT, other APIs, new Blockchain connectors etc
- Developers and gateway operators can monetise what they’re offering to the rest of the network through payment channels facilitated by the Treasury

When is OVN Live?

The OVN Network launched on the 30th June 2020 on Testnet and Mainnet blockchains, initially starting with Ethereum, Bitcoin and Ripple.
The OVN Treasury has also been deployed on the Ethereum Testnet and Mainnet with the detail provided: https://github.com/quantnetwork/overledger-treasury-community/tree/master/Code

Payments

We are enabling payment channels on Mainnet at the next release, after the initial stress test of the OVN, Gateways and Treasuries.

From launch, all payment channels will be enabled on Testnet and all Gateway Operators and registered Developers will be provided 1000 Testnet QNT to start testing the functionality of gateways, payment channels and treasury.

The Testnet environment is the mirror of the production Mainnet implementation.
At the next release and update and after the stress test, all registered developers and gateway operators are required to update their account on the developer portal to receive Mainnet (production) BPI Keys by completing our onboarding and KYC

process. This is available to all developers at launch and will be enhanced and fully automated.

What is the OVN Dashboard?

The OVN dashboard will be available to all registered developers in the Developer portal. It will show a combination of network and transaction metrics across the Overledger Network and will be continuously updated.

Status updates can also be followed on @OverledgerNet on twitter.