iov42

The identity platform for building trust

High-Level Architecture

Table of contents

Building a platform

iov42 has built a platform that uses simple building blocks to create easy-to-use applications on a trusted, distributed ledger technology (DLT) architecture. We envisage a global infrastructure consisting of interconnected networks, where people, organisations and governments can interact in trusted, meaningful ways to solve hard problems by leveraging the benefits of an identity based, asset hosting digital network.

We have identified four key goals for our platform's design in order to meet these objectives:

Identity at the Core

In order to be useful across the universe of use cases, identity is key—having the right information about the participants in a transaction allows the transaction to happen.

Native Multi-Asset Support

In order to cater for all use cases, a full expressive asset type model is needed to facilitate the representation of any asset type.

Regulatory Adaptability & Governance

With regulatory constraints and the demands for governance both increasing, adaptability to shifting requirements is essential for long term viability.

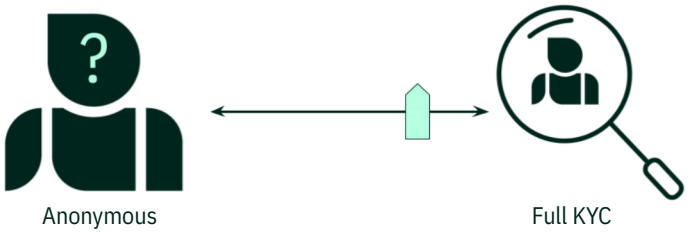
Performance & Scalability

As an infrastructure play, the network needs to support the anticipated demands.

Identity at the core

An individual's biggest asset is their identity. Your identity gives you access to products and services and it enables the establishment of ownership, amongst other things.

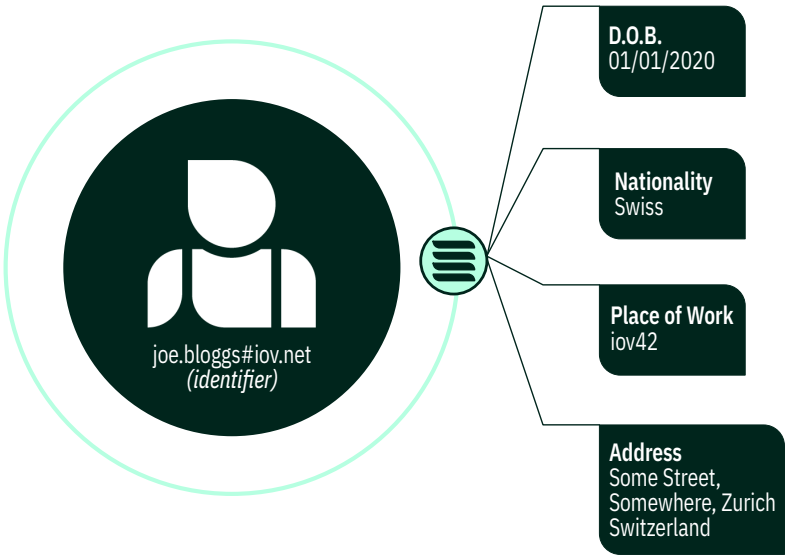
Trusting an identity is completely subjective and is based on the intended use. The requirements for establishing trust in an identity can be thought of as sitting on a sliding scale—starting at remaining anonymous all the way to completing a full KYC process:



For example, setting up a social media account often takes little more than providing an email address and password. On the other hand, if you want to set up a bank account, you will likely have to provide a government-issued I.D., some proof of residence, and some sort of taxpayer identification number, in addition to completing the paperwork from the bank.

The iov42 identity model has been designed to accommodate this flexibility. This enables an identity subject to decide which claims they wish to make about their identity, and, more importantly, which claims they would like to share with others.

This is possible by representing identity as an identifier that has associated claims, such as those listed in the image below.



What are claims?

A claim can be any piece of information that asserts some fact related to a given identity. For example, my name is Joe Bloggs. I claim that:

- I was born on the first of January, 2000;
- I am a Swiss citizen;
- I work at iov42; and
- I live in Zürich.

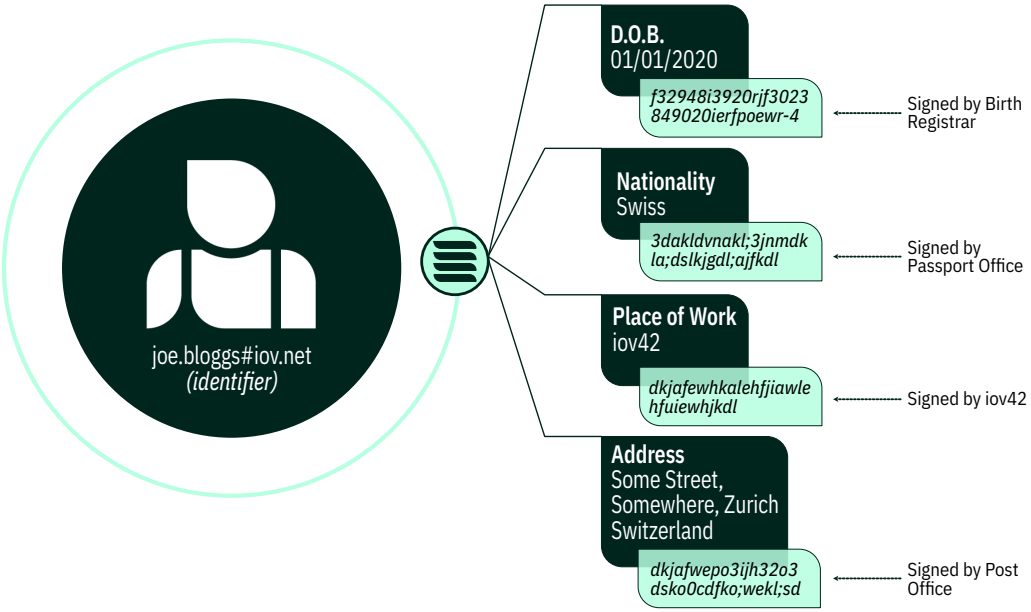
When Joe Bloggs makes a claim about his identity, this claim is stored as a hash of the claim against his identity within the iov42 network.

However, by itself, a claim is not very useful in contributing to the trust in an identity, since the identity holder could make a claim about pretty much anything. The key to building trust in any claim is to have it endorsed by third parties.

What are endorsements?

On the iov42 platform, endorsements are captured by use of cryptographic signatures. An endorsing party, independent of the identity holder, can endorse an identity's claim.

Once an endorsing party signs a claim, it is submitted to the iov42 network, where it must then be validated by the network's participants. Once validated, the claim and related endorsement are added to the identity to enable a richer expression of the identity, which can later be used to assert trust in trusted transactions.



Note: The signatures demonstrated here are purely illustrative and do not attempt to represent real cryptographic signatures

Delegated identities

The iov42 platform supports the creation of delegated identities that can perform any operation on behalf of another identity. This is a pragmatic option for many users on the platform, since delegation of responsibilities and tasks is inherent to most organizations.

For example, a claim that Joe Bloggs makes about his bachelor's degree would be sent to his college alma mater, Crypto University, which, in this case, would also have an iov42 identity. However, it would be extremely inefficient if only one active individual was processing and endorsing all claims being sent to Crypto University. Instead, the main Crypto University identity could delegate the authority to endorse or deny claims about bachelor degrees to select employees of the undergraduate records office. With this authority, the delegated identity would create the endorsement for Joe's claim on behalf of Crypto University.

The iov42 platform does not permit an already delegated identity to create a further delegated identity. This prevents situations in which the most recent delegated identity loops the chain of command back to the original delegating authority.

It is important to remember that the trust provided by an endorsement depends on the perceived trustworthiness of the endorsing party. So while a delegated identity endorsing claims on behalf of Crypto University would be considered a reliable source of verification regarding Joe's degree, the same trustworthiness would not apply to an endorsement given by Joe's college buddy.

Trusted Assets

Having created a flexible model for identity and the tools to build identity trust models, the logical next step is to apply that identity to ownership of assets. The ownership and transfer of assets is the raison d'être for blockchain networks.

The iov42 platform allows for the modeling of virtually any asset that can be represented in a digital form. Unlike some other platforms, the way in which assets are defined on the platform is not tied to any underlying network asset, such as Ether for the Ethereum network, for example.

iov42 has designed a rich asset model that allows the custom definition of asset types. Once an asset type has been defined, instances or quantities of that asset type can be created.

The iov42 platform recognizes two main asset types:

- Quantifiable
- Unique

As the name suggests, quantifiable assets can be quantified, i.e. they involve a quantity that can be owned. Each instance of a quantifiable asset is the same and there is no way to distinguish between them. An example would be fiat currencies—the money you have.

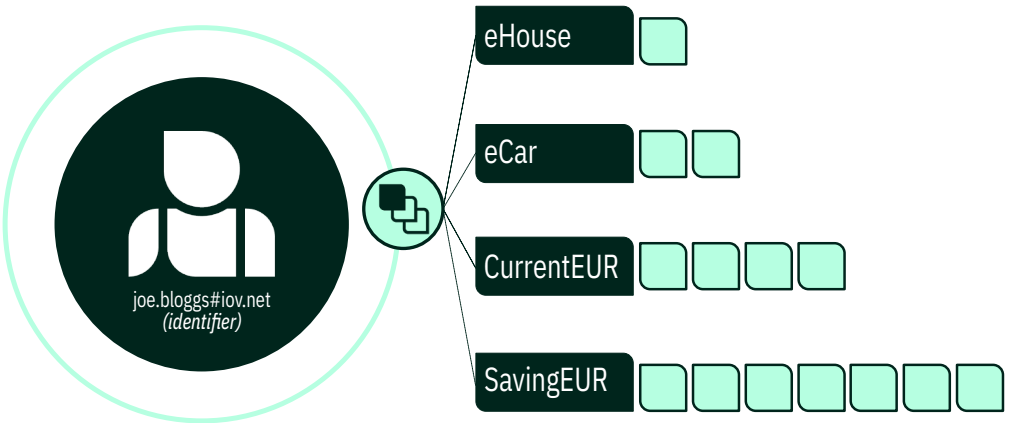
Unique assets are all unique and are not fungible. Examples of these could include a car or a house — each instance of which is different from every other instance.

In the future, the iov42 platform will recognize a third asset type category—structural assets. Structural assets are assets that have a relationship that must be maintained, most commonly a singular collective asset with individual component assets. A block of flats is a good example of a structural asset: the block itself is an asset, while each individual flat is also an asset, and the relationship between the whole and its parts is fixed.

Single identity — multiple accounts

Every asset on the iov42 platform must have an owner. It should be noted that the owner of an asset can be different to the identity that created the asset type.

An identity on the iov42 platform can own any number of different assets. Quantitative assets can be split into different accounts, similar to having multiple bank accounts of the same currency.



This approach has several benefits:

- Performance — partitioning of processing and storage by asset type and identity removes contention and bottlenecks seen on some other platforms
- Functionality — each asset type can have different functionality based on their own requirements
- Permissioning — intrinsic separation will facilitate clear permissioning models
- Adaptability — future legislation may affect certain asset types and this can be handled without affecting other asset types
- Once assets are represented digitally and their ownership clearly defined in a trusted manner, then the opportunities to transfer those assets will lead to a whole new class of digital value transfer.

Claiming and endorsing assets

Similar to identities on the iov42 platform, assets can also have claims and endorsements. However, only asset types and unique assets can have claims and endorsements. It doesn't make sense for quantitative assets to have them, because a quantity of something is neither unique nor constant. However, an asset owner can make a claim about an account that holds quantitative assets. For example, I could make a claim that my SavingEUR account is anti-money laundering (AML) compliant.

When an asset owner creates an asset type or owns a unique asset or an account, it can be endorsed by a regulatory body, which bolsters the asset's trustworthiness. Building trust in assets is particularly important when considering regulatory compliance.

Transferring assets

On the iov42 platform, asset owners can transfer and exchange the ownership of assets.

Atomic Swaps on the iov42 Platform
Across the DLT industry, an atomic swap usually refers to the exchange of cryptocurrencies across different blockchains without a centralized exchange. More generally, an atomic swap describes a peer-to-peer value exchange that is only executed once both parties transfer their agreed-upon assets.

The basic concept of an atomic swap has been built into the design of the iov42 platform so that the swap of assets are inherently atomic—either an exchange of assets happens in one instantaneous transaction, or it fails. The platform's design makes it impossible for a transaction to be half-complete or in any other stuck state. This feature is important because it eliminates the risk of one party not fulfilling their side of the transaction.

Let's say Alice and Bob are two identities on the iov42 platform and Alice has decided to transfer ownership of her car to Bob in exchange for 20,000 euros. When Alice and Bob authorize this transaction, either the transaction will be successful and the swapping of assets will happen simultaneously (atomically), or it will be denied and the transaction will not proceed.

The iov42 platform can also support multiple legs in a single atomic transaction, which could look something like this:

- Alice sends Bob her car and surfboard
- Bob sends Alice 20,300 euros
- Bob sends Carol his vintage electric guitar
- Carol sends Bob 5,000 euros
- Carol sends Alice her electric bike
- Alice sends Carol 1,500 euros

Distributed Asset Allocation

The iov42 platform supports a process called “Distributed Asset Allocation” (DAAL), which includes reserving assets, and in doing so allows multiple, overlapping transactions to be performed against the same account, while preventing double spending.

DAAL takes place during the consensus reaching process. In determining the validity of a transaction, the voting nodes will reserve the appropriate balance against the account that submitted the transaction. In the case of unique assets, such as Alice’s car, the “balance” of this one asset is reserved. If there is an insufficient balance for a requested transaction, it will be rejected.

DAAL is analogous to what happens when you use your bank card during a shopping trip—you may use it multiple times throughout the day at different shops. As long as you have sufficient funds in your account, each transaction will go through, even if the money won’t actually be debited from your account until one or two business days later.

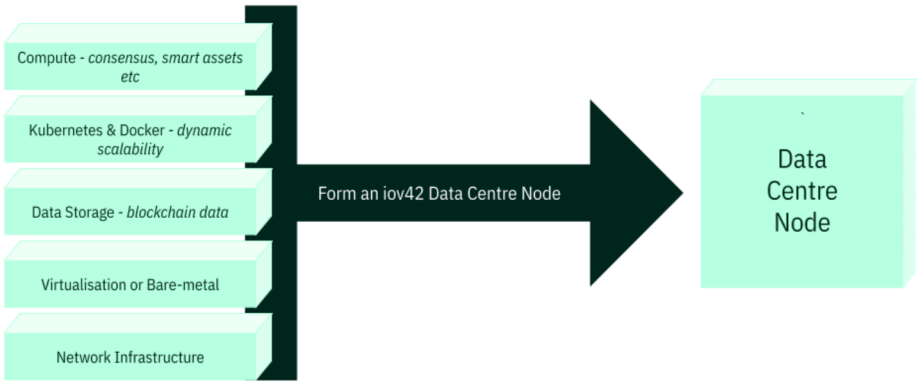
Building for performance and scalability

In traditional blockchain models, having more nodes within a system improves resilience against system-threatening events such as power outages, other technological failures, or certain exploits. Some blockchains are being run on thousands of nodes.

However, an increasing number of nodes does not necessarily improve the performance of classic blockchains. If each node must process and record all of the blockchain's transactions, as well as store other related data (e.g. cryptocurrency wallet balance, smart contract code, etc.), the performance of the blockchain could be greatly limited by the computing and storage capacity of one node, as well as the need to use slow consensus algorithms to prevent unwanted interventions.

The traditional blockchain model of a single device serving as a node simply does not scale.

In order to build a DLT network that can operate at a global scale, iov42 has reimagined the structure of the node. Instead of using single computers as nodes, the iov42 network uses data centres that can leverage all the advancements and scalability that comes with distributed computing and cloud supporting technologies. And because the iov42 network has been developed using technologies such as Docker and Kubernetes, it can be deployed to different cloud providers or even a traditional data centre.



Each node is a data centre

With nodes as data centres, the various functions of a node—communicating, validating, committing, synchronizing, storing data, etc.— can be broken down and carried out independently. The main benefit of using data centres is scalability, which in turn improves resilience, performance, and the ability to add resources as needed as the data across the system grows.

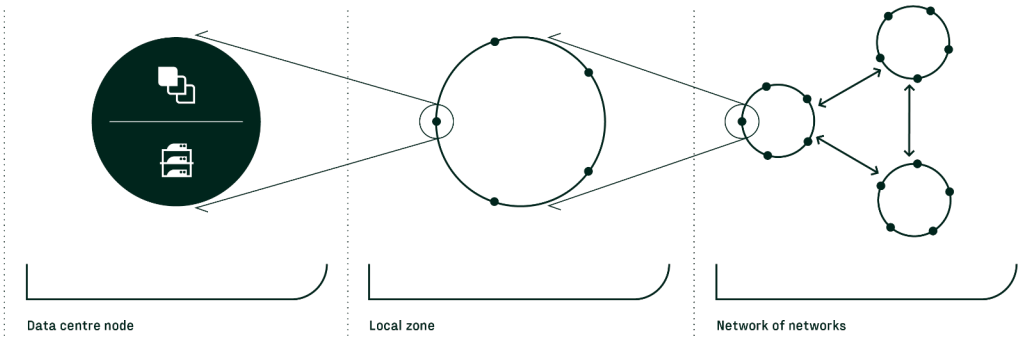
If each iov42 node is a data centre, this means not everyone can run a node in an iov42 network.

However, iov42 considers this to be a benefit to the network rather than a constraint. Limiting the number of participants within the network has a positive effect on the performance of the system. This also means that node operators will be recognized entities that agree to collaborate within an iov42 network. Deliberate network formation through strategic node selection increases the system's flexibility to address

issues such as governance, industry-specific security concerns, and data locality.

Connecting iov42 nodes

Another unique feature of iov42 nodes is the way they connect with one another. Instead of thousands of nodes interconnected globally, only a few nodes connect locally to form what iov42 calls a “zone.” Across the iov42 network, zones can be optionally connected, enabling local regulatory frameworks to be built into each zone and creating a “network of networks.”



The iov42 Trust Zone

The nodes in a zone form the basis of a single DLT network. Every node in the zone participates in consensus and has a copy of the immutable history of all of the zone’s activity. All data, including transactions, remain within the zone. This enables the data centre nodes to comply with any relevant data locality regulations.

An iov42 zone can be created based on factors such as geographical location, industry, or even regulatory requirements. In most cases, geography will be the determining factor.

For example, a group of petroleum suppliers could form a zone to allow their customers to trade fuel and carbon certificates within a certain region. Another example could feature telecommunications companies or internet service providers (ISPs) coming together to offer the iov42 platform as a service for their customers to develop DLT solutions.

The zone model advantage

The zone approach has advantages for performance, security, and governance. Limiting the number of nodes and their geographical proximity to one another ensures a rapid consensus process and a higher number of transactions per second. Furthermore, since the nodes are all known entities to each other, there is little incentive for zone participants to undermine the zone’s integrity. Lastly, governance is built into each zone through legal agreements made between the operators of the nodes. If a dispute occurs amongst the nodes in a zone, the geographical bounds of each zone allow appropriate and efficient legal proceedings to take place.

But what about global reach?

Theoretically, an iov42 zone could be formed anywhere in the world, where the right infrastructure exists. The zones are designed to eventually be able to connect with one another and form a global network of networks. This would lead to the formation of digital borders across the platform that could truly meet demands of scalability, interoperability, and regulatory compliance.

How does consensus work?

Although the design of the node and the network contribute to the performance and scalability of the iov42 platform, its consensus process is one of the most critical aspects influencing the platform’s security, performance, and efficiency.

DRME: A novel approach to consensus

In an iov42 network, consensus is responsible for protecting anything that requires trust — from users making claims about their identities to exchanging the ownership of an asset on the network. Ultimately, no changes can be made to the state of the system without going through consensus.

iov42 has developed its own consensus mechanism called DRME (Distributed Random Master Election). This proprietary consensus algorithm leverages the architecture of the network to be highly-performant and energy efficient, while being able to randomly assign which node leads the coordination of any given consensus decision on a per transaction basis.

The DRME process is divided into three key parts:

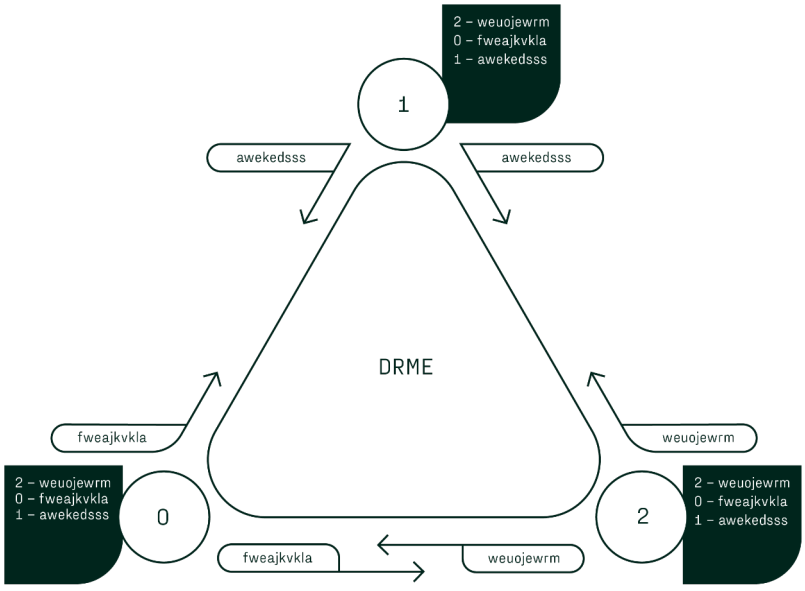
1. Master election
2. Voting to reach consensus
3. Committing the transactions to the network

For each transaction that passes through the platform, one of the consensus participants is randomly elected to be the “master” that will coordinate the voting process amongst all network participants to determine whether the transaction is valid or not. Based on participant votes, the master ultimately decides if the transaction is valid and can be committed to the network’s immutable ledger, or if it is invalid and must be rejected.

1. Distributed Random Master Election (DRME)

iov42’s consensus process starts with its master election algorithm, DRME, which is where the entire process gets its name from. DRME is the process that establishes which participant decides the validity of each transaction. The goal of this process is to be completely random, as well as agreed upon by all participants.

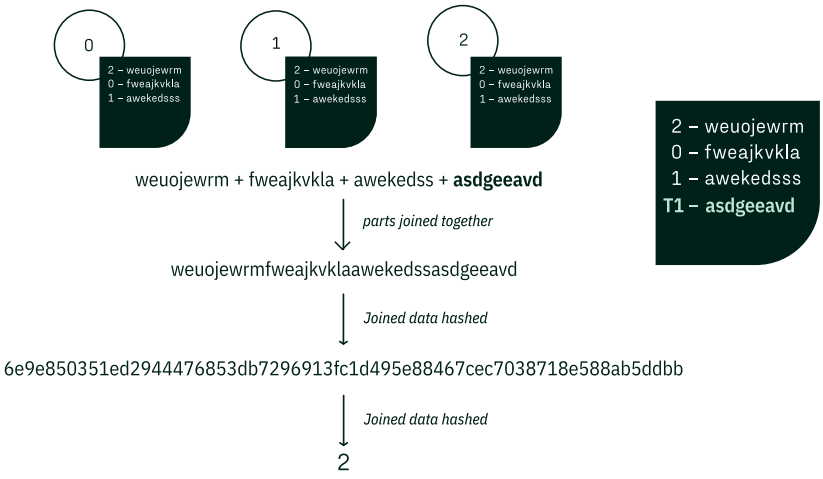
DRME starts with a series of messages known as DRME fragments. Each fragment contains a completely random chunk of data of a known length. All participants within the network generate and broadcast these random fragments to all other participants at regular time intervals. The received order of these messages is identical across the network, so each participant has the same understanding of the state of the system.



In this example, there are three participants in the network. All of the participants are sending DRME fragments to each other at regular intervals. The order in which the fragments are received is random, but deterministic, and reflected in a message log. In this example the message log shows that the fragment from Participant 2 was received first across the network followed by the fragments from Participant 0 and Participant 1. The participants will continue to transmit DRME fragments at regular intervals.

Incoming transactions are broadcast to the network participants through the same path that all DRME fragments are broadcast. This means that fragments and incoming transactions are interspersed, ensuring that each participant has the same view of the world when a transaction needs to be validated.

When a transaction arrives, the latest fragment from each node is joined together with a unique value from the transaction. This combined fragment is first hashed using SHA-256. The resulting hash value is then passed through a modulus function, based on the number of participants. The result of the modulus function determines which participant will act as the master for that transaction.



In the above example, a new transaction has been received. The latest DRME fragment from each participant is ordered and combined. Then the unique data from the transaction—in this case, "asdgeevd"—is added to the string of combined fragments. All of these combined parts are passed through a hash operation to produce a value that is then passed through a modulus function. As mentioned above, the modulus function is based on the number of consensus participants, so this example uses MOD3, since there are three participants. In this example, the modulus function produced a value of 2 which means that participant 2 will be the master for this single transaction.

2. Voting to reach consensus

The role of the master is to coordinate the activity for any given transaction. The elected master asks all participants, master included, to vote on the validity of the given transaction. Each participant will check that the request is valid based on its understanding of the state of the system (e.g. “is there enough balance to perform the transaction?”). If the transaction is valid, participants will reserve the appropriate balance against the transacting account though the DAAL process and send back its signed vote to the master.

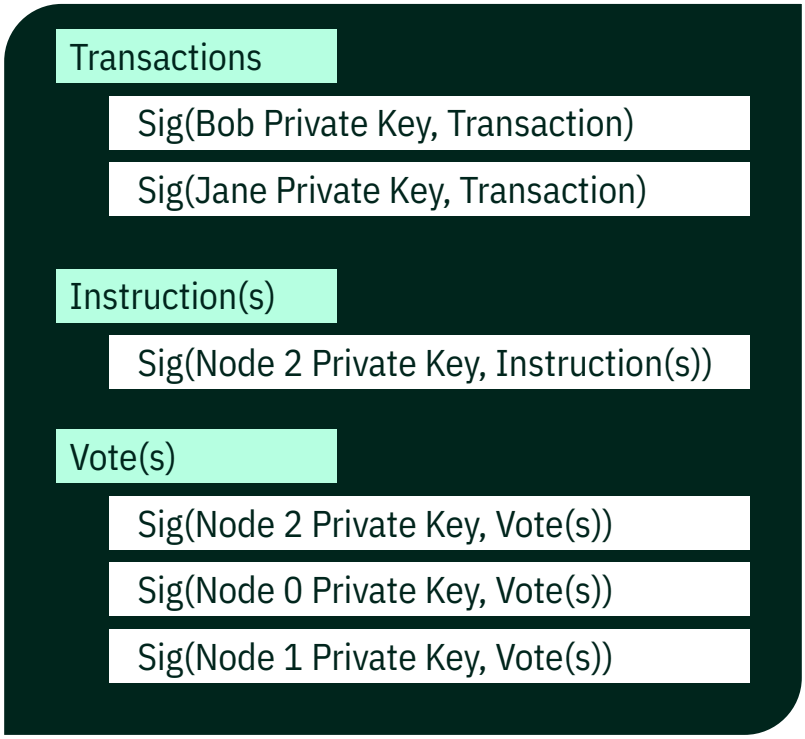
Throughout this consensus-reaching process, integrity is ensured by the use of digital signatures at each step. First, each transaction that is submitted must be signed by the identity that submitted it. The master then signs its instructions before sending them out to the participants to prove it was the source of these instructions. Next, each voting participant signs its vote to prove it has voted. Finally, all signed votes are collated by the master.

3. Committing the transaction

Once the Master Node has collected enough votes and attached these as a part of the proof for the transaction (some transactions may require a majority, some may required full participation) it will then issue a commit message (in the case of a valid transaction) which tells all nodes to commit the transaction to the immutable store.

If the system participants concur that the transaction is valid, the master will issue a commit message. This message takes the form of a transaction proof that contains all of the steps and signatures associated with the transaction.

This proof (rendered on the following page for demonstrative purposes) is then signed by the master to prove it is the collator of the proof. Finally, the proof is committed to the network’s immutable distributed ledger.

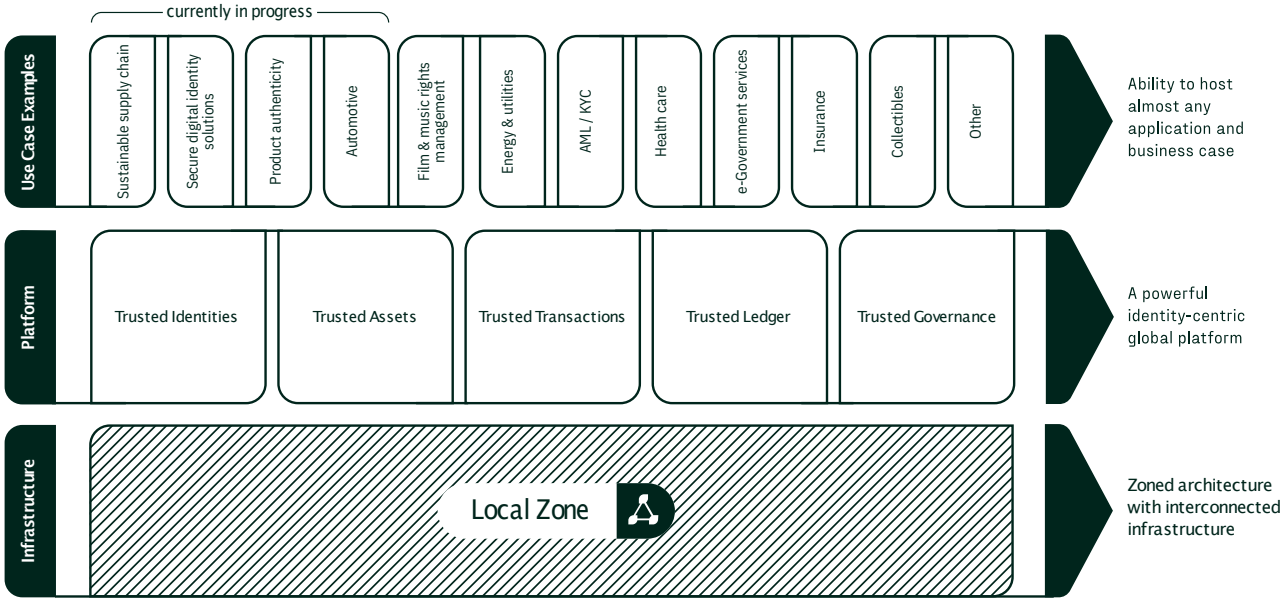


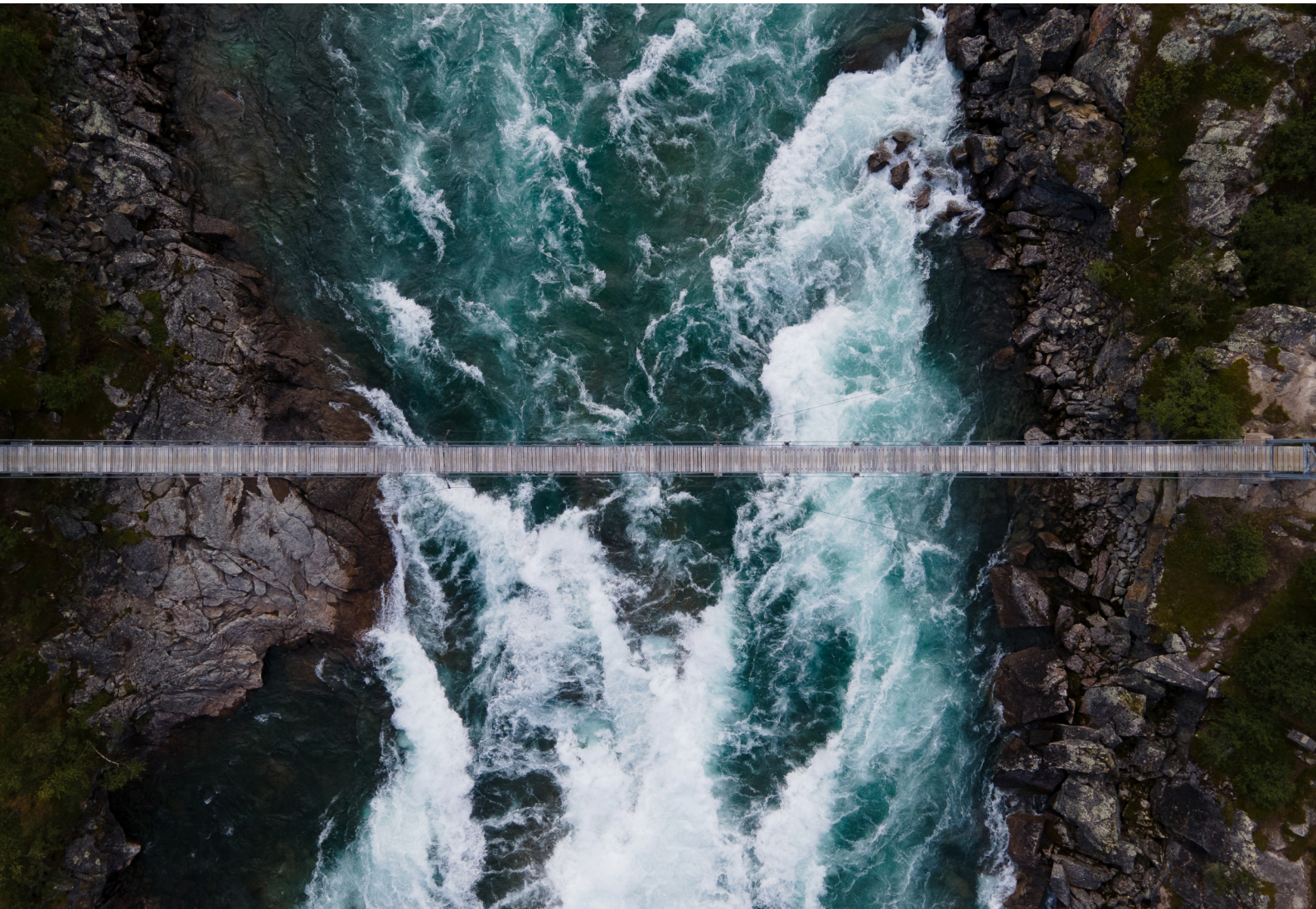
Why is all of this important?

While the randomness of DRME ensures that a bad actor cannot manipulate a iov42 network, the protocol's per-transaction approach allows the global iov42 platform to combine high performance, security, and low energy consumption, positioning iov42 as an ideal DLT solution for enterprises and governments.

Conclusion

iov42's goal is to build a compelling architecture that enables its users to take advantage of an Internet Of Value for their own use cases and, ultimately, to become the location where innovation can generate new economic and social benefits.





DISCLAIMER

No warranties: The information in this document ("Document") is provided without any representations or warranties, express or implied. Without limiting the scope of the aforementioned sentence, the ValueWeb Holding Limited ("Company") and its executives do not warrant or represent that the information in this Document is true, accurate, complete, current or non-misleading. Data, figures and numbers in this Document are based on assumptions and estimations. They are not reviewed and they are unaudited.

No advice: This Document contains general information about the Company and its affiliates. The information in this Document is not advice and should not be treated as such.

Confidentiality: Information disclosed in this Document and, in particular, the existence and content of this Document in general are to be considered strictly confidential and no shareholder or other person is allowed to disclose them to any third party, excluding other shareholders of the Company, without the prior written consent of the Company ("Confidential Information"). The foregoing confidentiality obligation shall not apply to any information or facts that are or become publicly available.

Intellectual property: The Company shall retain all right, title and interest to its Confidential Information. No licence under any intellectual property rights (including trade mark, patent, or application for the same, or copyright, which are now or may subsequently be obtained) is either granted or implied by the disclosure of Confidential Information.

No legal claim: The information in this Document is without prejudice and does under no circumstances entitled to any (legal) claim against the Company and cannot be used for any (legal) claim against the Company or other companies within the ValueWeb Group. The receiver of such information is not entitled to use the information in this Document before court or in any other (legal) proceeding. Any liability arising from the information in this Document is explicitly excluded.