intoNet

Technical White Paper

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

1. Abstract

The IntoNet team is building a next generation decentralised ecosystem for global nonprofit (NPO) and non-governmental organisations (NGOs) based on blockchain technology. IntoNet provides a Blockchain as a Service (BaaS) solution, allowing any organisation to deploy private blockchain and create a custom cryptocurrency with advanced capabilities including smart contracts.

In many cases individuals and organisations make global donations and payment to help NGOs and NPOs with disaster relief (hurricanes, floods etc.), promote social and economic goals and provide direct (financial) or indirect (equipment, food etc.) aid to people in need. However, in many cases these donations and payments take too long to be processed and reach the right hands to achieve the goals they were meant to address. In addition, donors are challenged to achieve visibility and transparency into the cash flow and effect caused by their monetary aid.

IntoNet will use blockchain technology to revolutionise and democratise the process of monetary aid transactions with NGOs and NPOs by placing the power and control over donations into the hands of the individuals and the organisations that provide it as well as the target NGOs and NPOs they are looking to aid.

Our aim is to give donors and organisations looking to alleviate and relieve disasters direct access to financial aid opportunities in the crypto world and to enable NGOs and NPOs to raise capital for financing their projects in an efficient, cost effective, and secure way. In addition, we seek to clearly track transactions and learn from the data that will be aggregated in that process, to improve their services towards people in need as well as towards their donors.

IntoNet's main cryptocurrency (ITN) will be paired with the Swiss Franc (CHF), so every issued token will be backed by a deposit of 1 CHF into a Swiss bank account, ensuring a one-to-one exchange rate between ITN currency and the Swiss Franc, allowing it to maintain clear and stable intrinsic value. In addition, IntoNet will develop white labeled cryptocurrencies for nonprofit and government organisations, deployed across private blockchain systems within the organisations.

Our unique strength is our team's ability to enable a first of its kind ecosystem based on a network of world leading NGOs and NPOs. When combined with blockchain technology, and the backing of Emerald Bank, this unique ecosystem will allow us to bring to market a powerful, secure way of helping NGOs and NPOs using a cutting edge technological approach, while maintaining the highest standards of governance by providing a currency which holds real intrinsic value backed by one-to-one CHF deposits.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

Our engineering team acquired core knowledge and experience in developing software with the highest standards of security, privacy, anonymity, data protection and encryption – while collaborating with Europe's leading scientific research institutions.

Our technical team includes experts in information security, scale and agile development. We have gained vast experience in information security and large scale deployment. Previous projects include collaborations with Deutsches Elektronen-Synchrotron (DESY) for the development of a system which provided end-to-end encrypted storage over dCache (distributed data storage) protocol, used by many scientific institutions worldwide. We have also collaborated with the European Middleware Initiative (EMI) for a commercial implementation of Hydra, a key fragment storage system, which provides the highest levels of data security by splitting and storing encryption keys in multiple locations worldwide. This process ensures that if a server is compromised an attacker will not be able to recover the full key or gain access to the data.

2. Regulation and Governance

IntoNet will work as a technology provider partnering with Emerald Bank which will be regulated as a deposit taking business with the Swiss Financial Market Supervisory Authority (FINMA). In addition, IntoNet will build its technology to meet all of FINMA's standards for cryptocurrency and will apply for payment processing regulation. Unlike traditional cryptocurrencies which have no intrinsic value, IntoNet's tokens will be paired to the Swiss Franc, thus benefiting from a secure, safe and efficient way of making payment via blockchain, while maintaining a stable intrinsic value with clear exchange rates.

There are multiple reasons to pair and back the token by Swiss Franc. Beyond providing the token with real intrinsic value there are two additional benefits: relying on strong fiat currency backed by the financial stability and governance of Switzerland and benefiting from the peace of mind and safety of managing all financial deposits as well as crypto vaults within Switzerland, which is known both for its high financial security standards as well as high level of regulations and as a pioneer in the world of cryptocurrencies.

3. IntoNet Premises

IntoNet provides white labeled cryptocurrencies and its own main cryptocurrency called ITN, whose value is based on the CHF. The ITN is managed on a decentralized blockchain and provides the following benefits:

3.1. It serves as an accepted payment and donation means for the world's leading NGOs and NPOs

3.2. NGOs and NPOs are able to hedge ITN cryptocurrency trading and other related risks due to the pairing with the CHF

3.3. It is managed by a smart contract which enables verification that the tokens are being used for the right purpose; for example people, organisations and even countries can make a pre-deposit for future disaster relief. Their deposit will include a legal contract which will be automatically executed in the event of a disaster – aiding relevant NPOs and NGOs and making sure their money will be used in the proper manner.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

4. Business Roadmap

4.1. Development of a blockchain based crowdfunding platform will allow project funding based on Sustainable Development Goals (SDGs) KPIs.

4.1.1. In the first phase the platform will use blockchain for distribution of user and project metadata and for the creation of transparency and higher security

4.1.2. In the second phase the platform will introduce cryptocurrency as a means of funding, making the funding process faster and with reduced fees

4.1.3. In the third phase the platform will introduce smart contracts for the automation of funding and reportingCreating a cryptocurrency based on standards which will be approved by FINMA.

4.1.4. IntoNet will create its own proprietary ITN token

4.1.5. IntoNet will provide a platform for the creation of white labeled cryptocurrencies

4.2. Partnering with Emerald Bank (which will be regulated by FINMA as a deposit taking business) for the reserve of CHF fiat currency as well as the provider of the exchange service between ITN currency and CHF fiat.

4.3. Providing the currency to NGOs and NPOs against an equivalent CHF deposit into Emerald Bank.

4.4. Integrating digital wallets into the NGOs and NPOs mobile and web applications, allowing them to accept donations and payments via ITN token.

4.5. Developing additional financial tools allowing NGOs and NPOs to gain additional financial strength and flexibility from using the ITN token (see loans and cards).

5. Target Market and Industry Use Cases

5.1. Initially we will target the world's leading NGOs and NPOs, with later potential expansion to support governments and central banks looking to create a digital cryptocurrency which is controlled and backed by their own real assets.

5.2. IntoNet will create the Sustainable Development Goals Funding Platform, allowing organisations to apply for the funding of projects which address one or more of the SDGs. The platform will provide donors with full transparency into the funding process, making sure that funds make their way to the right projects, quickly, efficiently and with low transaction costs.

5.3. The Humanitarian Organisation use case – Humanitarian organisations rely on donations and monetary aid for disaster relief. Those transactions may come from anywhere in the world. In these cases, both the donors as well as the management of the humanitarian organisation want to ensure that the money flows quickly and efficiently to provide help on the ground in the most optimal manner. Using cryptocurrency will reduce transaction fees, as well as speed up the process and increase visibility and accountability for the financial aid. In addition, the cryptocurrency wallets can be incorporated into Points of Sale (POS) allowing merchants to quickly accept cryptocurrency as a viable currency, thus providing the needed supply for any kind of aid operation, and later reusing the cryptocurrency for purchasing from suppliers or exchanging it for fiat money at a known rate.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

5.4. Corporate transactions – In some territories, such as Kazakhstan, local payments between companies bear high transaction fees. Using a cryptocurrency which is coupled with a fiat currency can allow for instant, secure transactions without the associated high fees.

5.5. Mobile payments for the unbanked – Due to the unavailability of banks and low penetration rate of credit cards in emerging markets such as Kenya and the Ivory Coast, many individuals remain unbanked. Even those with an account rarely visit the banks due to the long distances between locations. As such, people rely on mobile payment technologies (e.g. MPESA) or in some cases travel to the local post office, which is still far away, to get payment for a job they have completed. As mobile payments are controlled by the telecom companies, the government has only partial visibility into the transactions. These telecoms are usually privately held companies, meaning that the government has no control over the amount of POS locations, service level or availability. In places where the economy relies on cash the problem is compounded as the government is very limited in its ability to charge associated income taxes. To remedy this situation, governments are now looking for a monetary solution which can be easily implemented on any mobile device, while allowing the government to gain full visibility and analytics regarding the transactions and payments being made, as well as ensure their desired level of service to their citizens.

6. ITN Exchange and Payments

6.1. Emerald Bank, which will be the official regulated banking partner of IntoNet, will help convert ITN into CHF and other fiat currencies by operating exchange and payment services.

The exchange service will include:

6.1.1. Acceptance of credit cards and bank payments for ITN tokens

6.1.2. Robust KYC and AML to validate all traders and prevent money laundering

6.1.3. Future integration with PayPal, Alipay and other payment means

6.1.4. Mobile and web wallets integration into a merchant's POS and within NGOs, NPOs and member applications

7. Hedging Crypto Trading Risks

Current cryptocurrencies such as BitCoin or Ethereum are considered by many to be very volatile and to have no intrinsic value. IntoNet will help reduce volatility risk due to the fact that the token is fully paired with the value of the Swiss Franc.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

8. Technical Roadmap

8.1. Launching IntoNet Blockchain

8.1.1. Developing IntoNet Blockchain Infrastructure – a semi-private and permissioned blockchain, built upon a well-known and proven framework - the Hyperledger Fabric

8.1.2. Initially, the IntoNet Blockchain will be centralised and operated by IntoNet nodes.

8.2. Developing SDG Grants platform – the first application to be built on top of IntoNet Blockchain. It will serve as a fundraising platform for NPOs and NGOs using the UN-defined Sustainable Development Goals. Using the SDG grants application, candidates can apply for donations for projects intended to fulfill SDG goals, providing details about the specific project (goals, locations, roadmap, etc.) and details on the candidate's organisation. Donors can then search and review the various donation requests and choose the projects to which they wish to donate.

8.2.1. In the first phase the platform will use IntoNet Blockchain for the distribution of user and project metadata and to promote transparency and increased security. No cryptocurrency will be available during this phase - donors will donate through traditional channels (their donation metadata may be recorded on the blockchain).

8.2.2. In the second phase, when ITN cryptocurrency and its backing fiat reserves are created (see below), the SDG platform will enable funding with ITNs, making the funding process faster, more secure and with lower fees.

8.2.3. In the third phase the platform will introduce smart contracts for semi-automation and control of funding and reporting. For example, a smart contract will guarantee that a donation amount is fully paid only if the candidate has provided proof of achieving their declared goals.

8.3. IntoNet Cryptocurrency and Financial Ecosystem:

8.3.1. Create the native IntoNet cryptocurrency, which has been given the 'ITN' ticker. The ITN tokens will be managed by a smart contract deployed on IntoNet Blockchain, inspired by the Ethereum ERC-20 standard

8.3.2. Integrate with Emerald Bank to establish proof of reserve methodology and procedures, thereby ensuring that the ITN supply is backed by a CHF fiat balance - the ITN amount in circulation must always be equal to or lower than the actual CHF balance in the Emerald Bank reserve account.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

8.3.3. Add new ITN tokens, or remove ITN tokens from the total supply. This will only be done by authorised Emerald/IntoNet operators following the completion of the proof of reserve procedures.

8.4. Developing applications and custom cryptocurrencies for various organisations and use-cases:

8.4.1. Web and Mobile Wallets - IntoNet will develop web and mobile client applications to be used as stand-alone wallets or to be integrated into NGOs/NPOs member applications. The wallet will provide several functionalities, including:

8.4.1.1. View ITN (and other IntoNet custom cryptocurrencies) balance
8.4.1.2. Send and receive ITN and other IntoNet-based tokens
8.4.1.3. Display personal transaction history
8.4.1.4. Interact with the Blockchain and smart contracts (restricted by access controls)
8.4.1.5. Secure storage of private key/s
8.4.1.6. Backup and recovery procedures

8.4.2. Custom Cryptocurrencies - IntoNet will create custom cryptocurrencies which will be white labeled and customised for the unique needs of NGOs, NPOs as well as governments which work with Emerald Bank. Each custom cryptocurrency will be based on a separate smart contract, using the same standard and logic as the ITN currency (and same proof of reserve methodology). By default, any custom cryptocurrency is backed by 1 CHF and optionally, custom cryptocurrencies can be backed by other fiat currencies.

8.5. Expanding and decentralising the IntoNet Blockchain network:

8.5.1. Per each organisation or government entity that joins IntoNet (with or without custom white labeled cryptocurrency), IntoNet will deploy additional operating peers (endorsing, ordering service, committing) that will be partially controlled by the joined party.

8.5.2. These peers will participate in a dedicated IntoNet channel that will be created for the specific organisation (with a segregated ledger and smart contracts only accessible for that channel) as well as in a global channel that connects all organisations and IntoNet together (such a channel may serve as a cross-organisation collaboration and exchange between custom cryptocurrencies).

8.5.3. By deploying those peers (and creating endorsement policies that require the organisation’s signatures), IntoNet will be decentralised from the organisation’s perspective.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

8.6. Blockchain and Wallet Features - developing and providing advanced features on top of IntoNet Blockchain and wallets. Such features may include:

8.6.1. Multi-signature accounts

8.6.2. Decentralised exchange - exchanging between ITN and custom IntoNet tokens

8.6.3. Two-factor authentication - additional layer of security to protect IntoNet accounts rather than relying on private keys alone. A possible 2FA scheme may involve off-chain OTP sent by email or SMS while submitting the OTP hash to IntoNet smart contract and requiring the client to solve the hash challenge on the IntoNet Blockchain

8.6.4. Decentralized marketplace

8.6.5. End-to-end encrypted chat - using the pre existing private and public keys, any account owner on IntoNet Blockchain will be able to send encrypted messages to any other account owner using global channels, dedicated smart contracts and dedicated chat applications (which may be integrated into the wallets)

8.6.6. Fraud and scam detection - enable users to report fraud or scam attempts, implement algorithms to detect potential frauds and support blacklisting of specific accounts that are suspected to be in use by scammers

8.7. Reward Engine - Developing a reward engine that enables each organisation to integrate reward programs into their members' applications.

8.7.1. The reward engine will be based on an abstract smart contract interface that can be implemented per each organisation's needs

8.7.2. The reward transactions will be controlled by a transparent and secure smart contract, using ITN cryptocurrency or a custom white labeled cryptocurrency

8.7.3. A reward balance will be allocated per organisation, based on the organisation's own funds and/or IntoNet reward funds (pre-allocated by Emerald Bank)

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

8.7.4. The specific logics of reward eligibility will be developed per use case. A possible use case is rewarding users who create content that promotes an organisation's interests

8.7.5. Example reward use cases will include:

8.7.5.1. Rewarding users for content creation and curation

8.7.5.2. Rewarding users for alerting and providing critical safety information

8.7.5.3. Rewarding organisations for meeting project deadlines and deliveries

9. IntoNet Blockchain - Technical Properties

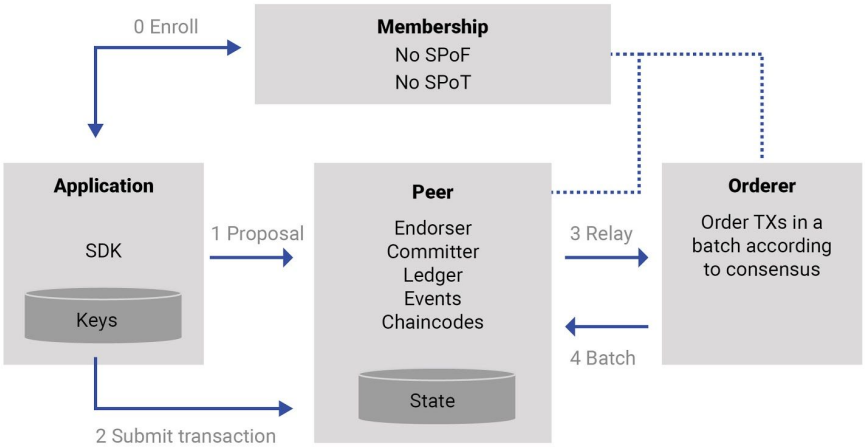
9.1. IntoNet Blockchain is built with a hybrid centralisation and distribution model - it is private and centralised in the sense that transaction validations, consensus, blocks commitment and the storage of the ledger data can only be operated by pre-authorised nodes. On the other hand, partner organisations may operate some of these nodes - making the network more decentralised, and IntoNet provides distributed applications based on reviewable smart contracts. Using this model, IntoNet Blockchain has the core benefits of popular public blockchains (such as Bitcoin and Ethereum), while avoiding common drawbacks of such blockchains, like low scalability, high transaction fees, expensive energy consumption, 51% attacks, chain splitting and more.

IntoNet is built on top of Hyperledger Fabric framework, which was originally developed by IBM and is already being successfully adopted by several industries around the world. The architecture concepts and properties of Hyperledger Fabric enable IntoNet to implement the hybrid blockchain model described above. IntoNet uses the framework as a robust basis on top of which it develops its own proprietary core solution and intellectual property.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

9.1.1. *Figure 1. High Level overview of the Hyperledger Fabric Architecture*



9.2. Following are key properties and architecture concepts of the blockchain (more detailed specifications are available on Hyperledger Fabric Docs):

9.2.1. **Private consensus network** - consensus is reached within a closed (private) network of pre-authorized and highly-trusted nodes. These nodes will be operated by IntoNet, Emerald Bank and potentially its partners and customers (large NPOs and NGOs, African governments).

9.2.2. **Simple consensus algorithm** - since consensus is made within a closed network of highly trusted nodes, a simple fault tolerant algorithm is used, thus allowing:

9.2.2.1. High scalability and throughput

9.2.2.2. Low energy usage

9.2.2.3. No transaction fees (and hence no prioritised transactions)

9.2.2.4. Security - No malicious actors can take over consensus power (the private consensus participant nodes will be highly protected)

9.2.3. **Secure consensus protocol** - the consensus protocol (which is responsible for the entire transaction process flow) is comprised of 4 steps, involving the client

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

application and 3 types of blockchain nodes. The consensus design guarantees that transactions are securely validated (or rejected) and committed by distributed nodes, so even if some nodes in the process are compromised or misbehave, the network and ledger data remain stable and reliable:

9.2.3.1. First step: the client application sends a transaction ‘proposal’ to several ‘endorser’ nodes (each application may choose different nodes randomly or consistently), which are responsible for validating the transactions and simulating their execution. Each endorsing node sends the resulting output back to the application, signed with its own private key.

9.2.3.2. Second step: The application validates the transaction endorsements. This validation includes:

9.2.3.2.1. Validation of signatures

9.2.3.2.2. Minimum number of required valid endorsements (as defined in a configurable endorsement policy) - all having the same output result - is reached

9.2.3.2.3. The valid endorsements meet the requirement of the endorsements policy in regards to the identity of the endorsers (for example, the policy may require at least one signature from each organisation unit)

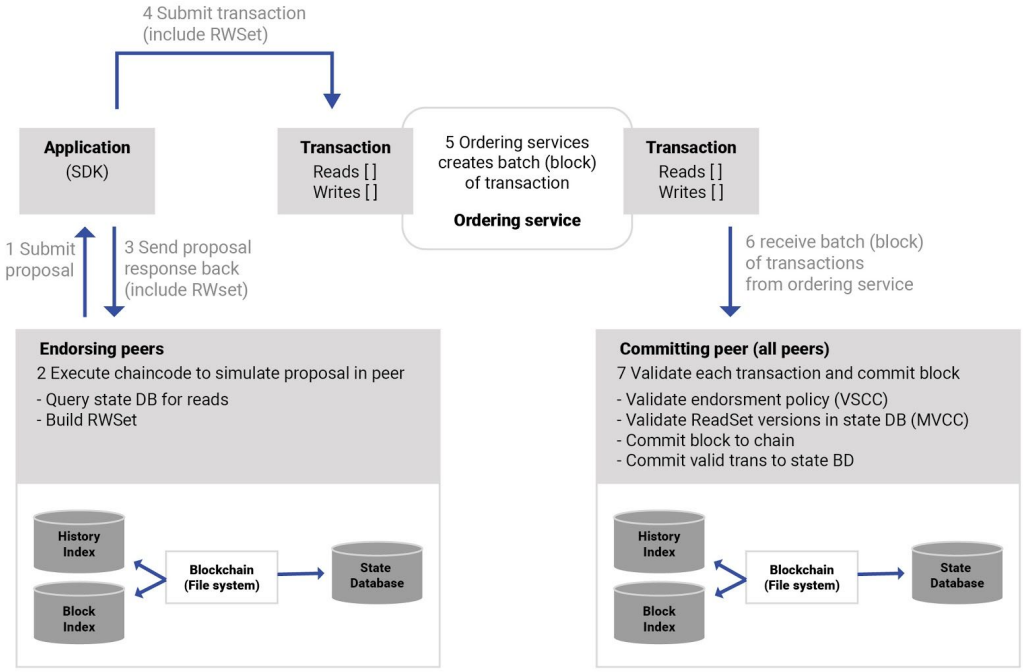
9.2.3.3. Third step: The application sends the endorsed transaction messages to an ‘Ordering Service’ node (either directly or through ‘proxy’ nodes), which is responsible to validate the endorsements (the application validation is not trusted, endorsements are validated again from scratch), to batch multiple transactions in their sequential order in a block, sign the block and send it to committing nodes.

9.2.3.4. Fourth step: Signed transaction blocks are sent from the ordering service to ‘committing nodes’, which execute all transactions in the block by their sequential order and commit the output states to the ledger. Committing nodes may be operated on the same peers as endorser nodes and they maintain the entire ledger data that is relevant for their channels. The committing nodes validate the transaction endorsements and also validate that the state of the keys involved in each transaction has not been changed since the transaction was made (to prevent double spending and other race condition issues). In this step, transactions are either finally confirmed or finally invalidated.

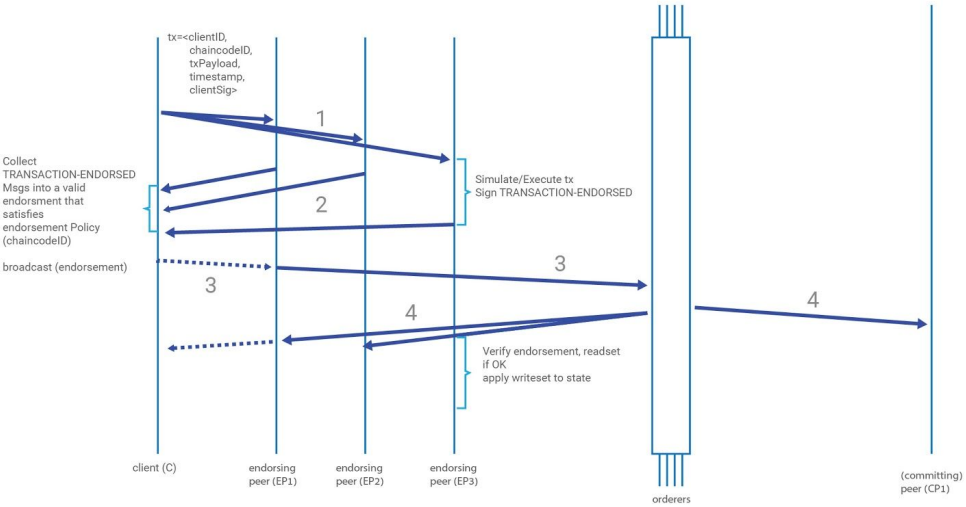
Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

9.2.4. Figure 2. Consensus Architecture Overview



9.2.5. Figure 3. Illustration of the transaction flow (common-case path)



Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

9.3. **Permissioned Blockchain** - The blockchain data (the ledger), operations and smart contracts are protected by authentication and access controls based on node types, identities and roles.
All participants in the network must be granted a certified identity by a membership service provider (MSP). The membership model is based on X.509 certificates:

9.3.1. Root CA certificates - produced and owned by IntoNet/Emerald.

9.3.2. Intermediate CAs - IntoNet root CA will issue intermediate CA certificates to its customers and partner organisations.

9.3.3. Each intermediate CA will issue individual certificates to eligible end users.

9.4. **Access Controls** - Access controls are managed in several layers:

9.4.1. Network roles by node type (core services like consensus, ledger storage and membership can only be run by pre-authorised nodes).

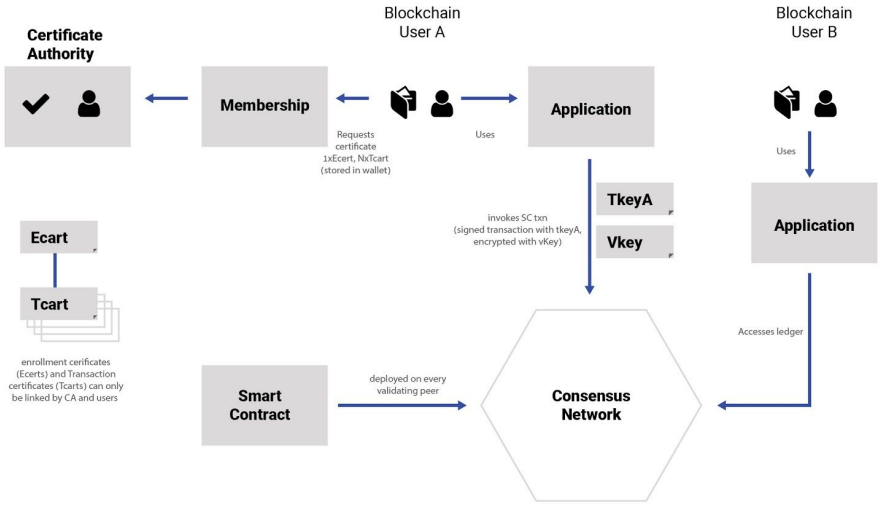
9.4.2. Channels - IntoNet Blockchain network maintains multiple channels, which are like segregated ‘subnets’. Each organisation will have its own channel (and possibly multiple channels) and each user identity will belong to one or more channels. Communication (transactions) made within one channel can only be accessed by members of that channel, thus enforcing full segregation between different organisations (or tenants).

9.4.3. Smart contract access - smart contracts in IntoNet Blockchain can only be created by authorised identities. In addition, a smart contract is deployed to a specific channel so that only participants of that channel can interact with the smart contract. Finally, executing a smart contract and reading its state requires authorisation.

Strictly Confidential, all rights reserved to Emerald 2017

6, Place de l'Université Case
Postale 85 1211 Genève 4 - CH
info@intonet.com
www.intonet.com

9.4.4. Figure 4. Membership and Access Control Overview



9.5. **Network Encryption**: Network communications are encrypted and protected by TLS

10. Proof-of-Reserve Methodology

IntoNet and Emerald Bank will establish Proof-of-Reserve methodology to provide assurance that the ITN (and IntoNet custom tokens) supply is backed by actual fiat currency reserves held in Emerald Bank account/s.

The Proof of Reserve methodology includes:

10.1. Visibility of relevant bank account balances - the bank accounts used for backing the IntoNet cryptocurrencies will be visible to auditors and interested parties

10.2. Emerald Bank will undergo periodic audits by professional auditors

10.3. Smart contract functions that control the cryptocurrency supply (add, subtract, freeze) will be highly protected:

10.3.1. Authorised to only a few trusted personnel
10.3.2. Require multiple approvals (by multiple personnel) before committing the change
10.3.3. Optionally require two-factor authentication
10.3.4. Produce logs / events that are constantly monitored by both Emerald and IntoNet

Strictly Confidential, all rights reserved to Emerald 2017