Digmus

Decentralized Anti-Counterfeit Platform

Counterfeit goods account for up to 2.5% of world trade, which means that current methods of protection against forgeries are not very effective. After extensive consultation with manufacturers and suppliers, we are developing a system for storing and verifying information regarding authenticity for various products.

Our system includes two main components. The first component is a blockchain to store unique product keys and the history of a product’s transfer between suppliers.

The second component is a mobile app to verify the product key, and provide verification for additional signs of authenticity.

According to our plans, by 2021 the total amount of profit distributed between all members of the ICO (Initial Coin Offering) will reach US$4 million a year.

Overview of the Problem

The large amount of counterfeit products sold in the world is a problem for most markets. According to experts, in 2013 about 2.5% of world trade – US$461 billion[1] – was associated with forged and counterfeit goods. This means customers are getting low-quality or fake products, and manufacturers are suffering financial and reputational losses[2].

World black market analytics from Havoscope.com state that the sales volume of counterfeit drugs alone is as high as US$200 billion a year. To compare, the amount that the pharmaceutical company Bayer AG made in 2016 is €47 billion[3] (about US$55 billion). No less important is the fact that consumers are deeply concerned about the quality of the medicine they are taking, as their health or even their very lives depend on it. This is why both manufacturers and consumers need to be able to deal with forgeries in a simple and effective way that is modern, low-cost, and universal.

Existing Solutions

Governments try to protect buyers from forged goods and manufacturers from unfair competition. But the effectiveness of these efforts is limited by, among other factors, corruption, slow reaction speed, and the difficulty of identifying counterfeits. This basically leaves the task of verifying authenticity of a product to the buyer.

It is in manufacturers' best interest to decrease the amount of counterfeit goods, so they develop different techniques to assure consumers of the authenticity of their products. Liquors are being poured into unique and difficult to forge bottles. Expensive goods are being protected by special holographic stickers. Manufacturer and consumer unions publish guides regarding the packaging and appearance of products to help buyers distinguish originals from forgeries[4]. Some more advanced manufacturers assign their goods unique numbers that can be checked on their websites. In some cases, large, powerful consumers or legal regulations require such numbers to be assigned.

These measures are only effective if the buyers know how to verify the information, which they often don't. And even the most determined and knowledgeable consumers often have trouble getting this information in a timely, useful manner in their everyday lives. Thus, granting them an easy, fast, and universal way to access verification information is an essential step in solving the problem of counterfeit goods.

Proposed Solution

We propose a way to store and verify product authenticity information that is: easy to use for the buyer, low cost, easy to implement for the manufacturer, and effective in thwarting counterfeit trade. The business side of this system was designed after extensive consultation with luxury goods manufacturers and distributors.

[1] Trade in Counterfeit and Pirated Goods. Mapping the Economic Impact.

[2] Kevin Lewis. The Fake and the Fatal: The Consequences of Counterfeits.

[3] Bayer Annual Report 2016.

[4] For example, How to Identify a Genuine Nikon Camera.

Our solution has four components:

- A certificate center to check brand authenticity and issue electronic signature certificates
- A blockchain-based database storing product information and additional data to verify authenticity
- A mobile app that verifies the product by scanning the QR code or NFC tag
- Software that integrates with automation systems from SAP, Oracle, Microsoft, and others.

The certification center is controlled by Digmus and works with brand requests for system certificates. The certification center:

- Checks the ownership of the trademark.
- Prevents similar copycat trademarks.
- Revokes compromised certificates.

The blockchain contains the following data:

- Manufacturer data signed with the root certificate: company name, link to logo, public key certificate
- Product data signed with the manufacturer's certificate: model name, link to description*, photos and/or videos*
- Individual product unit data signed with the manufacturer's certificate: product class, unique code hash, purchase verification public key*, predicted sales region*, history of movement known to the manufacturer (up to the retailer's address)

* optional

The use of a blockchain repository instead of a centralized database is predicated on two objectives. First, a blockchain is something consumers and manufacturers are more likely to trust. Second, it allows us to create the investment system described later in this document, where the issued token value is directly linked to our success in the market.

The mobile application will have the following features:

- Scanning of QR codes or NFC tags with unique product codes
- Checking product information and displaying verification results: whether the blockchain has the unique code hash, which product it corresponds to, determining if that product has already been sold, browsing the product description, photos and video of the product and/or its packaging, distributor information up to the retailer it is slated to be sold at (dependent on information provided by the manufacturer)
- Scanning of a secret unique purchase code to confirm the purchase
- Informing the manufacturer of possible forgery
- Sharing the purchase on social networks.

Digmus architecture is shown in Fig. 1 below:

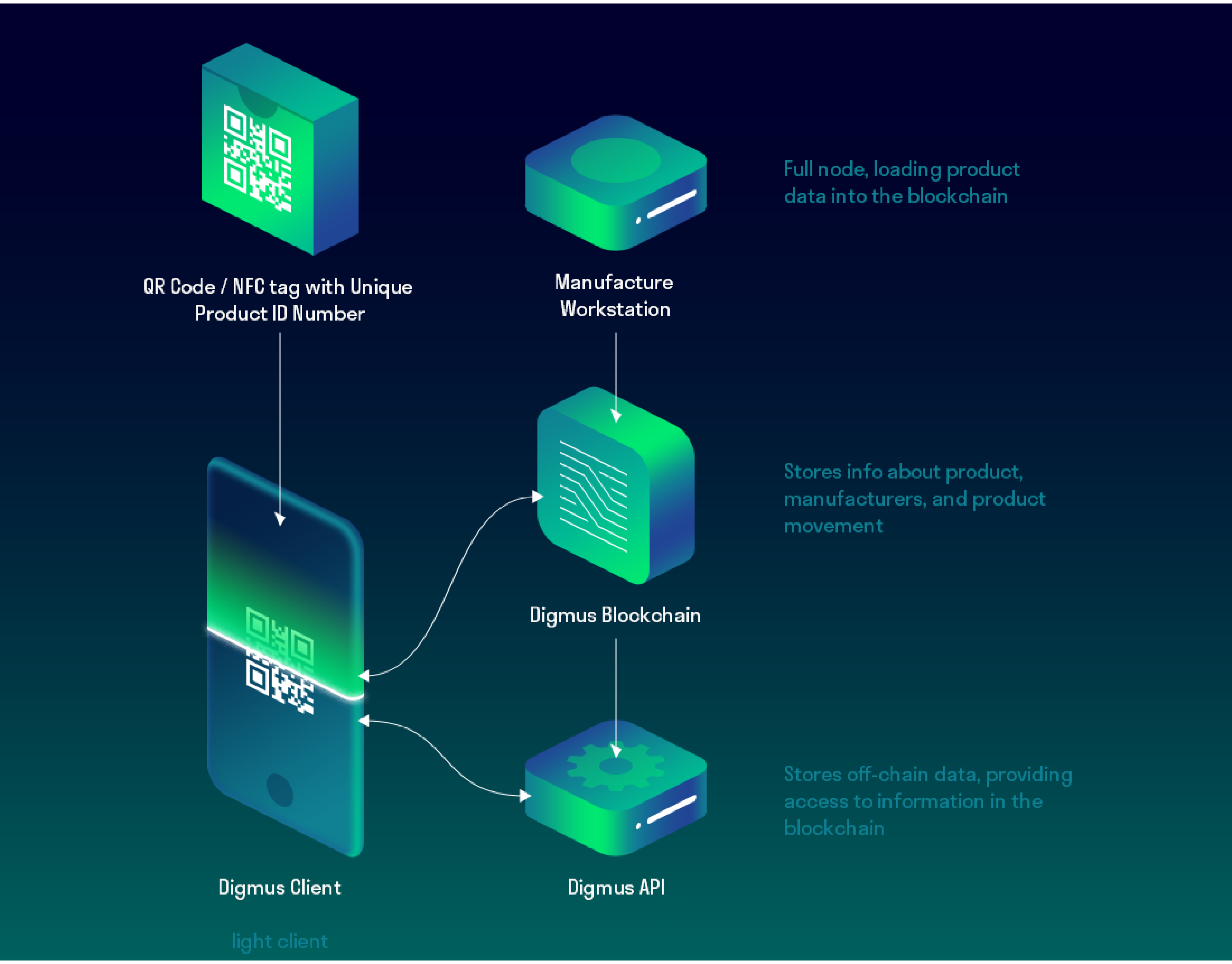

QR Code / NFC tag with Unique Product ID Number
Manufacture Workstation
Full node, loading product data into the blockchain
Stores info about product, manufacturers, and product movement
Digmus Blockchain
Stores off-chain data, providing access to information in the blockchain
Digmus Client
Digmus API
light client

Fig. 1. Digmus Architecture

The software to integrate with process control systems will be developed in close collaboration with specialists from this field, with speed of integration as a focus. At the same time, we will design a reference roadmap for manufacturers to integrate our technology.

Our solution can be implemented in any industry and in any country. With rare exception, approval from federal agencies is not required, but might be beneficial for expediting systems integration. After passing a certain market threshold, using our system, or one of the same type, will become critically important for market participants, as at that point the lack of authenticity verification on anything except the cheapest products will be considered suspicious.

Digmus is being designed with the following requirements in mind: cheap blockchain transactions (around US$0.05 per life cycle of an item), low miner reward, and low mining capacity (this means choosing PoS or DPoS). At this time, low confirmation delay is not a priority. In the first few years, quick feature development will be more important than a self-managing community. Accordingly, the protocol will be managed centrally until it is no longer warranted by circumstances.

For simplicity of development the prototype will use a centralized database. For beta and later versions we will switch to our own blockchain implementation with lower transaction costs. At this moment we are considering a Graphene-based system for these purposes.

All Digmus transactions, such as creating a new company, adding a new product, updating product movement history, etc., will require payment using an inside currency system - 'Genuineness' or GEN. Most of the coins from the transactions are "burned", with a small number being transferred to the miner as a reward. The exact share to be transferred is determined by blockchain usage, with additional reward from the author of the transaction. We are currently aiming for an 80/20 rate between currency burned and rewarded. Demand for GEN coins will increase with the popularity of the system, but the supply will decrease due to the destruction of coins, thus potentially leading to GEN cost increase.

It is, however, very important to keep the average lifetime cost for a product unit on Digmus negligibly small for the manufacturer. At this point we consider $0.05 per product unit lifetime to be a reasonable expense, and very low compared to potential losses due to counterfeit trade, but this amount may need to be adjusted later. For simplicity's sake, let's say that an average product unit lifetime cost in Digmus will be 1 GEN. This means Digmus should regulate coin emission to keep the value of 1 GEN at $0.05 or less. This is addressed in more detail later in the document.

Use Cases

Here are a couple of examples of how our system can be used by consumers and manufacturers:

Use Case 1: Manufacturer

Pharm Tycoon AG (PT) is producing a drug, Expenzium, selling 10,000 units a month for $1,000 per unit. They decide to use our system to lower Expenzium forgeries in the market. PT can convince their wholesale buyers to sign new contracts, making them report the final retailer the drug was sent to, up to the pharmacy chain or name of the hospital. The PT forgery protection budget is rather large, up to $10 per unit.

1. PT signs a contract with Digmus, receiving an electronic signature certificate as a manufacturer of this brand of products.

2. PT adds Expenzium to the Digmus blockchain: name, photos of the packaging and the drug itself, description, and any additional information they want to provide to the buyer, paying for this transaction in several GEN coins.

3. Unique IDs are generated for each Expenzuim blister to be manufactured next month - either by PT's own information system, or by using a function provided by the Digmus wallet.

4. Likewise, unique purchase IDs are generated for the same blisters, either by PT's own system or a function built into the Digmus wallet.

5. Unique unit ID hashes and public keys for unique purchase IDs are added to the Digmus blockchain, costing PT around 6000 GENs.

6. PT prints unique ID and purchase ID QR-codes for all units, and places them on the outside and the inside of the packaging, respectively. Those codes are linked to shipments, and PT updates their system with information regarding which distributor received which shipment.

7. After distributors receive their shipments, they update PT regarding movement along the distributors' chains. PT adds these movement stages (country, region, individual seller) to Digmus, spending around 4000 GEN to do so.

8. An Expenzium buyer scans the QR code on the outside of the package to compare the official data with the circumstances of their purchase. Optionally, the buyer registers their purchase using the QR code on the inside of the package, or, also optionally, informs the manufacturer of possible forgeries. PT can check purchase registrations on their software client, and Digmus sends them notifications regarding possible forgeries.

Use Case 2: Buyer

Alice wants to buy a Power Tools LLC hammer drill in a store that she does not completely trust. The price tag is $300, and Alice does not want to waste money on a counterfeit that will break in a couple of days.

1. Alice decides to purchase a hammer drill that uses Digmus verification, since this is the only one allowing her to verify product authenticity before the purchase.

2. Using the Digmus mobile app, Alice checks the hammer drill's QR code and learns that not only was it supposed to be sold on another continent, but this item has already been reported as purchased.

3. Alice leaves the questionable store and finds the same type of hammer drill at another seller, again checking using the Digmus mobile app.

4. This time all of the information checks out: the hammer drill is not reported as purchased, it matches the photos in the app, and is intended to be sold in the area Alice is in.

5. After the purchase Alice registers the unique purchase code to get an extended manufacturer's warranty.

Both user cases are shown in Fig. 2 below:

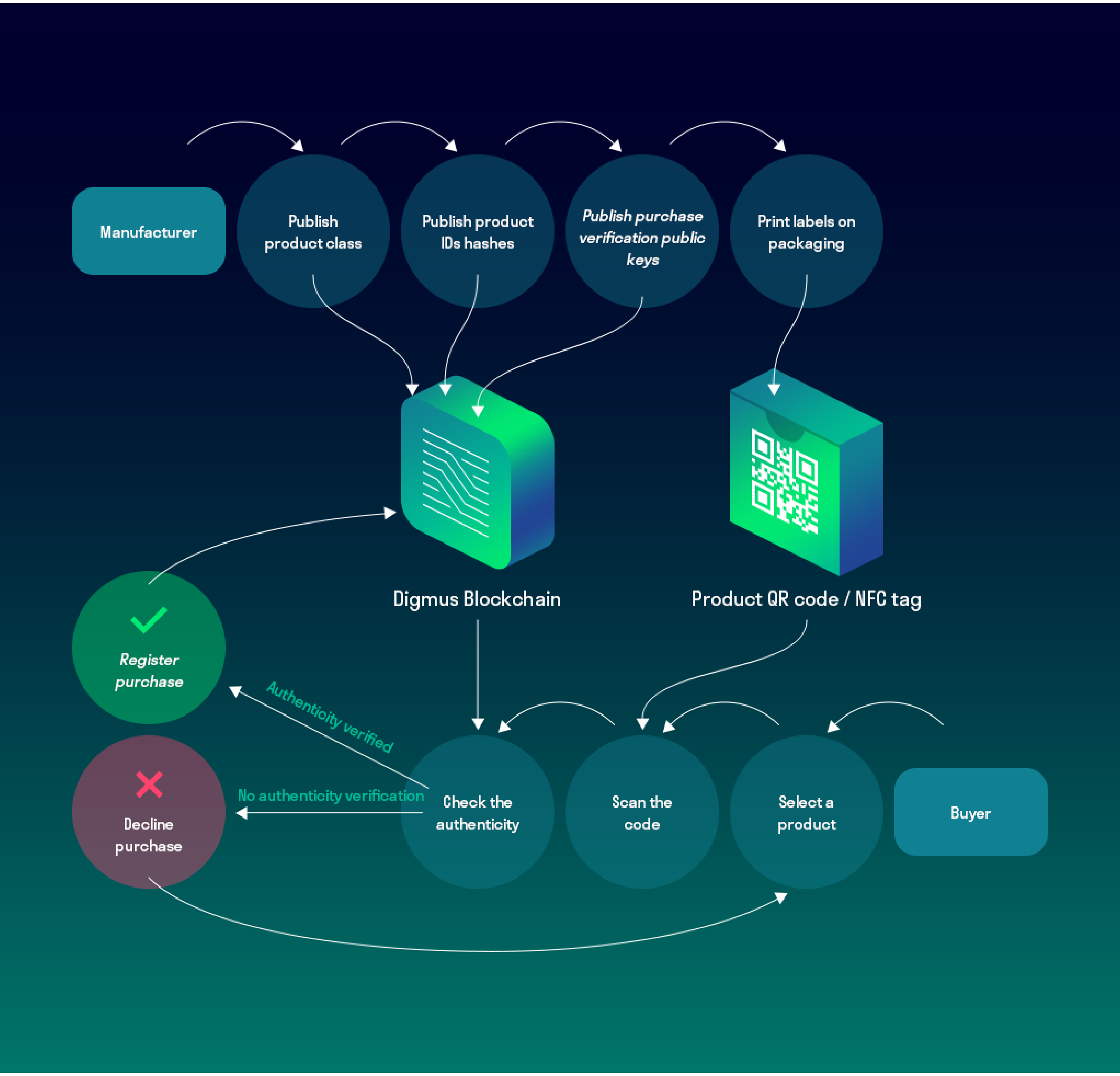


Fig. 2. Digmus dataflow diagram

Roadmap

This roadmap assumes that US$1 million is collected for the ICO (Initial Coin Offering).An amount less than this will significantly decrease the speed at which partners are attracted, as well as put the beta-version implementation date for blockchain and SAP integration behind schedule. While an amount over this will not significantly affect development speed, it will allow for more active system promotion, increasing the quantity of partners. Based on that, soft cap for the ICO will be set at 1650 ETH.

NOV 2017	ICO + Product prototype using a centralized database
JAN 2018	Test launch with partners
JUN 2018	Blockchain-based beta version and issuing of GEN currency
SEP 2018	Full integration for certain product categories for partners
FEB 2019	100,000 product units are being registered in the system monthly. SAP integration
SEP 2019	100 partners use our system
SEP 2020	Number of partners using our system increases to 200. 4 million product units are registered in the system monthly. Blockchain is updated for better scaling
SEP 2021	300 partners. 30 million product units being registered a month

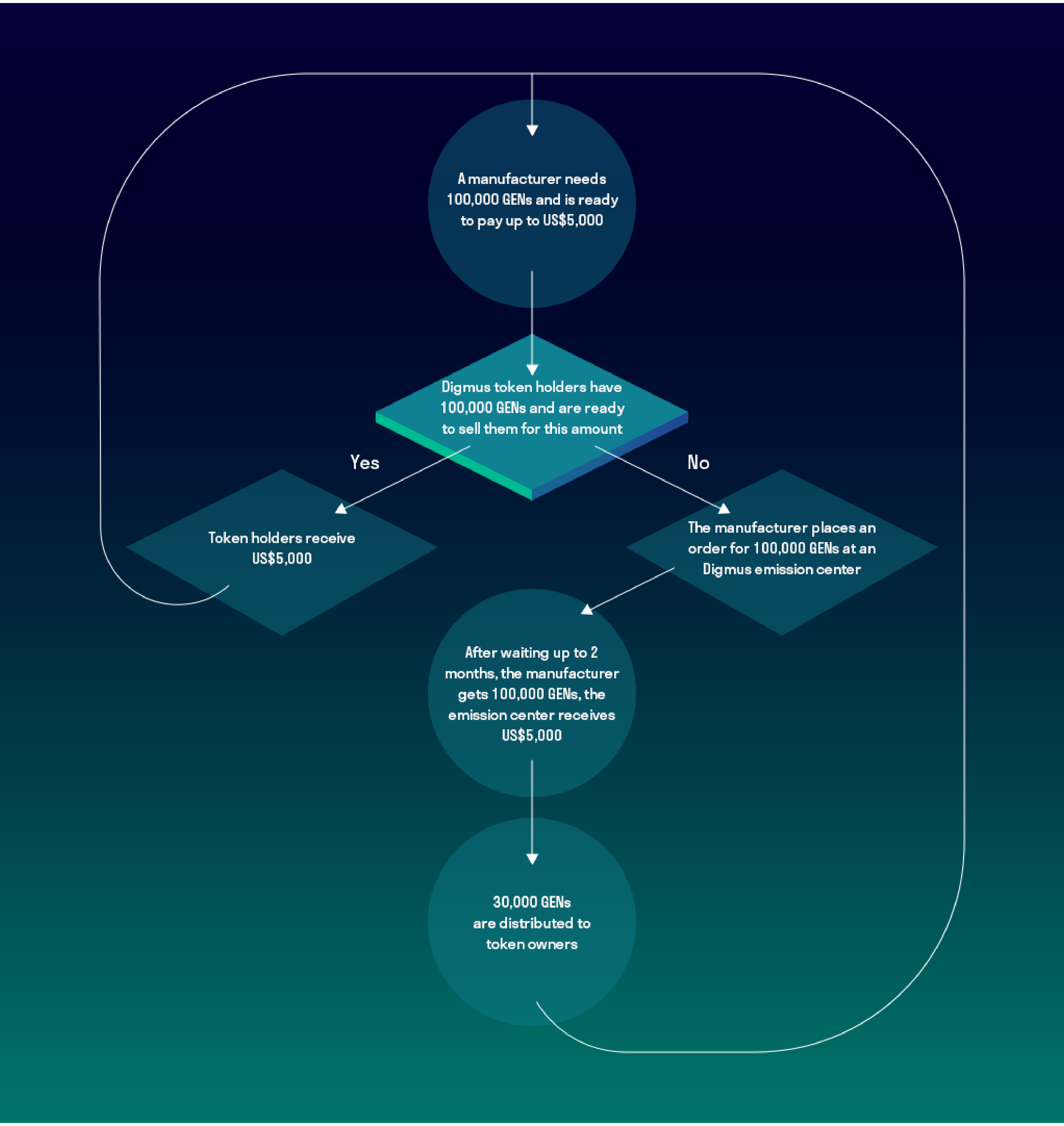
ICO details

For the ICO we will be selling Digmus tokens (DGM). The total amount of such tokens issued will be 10,000,000, with 6,700,000 being up for sale, 1,300,000 being divided between the team and initial investors, and 2,000,000 more being stored in the Digmus development fund. All unsold tokens will be "burned" (destroyed), as well as a proportional share of 3,300,000 tokens that will never be for sale. For example, if the total amount of Digmus tokens sold is 3,350,000, then the development fund will receive 1,000,000 tokens, with the team and investors share equal to a combined 650,000 tokens. Thus, under any scenario, ICO and pre-ICO participants will hold a 67% share of Digmus tokens.

Digmus tokens represent a share in the Digmus currency (GEN) emission. In the case of any such currency emission, the GEN balance of token owners will be increased in proportion to their share of DGM tokens. The emission will be managed in such a way as to insure a hard price cap for GEN coins.

GEN coins will be acquirable either on the exchange from token owners, or through a direct order from Digmus at a cost of $0.05 per GEN. Ordered tokens will be issued once every 2 months. At that time, token owners will receive 30% of the issued coins in proportion to the number of tokens they own, with the right to sell them at any cost they choose. This means the total amount of coins issued will be equal to 1.3X, where X is the number of coins manufacturers placed an order for.

A scenario for this process is shown in Fig. 3.



A manufacturer needs 100,000 GENs and is ready to pay up to US$5,000
Digmus token holders have 100,000 GENs and are ready to sell them for this amount
Yes
No
Token holders receive US$5,000
The manufacturer places an order for 100,000 GENs at an Digmus emission center
After waiting up to 2 months, the manufacturer gets 100,000 GENs, the emission center receives US$5,000
30,000 GENs are distributed to token owners

Fig. 3. GEN Emission in Digmus

This insures stable transaction costs for manufacturers, as well as being a way for token owners to make a profit selling GENs on the exchange.

Legislation and Risks

DGM tokens are not considered to be securities. Citizens of the USA, Canada and Singapore cannot be members of this ICO.

No Right of Control is Granted

Owning DGM tokens does not confer the right to control Digmus operations, nor does it confer ownership of a share, or property of Digmus. Owning DGM tokens does not grant the right to participate in decisions made by Digmus.

Profit is Not Guaranteed

Every and all calculations in this document are made for demonstration purposes only, and are not a guarantee that such results will, in fact, be achieved.

Legal Regulations

Blockchain technologies are being monitored and controlled by different agencies throughout the world. There is the possibility of DGM tokens being affected by their requests and/or actions such as, but not limited to, restrictions on ownership or use of digital tokens. Such circumstances in the future may alter or limit DGM token functionality, or constrain the DGM token exchange.

Investment

DGM tokens are not an official investment with legal power. The goals stated in this document may be subject to change, due to unforeseen circumstances. We plan to put all our efforts into achieving the described goals. All persons and parties participating in the DGM token trade accept the associated risks.

Risk of Insufficient System Popularity

Though one should not regard DGM tokens as an investment, their value may increase over time. It might, however, decrease, if Digmus is not in use by a sufficient number of manufacturers.

Potential for Losses

Funds collected during the ICO are not insured. In case of loss, there is no private or public insurer to respond to claims.

Risk of Failure

There is a possibility that, due to various circumstances such as, but not limited to, failed business agreements or unsuccessful marketing strategies, Digmus will not achieve its desired success.