Digital Currency DICE

Conceptual Design

Revision 1, *August – September, 2017*

Contents

1 Introduction

The rise of the cryptocurrencies in the past few years led to increased freedom and new ways to trade, generate and hold equity, and raise funds for business. The last one in its ICO form is quickly becoming a popular choice for seed fundraising in hi-tech start-ups. Cryptocurrencies however extensively suffer from some inefficiencies when it comes to raising funding for companies whose product has more physical nature such as robotics or other type of manufacturing in general. To make it worse, launching an ICO campaign has already become very expensive process for most early stage companies. The problems come from the fact that cryptocurrencies mostly rely on proof of work while for an early-stage company proof of ownership is a much more suitable choice since the nature of offering is almost exclusively in share equity. Hence only a few non-IT/non-Fintech companies have managed to adapt the cryptocurrency model and turn it into a successful ICO, while the traditional Angel/VC way is still more prevalent with such companies. In addition to that other problems mainly stemming from the complexity how modern cryptocurrencies work, limits many businesses from actively using them for fundraising.

This white paper outlines a new simple model, which is not based on traditional block-chain principles, but retains the benefits of cryptocurrencies, and is also bent in a certain way more toward traditional money, while at the same time offering unique benefits.

The proposed model is for a simple global decentralised self-controlling system for financial transactions.

2 Overview

The core element in the new model is called **DICE** (**DI**gital **CE**rtificate). DICE is a sequence of 1024 bits which conform to a certain set of rules.

Valid DICE units can be stored and later exchanged for physical goods, services, or digital content in a process called **Trading**.

The process of creating new DICE units is called **Mining**, in which computing power is used to generate a block of 1024 bits which can be considered as a valid DICE.

DICE economy is not based on block-chain. Instead, it consists of small clusters of **Miners** gathered around entities called **Operators** - IT hubs whose purpose is to perform validation of DICE units, and to maintain database of DICE units associated with the particular operator.

Any type of entity can be an operator in the global DICE economy.

Examples may include all business or non-business organisations, family, or even a single individual.

Operators are considered as limited trust parties (*only within the scope of DICE associated with the operator*), and all other users are considered as untrustworthy parties.

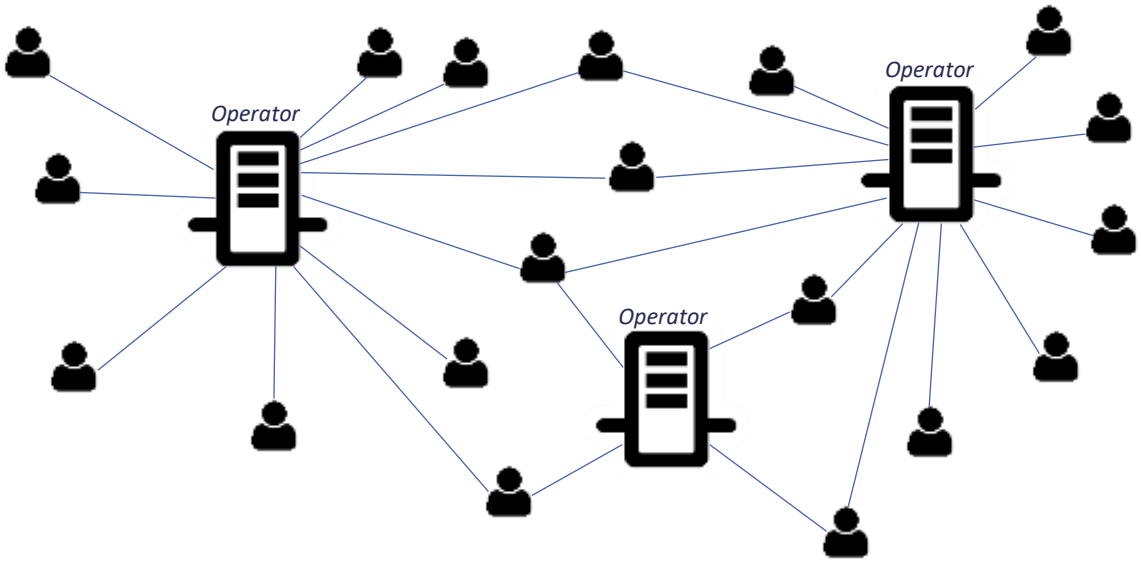
Every DICE unit is associated with only one operator on whose behalf it has been mined. The unit itself however, is valid in the global economy regardless of which operator it is associated with.

Newly mined DICE are initially owned by the miner who has mined them, and their value is added to the capitalisation of the operator on whose behalf they have been mined.

Therefore it is in operator's own interest to incentivise having as many as possible DICE mined and circulating in the economy, and associated with the operator.

Every individual can perform as a miner (optionally), and can mine for more than one operator as well.

Operators are completely independent from each other, but DICE units are global.

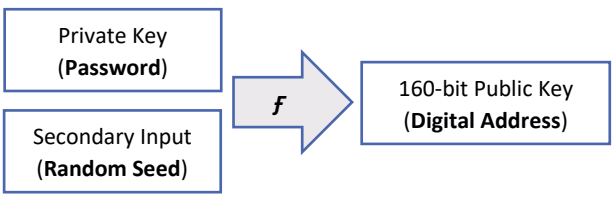


3 Digital Address

Digital signature is a sequence of bits, used to identify whether someone is the one they claim to be. DICE authentication is handled by asymmetric encryption [1] of all messages between users and operators.

Every miner or operator has their own pair of keys - public key and private key. The public key is what the entire network knows, and the private key is what only the miner or the operator knows.

During initial registration of the key pair, the user chooses a password which is private. That private password is then used to generate a 160-bit public key, which serves as personal address and identity in the DICE economy.



Data encrypted with the user's public key, can only be decrypted by knowing the private key, i.e. only the user alone can do that.

Therefore a network peer who initiates communication with another peer, always encrypts outgoing messages using the receiver's public key (i.e. personal address), and will be receiving all incoming messages encrypted using the own public key.

Whenever necessary, a DICE digital address can be represented as 40 hexadecimal characters grouped in eight 5-digit blocks for clarity:

XXXXX – XXXXX – XXXXX – XXXXX – XXXXX – XXXXX – XXXXX – XXXXX

4 Structure of DICE Unit

DICE unit is a binary block of 1024 bits (128 bytes) structured as below:

bit 1023 … bit 0864	Constant	**160-bit Operator Address**
bit 0863 … bit 0704	Constant	**160-bit Miner Address**
bit 0703 … bit 0696	Constant	**8-bit Threshold Level**
bit 0695 … bit 0664	Variable	**32-bit Timestamp**
bit 0663 … bit 0000	Variable	**664-bit Payload**

The first four fields form 360-bit "***DICE Header***" which is sent to the operator during validation claims.

Fields "***Operator***" and "***Miner***" are always unchanged in the scope of a particular miner who is mining on behalf of a particular operator.

The 8-bit "***Threshold Level***" field is set by the operator at the moment of generation of the DICE, and defines a minimum number of bits required to satisfy the validation condition for a newly mined unit.

The 32-bit field "***Timestamp***" is automatically filled at the moment of generation of the DICE with real-time current time and date expressed in Swatch Internet Time [2] @beats accumulatively passed since 00:00:00 on January 1st, 2001. One @beat is a period of time equivalent to 1/1000 of a day.

The data contained in the fifth field "***Payload***" is freely adjustable by the miner during the process of mining. This is the "secret" data of which the operator is not aware.

Units are distributed in their raw form (i.e. the original 1024-bit block which produces a hash conforming to the needed validation condition), however the operator who validates the DICE knows only the header and the hash from the payload, but not the original payload data.

A DICE unit can exist in the form of digital content (binary file, hex file, QR code), or as a physical printed note (QR code or text).

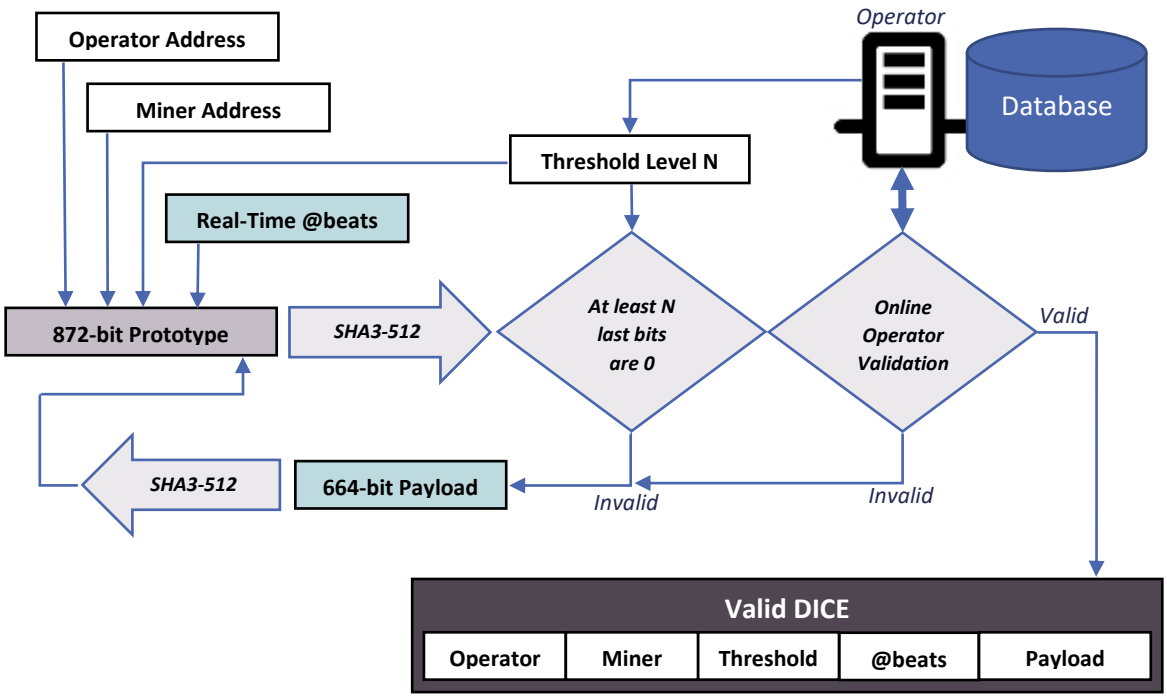
5 Mining

The process of mining generates new DICE units. Newly mined units are initially owned by the miner who has produced them. The miner can then exchange them for physical goods, services, digital content, other currencies, or other DICE units.

When generating a valid DICE unit, the goal is to have such 1024-bit block of data consisting of the fields defined in the DICE structure, so when SHA3-512 [3] is executed on the DICE payload, and the resulting 512-bit output is then added to the original DICE header, a new hash produced from the thus built 872-bit "prototype" block will have a certain number or more of its least significant bits, all equal to 0.

Therefore a miner's task is to produce a 664-bit "Payload" in a certain moment of time "Timestamp" in order to achieve successful hashing of the entire 1024-bit proposed data block, and then to have that hash confirmed by the operator.

The overall mining process is schematically displayed below:



From the shown diagram it can be seen that a proposed new DICE unit is formed from constant Operator and Miner addresses, a constant Threshold set by the operator, a real-time Timestamp, and a hash from Payload generated by the miner.

The initial verification is performed locally by checking whether the result of SHA3-512 function has N or more trailing bits 0. If this condition is not satisfied, the process repeats with a new Payload value.

In case the condition for minimum N trailing bits 0 is satisfied, the resulting 872-bit "Prototype" is sent to the operator for validation.

The operator would normally not honour ownership claims for new DICE units with mining timestamp older than a pre-set limit. The timestamp could also be used by the operator in the valuation process to incentivise mining of DICE units within a specified period of time.

For details about the messages exchanged during the process refer to chapter *"**Message Protocol**"*.

6 Threshold Level

In order for an operator to accept a new DICE unit, the first condition is that the hash of the DICE unit needs have a certain minimum number of its least significant bits all set to zero.

This value, together with the DICE timestamp, determine the value of a DICE unit.

As of late year 2017 the default threshold level is $\boldsymbol{N = 44}$

DICE defines that a unit can valued only within the (**N-10 … N+10)** range.

Therefore for ***N = 44*** the absolute acceptable minimum threshold would be $\boldsymbol{N_{min} = 34}$, and the absolute maximum would be $\boldsymbol{N_{max} = 54}$.

There is no defined maximum, however since the threshold level is stored in 8-bit space, the theoretical maximum threshold would be 256 (stored as value 0 in the field).

Operators set individual threshold level according to the stage they are in, and to the mining niche they are targeting. Too low threshold will result in mining of large quantity low-value DICE units, while too high threshold will render difficult and power hungry mining of a small quantity highly valued DICE units.

7 Unit Valuation

The value of a DICE unit is calculated as:

$$v = (k * 2^{(b-z)} * 2^{(z-N)}) \wedge 2^{(Nmax)}$$

Where ***v*** is the value of the unit, ***b*** is the number of trailing zero bits in the hash, and ***z*** is the threshold permanently level set in the DICE unit.

N is the default threshold, N_{min} and N_{max} are respectively the N-10 and N+10 limiting values.

The parameter ***k*** is a correction factor individually set by the operator for units with specific timestamps. The default value for ***k*** in all non-exclusive cases, is 1.

In order a DICE unit to be considered valid, it needs to satisfy the condition $\boldsymbol{b \geq z \geq Nmin}$

The case $\boldsymbol{b > Nmax}$ produces a valid unit, but its value is capped at $\mathbf{2}^{(Nmax)}$.

Therefore a unit generated at default threshold level N, and having exactly N trailing zero bits, will have value of one DICE.

It can be seen that since units are generated in a binary way, the valuation formula always generates result which is a number in power of 2, for units with value 1, or greater.

The same formula can also be expressed in a different form to simplify the calculation of units with value less than 1 (i.e. threshold level z<N):

$$v = \left(k * \frac{2^{(b-z)}}{2^{(N-z)}}\right) \Lambda\, 2^{(Nmax)}$$

By applying the absolute minimum acceptable threshold values N_{min} and N_{max}, the formula shows that the smallest possible fraction of a DICE unit is $\frac{\mathbf{1}}{\mathbf{1024}}$, and the highest single DICE value is **1024**.

Approximately $8.8*10^{12}$ hashes are required to reach the theoretical probability of 50% for producing a valid unit of one DICE. Assuming a typical single mining system has speed of 10^{10} hash/s, then mining of one DICE will need on average around 15 minutes computational work done by the mining system.

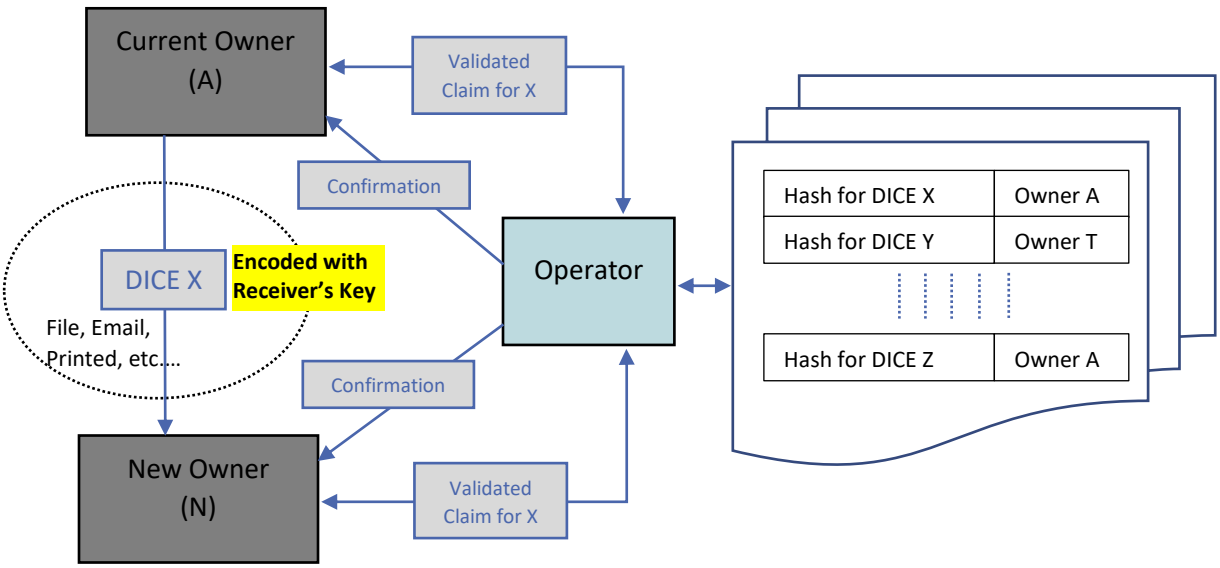
8 Trading

Trading in DICE economy is based on ownership claims rather than active transactions. No ledger of transactions exists anywhere in the network. The process can be described in a few generalised steps:

1. Current owner provides DICE units to the new owner. This could be in the form of digital content (binary file, email), or physical form (paper note, file storage device).
   Units are encoded with the new owner's public key.
2. Current owner places a claim for new ownership to the operator who handles the particular DICE unit used in the trade, providing the hash of the unit.
3. New owner verifies the DICE, and also places a claim for new ownership to the operator of the DICE, providing the hash of the supplied unit.
4. Operator verifies the validity of the unit, and the two claims, and stores in its private database the address of the new owner as registered owner of the DICE with the provided hash.
5. Operator sends response message to both parties informing them about the change of ownership of the unit.

This is repeated for every DICE unit involved in the trade.

The process for one unit can be visualised in the following diagram:



It can be seen that a successful transfer of ownership can only occur when the following conditions are met:

1. The current and the new owner both possess the actual DICE unit in its raw form.
2. The unit is a valid DICE unit.
3. The unit is known to the operator.
4. The operator recognises the current owner as legal owner of the unit.
5. The current and the new owner have both informed the operator about the upcoming change of ownership of the DICE unit providing matching hash generated from the DICE.

It is important to note that between trading parties DICE units are exchanged in their raw form, while claims put to the operator are only made using the hash of those units.

9 Ownerless DICE

Under certain circumstances an owner of a DICE unit may decide to release it on paper in form similar to a bank note. In such case the new owner of the unit is not known in advance until an ownership claim is put in front of the operator.

To achieve this goal, the current owner needs to release the DICE from ownership, which in the operator's database invalidates the unit and marks it as ownerless. From this point further the operator will assign ownership to the DICE to the first valid claim that comes with it.

In addition to that, more than one copy of the same ownerless DICE may exist. For example, the original owner may have released a number of copies of the same DICE for the first who makes a valid claim of ownership.

Ownerless DICE are distributed in the form of the full unencrypted 1024-bit data block. They hold no value until a successful claim of new ownership is confirmed by the operator.

Trade with ownerless DICE is less secure and a new owner always needs to check with the operator if the actual traded DICE is in fact ownerless at the time of the exchange.

10 The Operator Role

Every DICE unit is associated with a business entity called "Operator" who serves as guarantor over the validity of the DICE units associated with the operator (only), and also serves as executing authority in ownership claims for associated DICE units.

The operator keeps a database with hash for every known associated DICE, and the digital address of its current owner, and reacts on validation messages and claims of ownership sent from external users.

If an operator happen to seize operation, that would not affect the DICE economy beyond the units associated with that single operator only.

Operator does not keep raw DICE units in its database, but only the prototypes.

The DICE economy operates on fee-free trade. Miners have the intrinsic motivation to generate units which then will be used in return for goods or services. The motivation for an operator comes from the fact that all DICE mined on its behalf can be used as collateral in future deals. Therefore an operator performs its role in return for the miner efforts to generate DICE on its behalf.

11 Message Protocol

Users can send messages to operators during trade operations to enquire about the validity and value of DICE units, or to claim ownership over DICE units.

During a claim both user parties need to provide the new owner address. If the claim has been successful, the response will be stating the new owner's address as "***Current Owner***". For newly mined DICE the claim is made by the miner only.

In order to get the operator to accept any claim, a challenge is first given to the claimer. The challenge aims to prove that the claimer has the original data which produces the claimed hash.

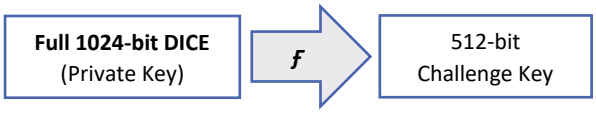
The challenge uses asymmetric encryption. [1] The original 1024-bit DICE block is known to the claimer only, and is considered as private key. Using the DICE, a separate 512-bit public key ("***Challenge Key***") is generated and supplied to the operator.

The operator generates “a secret message” in the form of a random 512-bit block, which is then encoded with the challenge key. The encoded message is returned back to the claimer, who can decode it only if he or she possess the original DICE block.

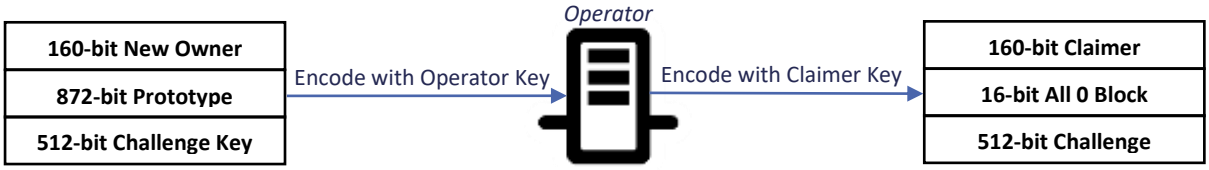
The operator will expect to receive a new claim with the originally provided secret message in its decoded form. Only after comparing the response with the actual content of the challenge, the operator can assume that the claimer does indeed have the claimed DICE block.

The operator will not respond to any messages containing invalid information, or having invalid length.

Step 1 (claimer generates challenge key)

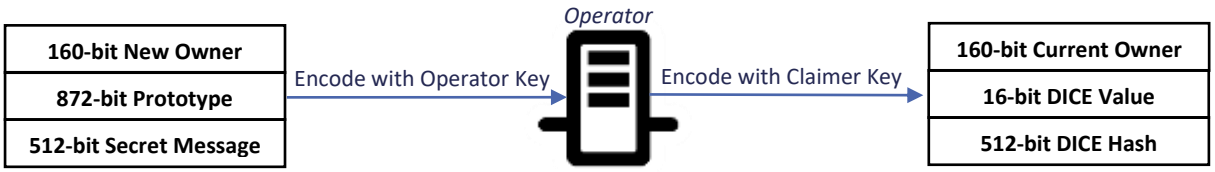


Step 2 (initial claim → receive challenge)



Step 3 (claimer decodes operator challenge)

Step 4 (respond to challenge → confirmation from operator)



The 16-bit “***DICE Value***” field holds the value of the item in bits 14…0, and bit 15 is ***1/x*** flag.

If the claimer passes the challenge:

1. If the operator has no record of the DICE hash in the claim, and the field “New Owner” contains data (not all 0), a new record in the database is created, and the address provided in “New Owner” is set as owner of the unit. This is the case of newly mined DICE.

2. If the operator has no record of the DICE hash in the claim, and the field “New Owner” is all 0, it is considered as validation/valuation claim only, and no further action is taken by the operator.
    a. The operator is aware of the DICE: the field “Current Owner” contains a valid address.
    b. This is DICE unknown to the operator: the field “Current Owner” contains all 0.

3. If the claimed DICE hash is already known to the operator, and the field “New Owner” contains valid data (not all 0), a separate claim about the same DICE, sent by the new owner is expected to conclude the trade. The new owner becomes registered owner of the unit.

4. If the claimed DICE hash is already known to the operator, and the field “New Owner” contains all 0, the DICE is removed from the operator’s database and released as ownerless.

12 Wallets

DICE does not requires special type of digital wallets.

A “wallet” can take any form of storage where units are kept. That could be for example a USB flash drive (for files), an inbox (for emails), or a physical wallet (for printed notes).

In any case a valid DICE unit is considered only a full 1024-bit block which can be validated successfully with the associated operator.

13 Potential Security Issues

There are several cases in which a malicious hacker could cause damage in a local operator’s cluster.

1. **Hijacking communication between any of the trading parties and the operator.**
   The only useful outcome in this case would be if the communication is hijacked before encoding, or the hacker also knows the private key of the hijacked party.

2. **Hijacking communication between two parties in a deal.**
   This could potentially supply the hacker with a copy of the DICE units used in the deal, assuming the communication is being hijacked before encryption, or the hacker knows the receiver’s private key. Acquiring a copy of the DICE would also require the hacker to modify the claim sent from the current owner to the operator, and insert the own digital address as a new owner of the unit. The hacker will then need to generate a fake claim to the operator for the ownership of the DICE.

3. **Acquiring a copy of ownerless DICE.**
   Since ownerless DICE have no current owner, the hacker would be immediately able to claim ownership over the unit.

4. **Gaining access over an operator's database**
   Such case would give a chance to the hacker to damage information of ownership of potentially all DICE units associated with the operator, however since there is no information stored in the operator about the actual DICE units (only their hashes), the hacker would not be able to gain any value for himself or herself.

5. **Gaining full control over an operator**
   The communication between an individual operator and other parties may be severed or corrupted. No personal gains for the hacker can be achieved in this type of attack.

In a corner case after many trade iterations, it can be assumed that eventually every user will possess a copy of every DICE associated with the operator. At that point the operator's database will remain the authority identifying the ownership of every DICE. Therefore a malicious hacker could be able to modify the database to assume ownership over units in it.

Compromising operator's security can potentially have damaging impact on the local cluster, but not on the entire DICE economy.

14 Initial Dice Offering (IDO)

The Initial Dice Offering can provide an easy way to a business to raise funds for its operation. In comparison with any other methods of fundraising such as ICO or IPO, expenses associated with IDO are miniscule and mostly come down to the cost of the operator's server equipment and supporting software.

IDO is the way for a new operator to enter the DICE economy.

When a business initially executes IDO and becomes operator, there are yet no existing DICE associated with the new operator. The business needs to encourage users to start mining thus generating value. Every new mined DICE that enters the economy, is added to the valuation of the operator. Then by paying in DICE associated with the operator, a miner can acquire certain equity in the business, production, or service.

By using the creation timestamp in DICE, an operator may define premium-value units to be mined within specified period.

15 Summary

• Self-supporting decentralised infrastructure based on clusters of individual users and small business entities.

• Model operating on static **Proof of Ownership** and claim of new ownership, and unaffected by multiple copies or double spending.

• Intrinsic tolerance toward paper and unencrypted tokens.

• Introduction of “Limited Trust Parties” with reduced scope for trustworthiness.

• Completely fee-free while all parties are still incentivised.

• Every miner is inherently an investor too in a business of own choice.

• Mining becomes the main value-generating asset for a new business.

16 References

[**1**] https://en.wikipedia.org/wiki/Public-key_cryptography

[**2**] https://en.wikipedia.org/wiki/Swatch_Internet_Time

[**3**] https://en.wikipedia.org/wiki/SHA-3