ZenDao

Whitepaper

Disclaimer:

This draft Whitepaper is for the information and discussion purposes and is subject to further adjustments.

No part of this document has a legally binding nature.

TABLE OF CONTENTS

TABLE OF CONTENTS

ABSTRACT

ZenDao, a decentralized platform developed on the Metaverse Blockchain, seeks to utilize the solutions provided by Blockchain technology in order to create a digital representation of the real-world collectibles on Blockchain and establish an unalterable digital provenance and ownership transfer channel.

By tokenizing collectibles, ZenDao aims to link physical assets with their digital representation on Blockchain in order to gain advantages related to the Blockchain technology, such as security, transparency, speed and ease of transacting. While implementing innovative tools, such as the smart script secured trade (“SSST”) and unique authentication mechanism, ZenDao unleashes the high value of the full chronicle of the collectibles’ life cycle, hence allowing history to speak for itself and augmenting the assets’ economic value.

INTRODUCTION

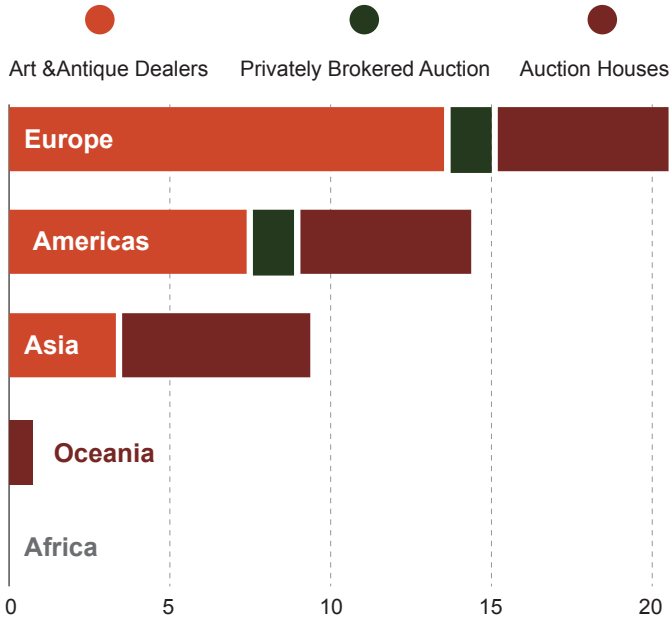
The global art and collectibles market (hereinafter “the market”) has been flourishing at an incredibly high speed during last decades (26% growth in the past ten years). The market has been building momentum over the past couple years and is ripe for disruption. Recent survey findings reveal that the volume of global sales in 2016 was $45 billion, a 1.7 percent increase compared to 2015.[1] Currently, the three largest markets for arts and collectibles are the United States, the United Kingdom and China.[2]

According to the Art Market Report, the market will continue to grow by 25 percent each year.[3] As the market continues to see a strong demand for high quality collectibles, increased wealth allocation in the market in the next 10 years is expected.[4] The survey conducted by Deloitte reveals that the growing percentage of global wealth advisors see a significant expansion in capital allocation toward collectibles as well as in the demand for servicing this class of assets.[5]

FIGURE 1

WORLD ART MARKET TOTAL SALES BY CONTINENT IN 2016

Such assets collectors’ motivation is driven not only by the emotional benefit of collecting, but is associated with the potential gains from capital appreciation and investing in an asset class, which represents a stable store of value. While 72 percent of the collectors declare that they buy art for passion with an investment view, 82 percent of art and collectibles professionals have stated that this is the main reason why also their clients purchase collectibles.[6]

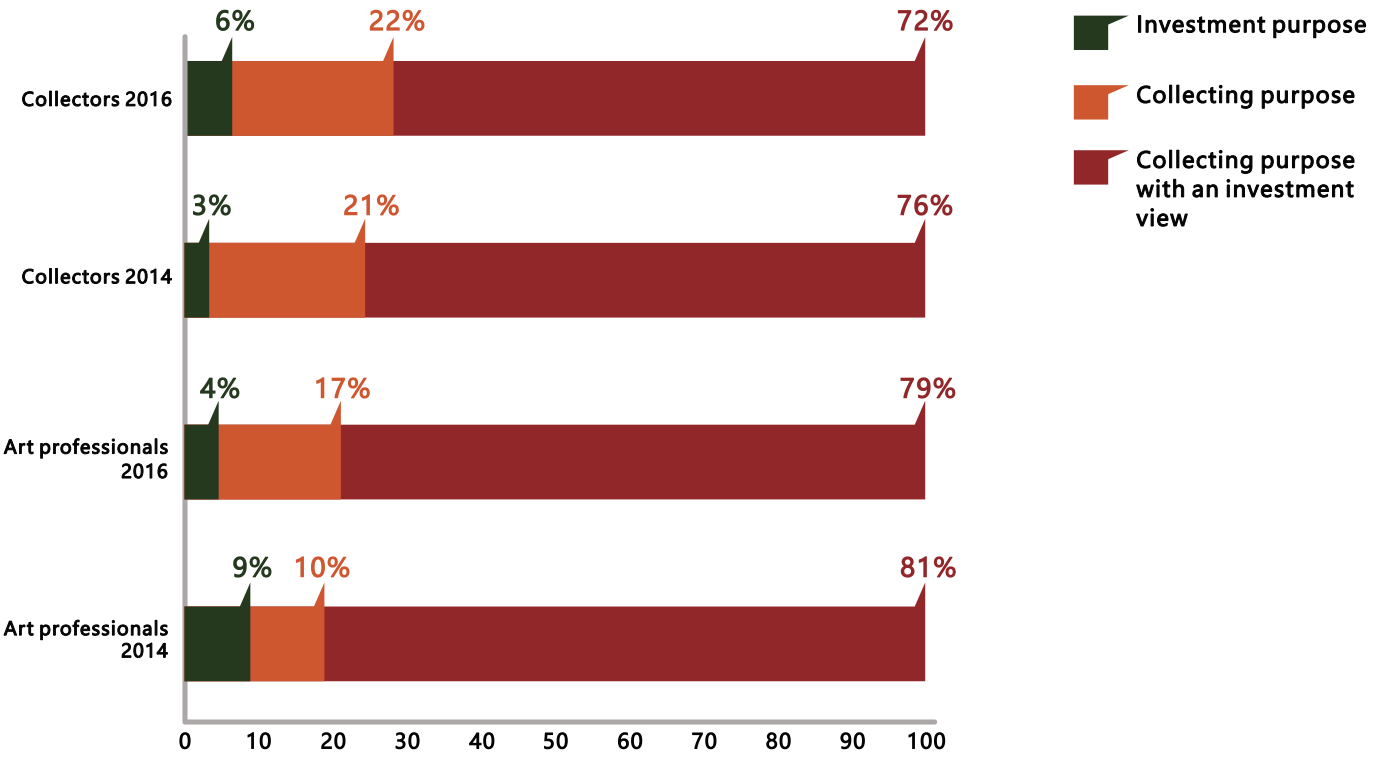


Maastricht University Graphic
Sources:artnet,Auction Houses,Orbis & MACCH Global Dealer Survey 2017

[1] TEFAF, Art Market Report 2017 (2017), 12.
[2] SAATCHI ART, Invest in Art: 2017 Report (2017) 11.
[3] TEFAF, Art Market Report 2015 (2015), 5. See also K Esterluss, The art of selling art: Young artists navigate the digital world (2015).
[4] Deloitte, Art and Finance Report 2016 (2016) 15.
[5] Deloitte, Art and Finance Report 2016 (2016) 15-16.
[6] Deloitte, Art and Finance Report 2016 (2016) 17.

FIGURE 2

Why are you/your clients buying art?



Source: Deloitte Luxembourg & ArtTactic Art & Finance Report 2016

An additional factor influencing the market is the fact that the supply of the market of collectibles is not elastic. Consequently, the price for collectibles considerably increases with each rise in demand.[7] Although collectibles market has its own specificities, the exchange is still based on the fundamental economic principles of supply and demand. As a result, the value of the collectibles can only increase over time. The value of those assets does not fluctuate in the short run and can provide a higher rate of return on investment than the stock market in the medium to long run.[8]

Yet, the collectibles market faces some major problems that need to be properly addressed. The market has been static for the past 300 years and is ready for disruption. The majority of the professionals (73%) and collectors (68%) agree that the innovations, such as applications of Blockchain technology, will play a critical role in the market as this technology will transform the art and collectibles industry.[9] This whitepaper describes the core problems that the market faces and highlights ZenDao' s plans to deliver innovative solutions to these challenges and fundamentally transform the art and collectibles industry.

[7] E Trojovska and P Trojovsky, Current Economics of the Art Market (2013) 246.
[8] SAATCHI ART, Invest in Art: 2017 Report (2017) 12.
[9] Deloitte, Art and Finance Report 2016 (2016) 17.

CURRENT MARKET CHALLENGES

Lack of Provenance

Provenance-related issues constitute a considerable threat to the market. About 75% of the market stakeholders agree that the authenticity and lack of provenance tracking mechanisms represent the biggest threats to credibility and trust in the market.[10] This is an important point to consider as the value of collectibles lies in where they come from, how they were used, which culture they belong to. As soon as they are treated as regular objects, they lose their additional value and they do not become any different to the regular objects we use in our daily life.

ZenDao believes that all the provenance information must be auditable, public and verifiable. Without accurate and trustworthy information on the provenance of the collectible, inaccuracy and incompleteness will negatively affect the asset valuation process as well as the trust of the market participants in the market and other stakeholders. This issue is easily illustrated by the frequent disputes arising in the collectibles market. These disputes generally fall within one of three categories: disputes concerning ownership, disputes concerning authenticity and disputes concerning value. The provenance of an art work is critical in each of those potential areas of dispute. By recording critical ownership and provenance information in an immutable Blockchain, the probability of errors and omissions is considerably reduced (if not inexistent). Furthermore, this new technology enhances the due diligence process, the quality of the information provided and facilitates compliance for the entire Art and Collectibles industry. ZenDao believes that establishing an unalterable digital proof of provenance on the Metaverse Blockchain can provide a sustainable solution that protects the interest of all stakeholders in the market.

Liquidity

One of the major issues plaguing the collectibles market is illiquidity. There are several causes for the illiquidity of the art and collectibles market. Firstly, unlike financial markets, the number of tradable collectibles is much lower than outstanding securities. Second, they cannot be traded in real time. Finally, the ownership on the single collectible and art pieces is not divisible.

As a consequence, expensive art pieces or collectibles cannot be converted into smaller and more liquid tradable units, which makes the barriers to entry relatively high. The traditional market is starting showing its limits. Market status quo is not fair and fully transparent as investors and owners of the collectibles need different intermediaries, mainly auction houses, to connect with each other and trade in return for the high service fees. This creates a volatile market environment, where market participants solely depend on the intermediaries. The art owners, collectors and galleries suffer reduced access to capital. Raising funds without losing ownership of their assets is impossible in the traditional art market.

ZenDao will implement solutions powered by the Metaverse Blockchain in order to change the existing standards on the market while reducing transaction fees, introducing transparency and creating new channels to enter the market at a lower cost.

[10] Ibid, 20.

Pure Valuation Methods

The economic value of collectible mainly depends on its intrinsic value, yet its value is inevitably affected by many factors. The authenticity of the art work, consumers' demands and scarcity has a direct impact on the market price. Currently, the price of collectibles is greatly affected by auction houses and the quality of their service. The credibility of the auction house plays an important role in determination of price of collectibles. On the other hand, this centralized method has significant flows as the probability of fake auctions is high and these auction houses can artificially increase the price of the collectibles. This is the striking problem in the current market as any pricing method loses its value in face of fakes, damages the confidence of participants in the market and seriously affects the healthy development of the market.[11] With ZenDao, the decentralized auction mechanism will enable the market participants to interact in an efficient, low cost environment and the market itself to determine the price of the collectible.

Forgery

Fraud represents a well-known issue of the international market of art and collectibles and one of the biggest threats to credibility and trust of the market. Since collectibles became a popular form of investment, they have been forged and faked while cheating an untrained eye. In many cases, the documents that are supposed to support the authenticity of the collectible are also forged. With the evolution of technology, such as the Internet, online auction sites, and the ease of international distribution, the number of forgeries has steeply increased. The main issue consists in detecting and proving the forgery as the market is large, complex, and diverse. Additionally, museum curators or collectors tend to avoid using legal means to protect themselves against fakes and inauthentic artwork as they are scared of the reputation loss. As a result, all the major stakeholders are hurt directly and indirectly: the artists who have created the piece of art, collectors who are being cheated when purchasing the forged works as well as the museums that use public or donated money to buy fraudulent works of art or works with a falsified provenance.

With the mechanisms currently in place, it is logistically impossible to monitor all of the transactions made by dealers, private collectors, and museums. Suspected forgeries are generally considered on a case-by-case basis, because they can usually be identified only by an expert in the field. ZenDao aims to address the market' s current weakness and apply the solution for identification of the real objects with secure authentication mechanism that utilizes Blockchain technology.

[11] A.N. Dvornayaad I.G. Knyazeva, Investment potential of the global art market (2013) 338.

ZENDAO AS A SOLUTION PROVIDER

The lack of information concerning the provenance of the collectibles, market illiquidity, pure valuation methods and the risk of forgery are the major challenges that can be detrimental to the interests of all stakeholders and to the healthy development of the market. By exploiting the solutions provided by Blockchain technology, ZenDao seeks to tackle the outlined problems and to revolutionize the current industry standards by bringing tangible improvements to the market.

ZenDao envisions achieving the established goals by implementing the following improvements:

Reliable store of provenance convenient and store of value

The tokenization of collectibles will enable ZenDao to link physical assets with their digital representation on the Blockchain in order to benefit from the advantages of this new technology, such as security, transparency, speed and ease of transacting as well as resistance to the system failure. Simultaneously, it will establish an unalterable and publicly traceable digital proof of provenance and proof of ownership transfer. ZenDao unleashes high value for collectors and art enthusiasts while providing insightful information on the collectibles' history and previous ownership, hence allowing history to speak for itself and augmenting the assets' economic value. The distributed ledger reliability will increase the value of the assets, while attracting investors, who will enjoy transparent and stable capital gains.

By allowing the collectibles to be converted and split into the multiple fractional digital assets, the full ownership or a small fraction of it can be sold to the market while the asset itself stays with the custodian that has a decentralized governance structure. The custodian is created and managed by the ZenDao Foundation. This provides the market participants with a trust organization, allows broader number of investors to participate in the market and reduces the costs of entry while reducing investment risk. Each token owner is given the full liberty over the tokens owned.

Increased liquidity

Currently, the market is plagued by high transaction costs and asymmetric information, which negatively impacts the liquidity of the entire industry. ZenDao aims to provide a cost efficient and decentralized way for the owners and investors to connect with each other and execute trade in real-time. By using Blockchain technology and integrating market resources to create a decentralized trading channel for collectibles, ZenDao aims to create a platform, where no trade, issuing or commission fees are applied. The provenance of each

collectible is fully transparent and searchable on the Metaverse Blockchain. Collectibles' issuance and delisting processes are simple. Furthermore, mobility of the asset value in the digital reality is maximized.

By creating a transparent, fair and open market and bypassing intermediation, ZenDao will transform the collectibles market. In ZenDao' s new reality, expensive and illiquid assets will be converted into smaller and more liquid tradable financial units, which will then be traded through a decentralized exchange. Investors will be able to diversify their risks by investing in a range of different assets, as opposed to having their funds concentrated in limited number of collectibles that are hard to sell. Meanwhile, collectibles' owners, collectors, museums and galleries will have a more convenient access to capital, allowing them to raise funds without losing ownership of their asset.

Fair valuation mechanism

By integrating a decentralized auction mechanism, the issuers of the tokens, which will enable to purchase shares of collectibles in the digital world, may offer those tokens to the buyers at a price commonly determined by the market. With decentralized auction mechanism embedded in the system, ZenDao allows the market participants to agree on the price of collectible in a transparent and competitive manner. Before, the opaque asset valuation standards greatly damaged the confidence of participants in the market. ZenDao will enable the market to derive the collectibles' price itself.

Stable market growth

ZenDao will apply a smart and decentralized inflation mechanism that would allow adjustments to be made without any central entities being involved in the process in order to balance the tokens' supply value and the value of the physical assets that back them. This would enable the market to grow in a persistent, predictable and stable manner, thus allowing the market stakeholders to enjoy more flexibility while mitigating risks.

ZENDAO AS A SOLUTION PROVIDER

HOW CAN BLOCKCHAIN TECHNOLOGY CONTRIBUTE

Blockchain, representing a shared and immutable ledger for recording the full history of transactions, fosters a new generation of transactional applications that establish trust, accountability and transparency. Having identified current challenges in the market, ZenDao aims at developing smooth solutions for complex problems by utilizing this technology. ZenDao sees public Blockchains as an engine to empower transparency and trust. It also believes that sharing value between different entities needs public Blockchain with longevity and sustainability potential. Thus, ZenDao platform will use Metaverse, a public Blockchain for smart properties and digital identities, in order to deliver its services.

Why Metaverse Blockchain

Currently, identity is left out at the protocol level, particularly in open public Blockchains. It is the missing link that allows the concept of digital assets on Blockchain to flourish and financial applications to play a role in a more inclusive digital banking and financial systems. Thus the value of having identity embedded at the protocol level is important because it allows building a verifiable function for applications built on top of Metaverse.[12] This aspect is especially important for ZenDao when choosing Metaverse Blockchain to deliver the services to the market. Within ZenDao platform, the functionality of the authentication mechanism is intertwined with the digital identity and asset ownership systems.

In Metaverse, an asset is a digital representation of a physical world asset and a smart property is how the asset interacts with humans. Essentially, Avatars (unique, deterministic, self-sovereign digital identities that do not rely on central entities or third parties to validate the identity) and smart properties will power all the decentralized applications on Metaverse.[13] As our lives become more digitalized, sovereign self-identities will be able to easily transact assets of any type and allow businesses and communities to empower themselves through many forms of digital payments where these different types of assets will drive us towards the Internet of Value.

Blockchain Technology Main Features

ZenDao is committed to transform the current market that faces some major challenges by implementing Blockchain solutions. In the following paragraphs, the main features of Blockchain are presented and will allow ZenDao to bring the efficiency and liquidity to the art market:

Decentralization

The data on the Blockchain is distributed and stored by the whole network nodes. There are no centralized management bodies. By applying this mechanism, the

[12] Viewfin, Metaverse: From Smart Properties, Avatars and Oracles to A New Virtual Society (2017) 6, available at: http://mvs.live/attachment/Metaverse-White-Paper(draft)-EN.pdf.

[13] Viewfin, Metaverse: From Smart Properties, Avatars and Oracles to A New Virtual Society (2017) 6-7, available at: http://mvs.live/attachment/Metaverse-White-Paper(draft)-EN.pdf.

immunity to data fraud and single point of failure are provided and the reliability of data storage is achieved.

P2P networking

Peer-to-peer networking on Blockchain solves the privacy-related problems common to the traditional centralized trade systems. Thanks to P2P network, the privacy is secured for the parties and this avoids the misuse of private information by the unauthorized parties.

Intelligent trading

On ZenDao platform, each collectible can easily be converted into the digital tokens (ZenDao Coins) on Metaverse Blockchain. Every single entry is secured in real-time and is non-reversibly stored on Blockchain. Based on the smart script mechanism encoded within ZenDao, the benefits of the involved parties are ensured by the decentralized system instead of the traditional structure that inevitably involves reliance on intermediaries.

ZENDAO KEY APPROACHES

CDP Authentication

Introducing CDP Authentication

Collectibles digitization process (“CDP”) authenticates collectables on the Metaverse Blockchain. Authenticating collectables proves the ownership of a collectible by generating the digital identities within the Blockchain. A hash function is applied for each new digitized identifying file. The hashes are recorded on the Blockchain along with the address of the identifying files that were uploaded into distributed storage and all this information is publicly available. The authentication of collectables via CDP is a decentralized process where no 3rd party is involved.

There are varieties of options for creating digital identifying files, for instance, scanning identification documents authorized by accreditation bodies, high resolution photographs from different angles illustrating in details the collectible and its features, microscope visuals of certain parts, or what is most recommended, 3D scanning technology, which analyses a real-world object to collect data on its shape and its appearance with its original color, with the accuracy of 0.03mm which is not detectible by visual observation.

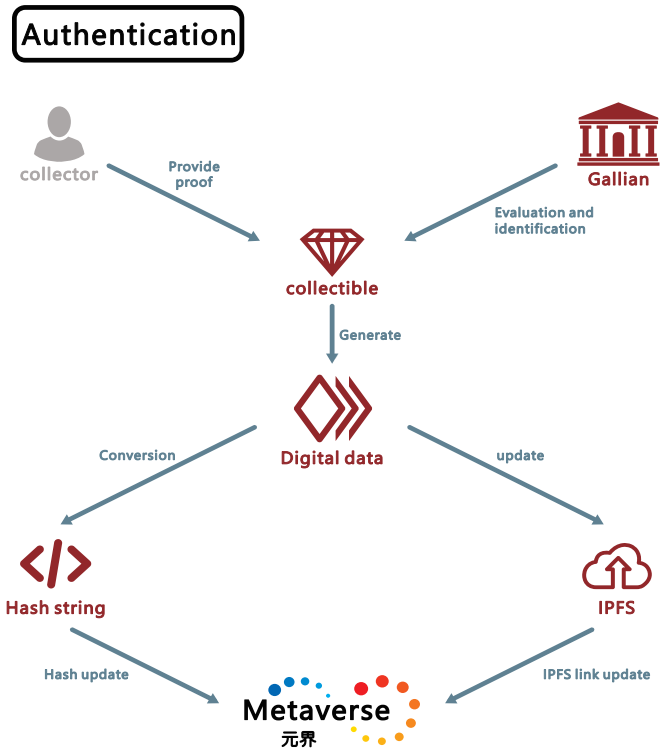
It is the decision of the collectible owner to choose using a single or a combination of digital identifying options for CDP authentication. Holder may need to consider about the value of a collectible and its acceptability by buyers based on different types of collectibles. Indeed, buyers will always demand the most accurate and detailed digital identifying documents. While it is not profitable for sellers to overspend in order to authenticate a low-value collectible, the owner of the collectible will always need to meet the quality criteria of digital identifying files when dealing with the custodian service or when starting a initial collectable token offering.

After creating digital identifying files, collectable holder may upload the files by using ZenDao decentralized application. The application will hash the files using a cryptographic hash function and the output hash value will be uploaded on the Metaverse Blockchain. By having the files stored in distributed storage, the hash address of the storage will also be included in the Blockchain within the same authentication. Therefore this will bind the file to the hash value in the Blockchain.

For collectables with several copies (e.g.: an antique which was reproduced several times), creating a publicly accessible digital identifying file of one of the objects does not secure the authentication of the object because other pieces share high similarities with it. The holder will have to create private identifying files of the object with a high degree of precision (a microscope visual will be ideal or the photograph of a unique mark on the object which is not known by the public). The private identifying files will also need to be hashed and have the hash value stored in Blockchain, but the holders will need to keep the file secret just like the private key of Blockchain address and only show to potential buyers when requested, as an extra proof of ownership. Owners of the unique collectable pieces may also apply with private identifying file mechanism to enhance the authentication process and privacy.

To audit the authentication process, a user will be able to check the digitized identifying file downloaded from the hash address within the authentication, or request for a 3D scan of the collectable and compare it with the digitized identifying file.

Introducing CDP Authentication



User case of CDP Authentication:

1.The collector provides the proof of owning the collectible. It is evaluated and authenticated by Gallian; [14]

2.The collector and Gallian can generate the digital data proving the ownership of the collectible;

3.This data is uploaded to the IPFS for distributed storage;

4.At the same time, this data is converted into a hash string as the unique proof of the ownership;

5.The hash strings and the IPFS link are updated on Metaverse asset network;

6.The digital asset is registered under the digital identity of the collector.

Technologies applied for CDP Authentication

3D scanning technology

3D scanning technology is being used in different areas such as law enforcement, real estate, virtual/remote tourism. Artworks and cultural heritages have been 3D scanned since 1999 starting with Michelangelo' s famous Statue of David.[15] At the end of the 90s and beginning of the 2000s, scanning an object was a long process that would take days of work. Nonetheless, thanks to the rapid improvement of new technologies, it has become more convenient, efficient and safe to scan artworks in recent years. 3D scanning does not cause any damage to the art piece, and is even safe for your eyes.[16] This type of modeling makes it much more convenient than the traditional molding techniques, especially when dealing with old or fragile objects.

Cryptographic hash function

Cryptographic Hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size. Hash function has the following main properties:

a) It is deterministic so the same input always results in the same output.

b) It is quick to compute the hash value for any given input.

c) It is infeasible to generate the input from its hash value except by trying all possible inputs.

d) A small change to an input should change the output so extensively that the new output appears uncorrelated with the old output.

e) It is infeasible to find two different input with the same output. [17]

Distributed storage

Distributed storage systems provide decentralized storage solutions, which have many advantages over centralized systems such as HTTP.

Firstly, the latency (time needed to transfer a package of data from one point to another) on decentralized networks tends to be much lower, which allows for fast transfer of files from one node to the other or from one node to an end-user.

[14] For the Gallian definition, please see the chapter Gallian services.

[15] Proceedings of the 27th annual conference on Computer graphics and interactive techniques, The Digital Michelangelo Project: 3D Scanning of Large Statues (2017), 131–144.

[16] 3DScanCo, 3D Scanning (2017), available at: https://www.3dscanco.com/3d-scanning-faqs/.

[17] Rogaway P and Shrimpton T, Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance (2014).

In addition, when one node goes down, all the other nodes possess the information and the deficient node can be conveniently replaced. This process is enabled by efficient auto-scaling. Moreover, the nature of the decentralized storage makes it resistant to censorship. If the content from one node is censored, all other nodes possess a copy of the data and it is easily retrievable. This makes the entire system even more transparent, reliable and secure.

Finally, integrating distributed storage application on Blockchain also ensures proof-of-work and proof-of-retrievability, which creates a publicly available record of all file movements and storage on the network. A cryptocurrency or token is often used to incentivize the storage of files and the verification of files movements. Consequently, this new technology does not only represent an efficient solution to current issues of centralized systems such as HTTP but also creates value for the contributors to the project.

Introducing Smart Script Secured Trade (SSST)

Smart script has the same concept with smart contracts but in some aspects is different from the smart contracts on other Blockchain networks. Smart script pre-defines the logic and terms within a contract as a script but let the users define the variables. In addition, the users do not need to understand programming language to set up a contract by themselves. Furthermore, it prevents existence of flaws within the contracts. Therefore, it is easier and more secure to use in practice, yet it gives users the freedom to customize the contract terms.

Use of SSST

Reversible trade based on SSST

Based on smart script, reversible trade can be implemented, therefore traders no longer have to worry about either purchasing at a price, which is too high or selling at price that is too low. If the trader is not satisfied after purchasing or regret to have sold her collectible share, the trade is always reversible and secured by a smart script based on the agreement settled a priori. After any party triggers a reverse trade during a transaction, the triggering party will need to pay reversion fee depending on the terms agreed within the contract.

To start a SSST trade, variables within the smart contract representing customized agreement (e.g. Digital identities of trade parties and traded collectible, reversible period, reversion fee rate if reversible trade option is selected) shall first be settled. The smart script will start to execute when all parties have signed the contract using their private keys and have transferred the payment to the smart script address. It will call an end to smart script when it meets the reversion expiring period or the reversion process is completed and confirmed by all parties.

Within a smart contract trade, besides buyer and sellers, oracles such as arbitrator and underwriter can get involved to provide trusted real-world information for smart script. It is not necessary within a SSST trade to have arbitrator and underwriter if both of the parties choose to trust each other. Users are free to set up the options within the SSST drafting process.

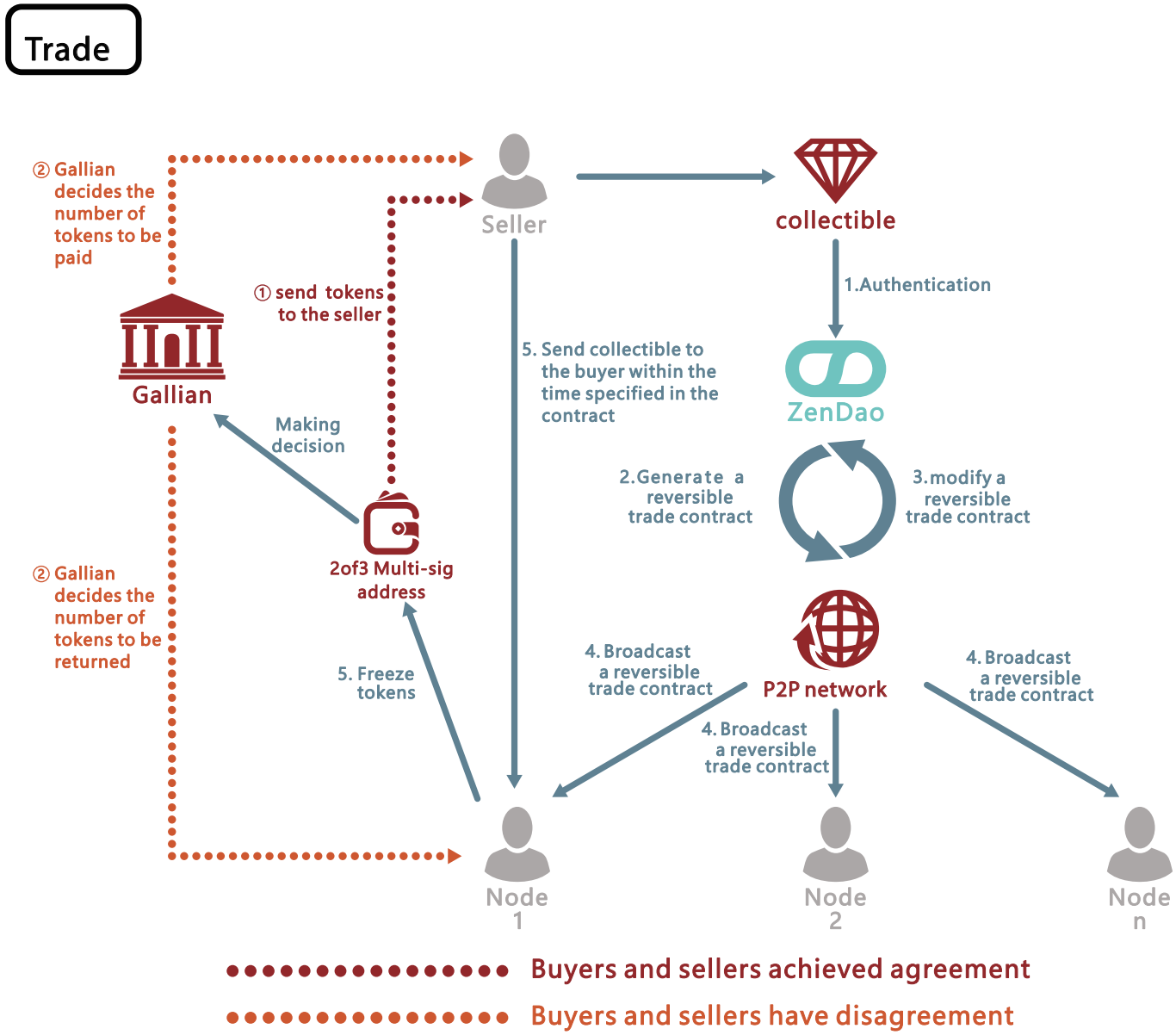
Arbitrator acts as ZenDao oracle to ensure the pre-check representing buyer before physical delivery under cases when buyer is not on site, and to input the true information into smart script to solve disputes. For a “buyer not on site” trade, the seller needs to have the object checked within ZenDao Gallian to prove the authentication together with the arbitrator, and the Gallian will be responsible to have the object delivered to buyer, including insurance during the delivery.

Underwriter acts as ZenDao oracle by acting as a guarantor for the party who is not willing to pay the underwriting fee. In return, the party is paying a certain fee to the underwriter. To ensure the execution, the relevant contracts and agreements will be made offline and only underwriters authorized by ZenDao Foundation will be able to provide this service.

To ensure security and feasibility, when signing the smart script, the contract address will be multi-signatured to freeze the underwriting fee. The private keys to this multi-sig address will be hold by the underwriter (if underwriting fee was paid by seller or buyer, they are the

underwriting parties), the arbitrator and the opposite trade party. This is to prevent the trade parties from colluding with each other in order to loot the underwriting fee that is not paid by them.

Roadmap of reversible trade based on SSST



User case of reversible trade based on SSST:

1.The seller A wants to sell a diamond with a price of 1 million ZDC, while he hopes expects the redemption of his asset within a month;

2.The Seller A authenticates the diamond on ZenDao platform and generates a smart contract to transfer it. The smart contract includes the price (1 million DGC), allowed redemption period (1 month), interest rate (5%). The seller A launches the contract to the P2P network;

3.Node B, willing to buy the diamond, receives the contract and wants A to make some changes to the specific terms of the contract. B contacts A to negotiate the contract. When they come to an agreement, A creates a new contract which includes the terms related to the price(0,9 million DGC), applied redemption period (3 month), interest rate(8%) and delivery date(1 week);

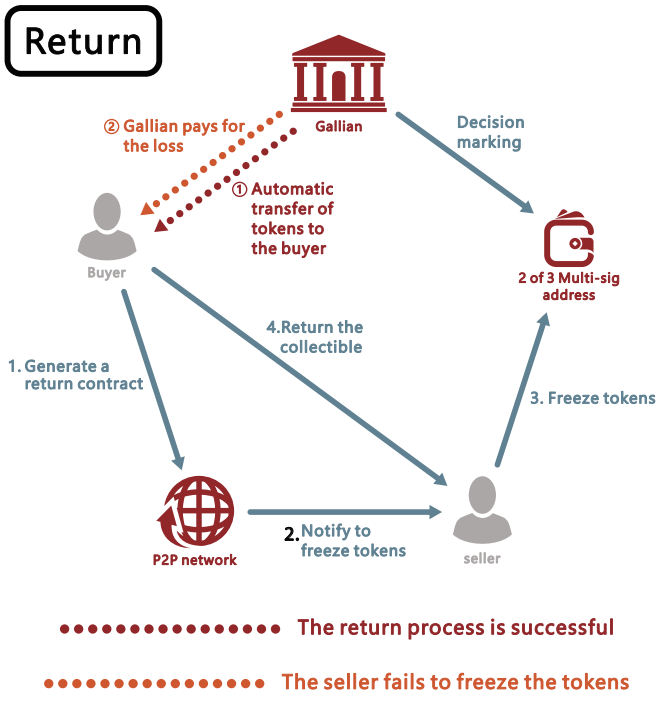
4.B checks the contract and signs it. Smart contract is

executed automatically: 0.9million ZDCs from B’ s account is transferred to the multi-sig address (there are 3 private keys to this multi-sig address, each of them owned by the seller A, buyer B and Gallian. Two out of three private keys signing the transaction are required in order to transfer ZDCs);

5.Within one week, if B receives the diamond and no disagreement exists between the parties, A and B sign the transaction with their private keys in the multi-sig address.0.9 million ZDCs will be transferred to A’ s account;

6.If there is some disagreement between A and B, such as delivery delay or the quality issues related to the diamond, Gallian will coordinate and make the final decision. For example, B received the diamond which has a defect on its surface, Gallian determines that B only has to pay 0,5 million ZDCs. 0,4 million ZDCs will be returned to the buyer’ s account. Due to the multi-sig address mechanism, if B disagrees with the decision, then Gallian can oblige B to comply with Gallian’ s decision.

Roadmap of return process within Reversible trade based on SSST



User case of return process within Reversible trade based on SSST

1. Buyer B in a reverse trade wants to return to the seller the collectible in agreed period of time (1 month). The smart contract states that the buyer has the right to return the collectible but has to pay an interest rate 5% * 0.9 million ZDC = 45,000 ZDC;

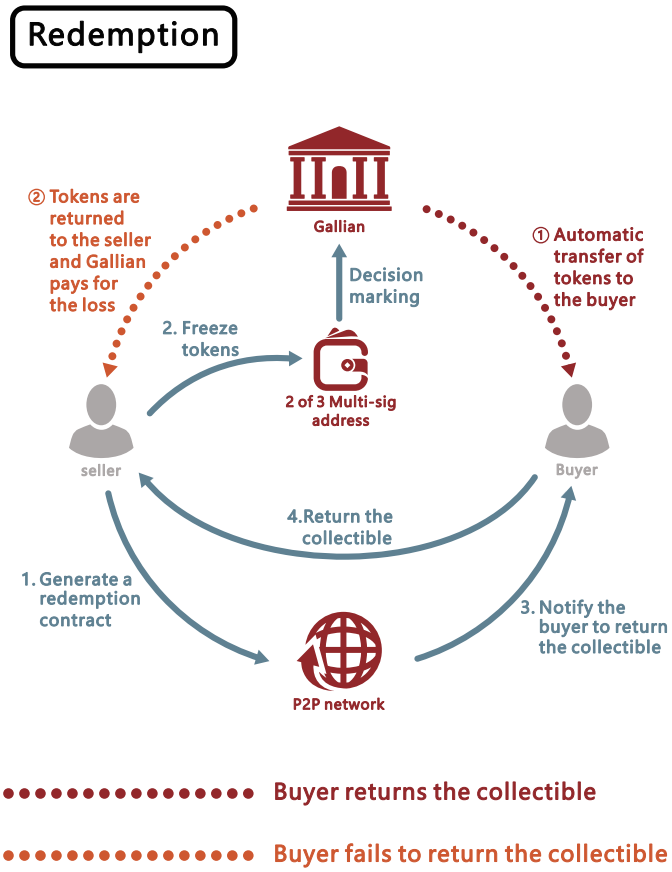
2. Buyer B executes the smart contract. The seller A receives the notification to freeze the tokens (0.9-0.045) million ZDC = 0.855 million ZDC in multi-signature address;

3. Buyer B returns the diamond to the seller within the agreed period of time;

4. If the seller A does not freeze enough ZDCs, Gallian covers the loss;

5. If A and B have an agreement regarding the return process and the diamond’ s quality, A and B will return 0.855 million ZDC to B;

6. If A and B have disagreement regarding the return process or diamond’ s quality, Gallian has the authority to make the final decision.



User case of Redemption process within Reversible trade based on SSST:

1.Seller A requests to reverse the trade to obtain the diamond within one month reversible period. It is agreed in the smart script contract that the seller owns the right to reverse the trade, but needs to pay 5% of the total trade value, which is 45,000 ZDC out of 900,000 ZDC as the total trade value.

2.Seller A transfers 945,000 ZDC to the smart contract address for freezing, buyer B will then be receiving a notification informing him to return the diamond.

3.Buyer B returns the diamond while the judge acts as a witness to avoid disputes. The frozen ZDCs will be automatically transferred to the original payment address of buyer B.

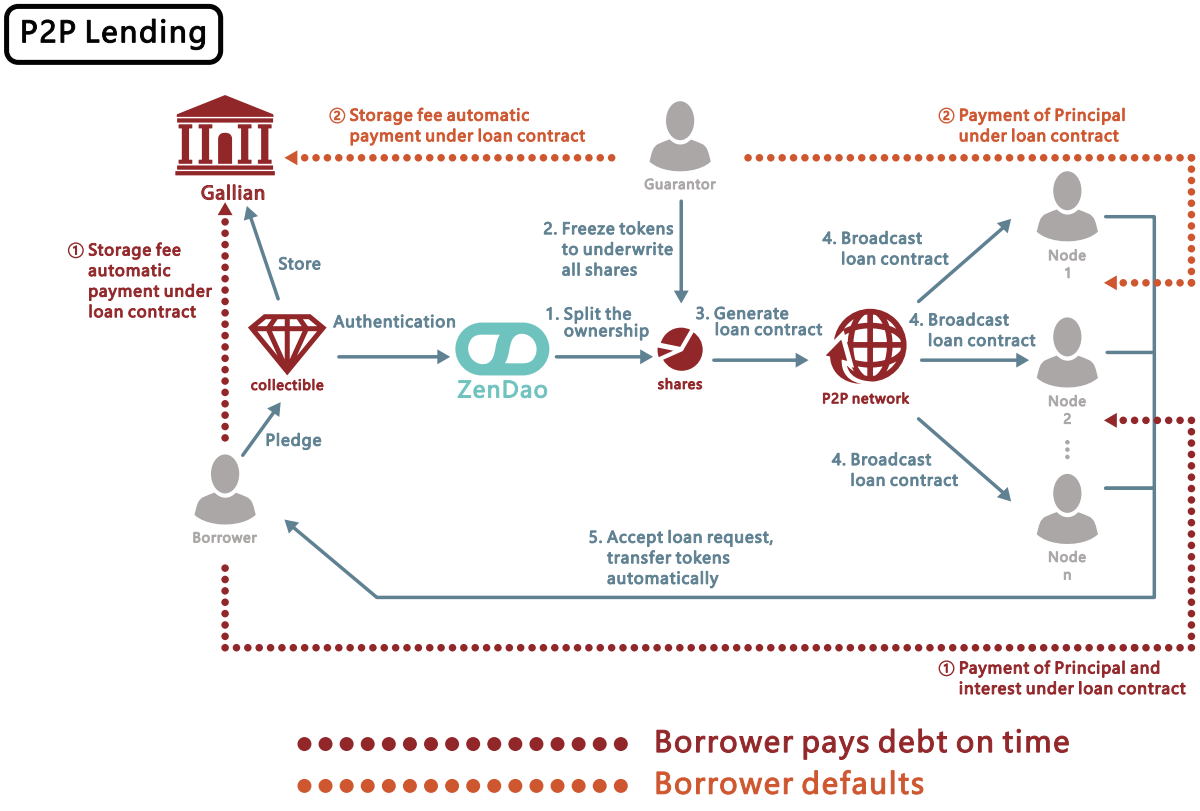
P2P Loans with collateral based on SSST

The collateral borrowing with collectible representing a pledge has a lower interest rate. Yet it has problems in terms of selling the pledged collateral when the borrower defaults as well as presents difficulty for P2P lenders to measure the risk without the knowledge of understanding the value of the pledged collectible.

However, to borrow and lend loans pledged by collectibles is much easier through smart script. Person who wants to borrow loans will need to keep the authenticated collectible with the ZenDao Gallian, and state the amount of loans within the smart script, which is usually lower than the market price. Person B who is interested in this particular collectible but thinks it is too high in price will then see the smart script offer published and participate it as the pre-buyer of the collectible. After that, people who are willing to lend will be able to obtain the lending offer by transfer token into the smart script address. If person A fails to meet his obligation, person B will then become the owner of the collectible with a lower cost, meanwhile ensuring the principle and the interest of lenders by the token he reserved within the smart script.

Within this model, the interest of lenders is ensured by the tokens sealed by the pre-buyer within smart script address and the lenders don’ t even need to know whom they lend to and what kind of collectible is pledged, thus it makes it easier for the borrowers to raise loans.

Roadmap of P2P loan based on SSST



User case for P2P loans based on SSST

1.The collector C has a diamond worth 1 million ZDC, and is willing to borrow 0.8 million ZDC by pledging it, and he agreed to return the loan along with interest within 3 months.

2.The collector C keeps the diamond with the custodian as a collateral for the loan after authentication that has divided the ownership into 100 tokens.

3.Pre-buyer D agrees to purchase all the 100 tokens representing the ownership of the diamond by paying 0.8 million if C fails to return the borrowing, the payment from D will cover the loan and interest.

4.Pre-buyer D transfers 0.8 million ZDCs to the smart script address, after confirmation by the network the smart script will be executed.

5.This smart script will be broadcasted to the P2P network, all the nodes are able to receive and observe the contract, and users who are interested in the return can sign up with the contract to participate within the loan. The smart script will automatically transfer the raised amount of ZDCs to the borrower as soon as the loan order is fulfilled.

6.After the due date, the smart script will check if C has returned the amount of ZDC that is agreed in the initial contract, and will distribute ZDCs to the relevant recipient if the return is approved, and C is able to collect the diamond from the custodian.

7.If C fails to transfer the relevant amount of ZDCs to the smart script address within the agreed period, the smart script will transfer the frozen amount of ZDCs from D and distribute it to the relevant recipient.

User case of option contract based on SSST

Bob, a promising painter, is selling one of his paintings for 1000ZDC. If the current price of each ZDC is 7 USD, the painting will cost 7,000 USD. Alice is interested in buying Bob’ s painting. However, Alice does not have at hand the total amount (1000 ZDC), and estimates that she will have the coins in one month. Since she is worried that in the meantime someone else could buy Bob’ s painting, she offers Bob 100 ZDC “option premium” if he reserves the painting for her. Bob proceeds to retire the painting from the market and gives Alice the option to buy the painting for 1000 ZDC within a month. If they both agree on the terms a smart script contract gets created where Alice now has the right to buy the painting for 1000 ZDC, but not the obligation. If in one-month period Alice does not buy the painting, the smart contract gets activated and Bob keeps the “premium” (100 ZDC). If Alice buys the painting (exercise the option), putting into effect the right specified in the smart contract, Bob gets 1000 ZDC, and he still gets to keep the “premium” (100 ZDC), for a total of 1100 ZDC while Alice gets the ownership of the painting.

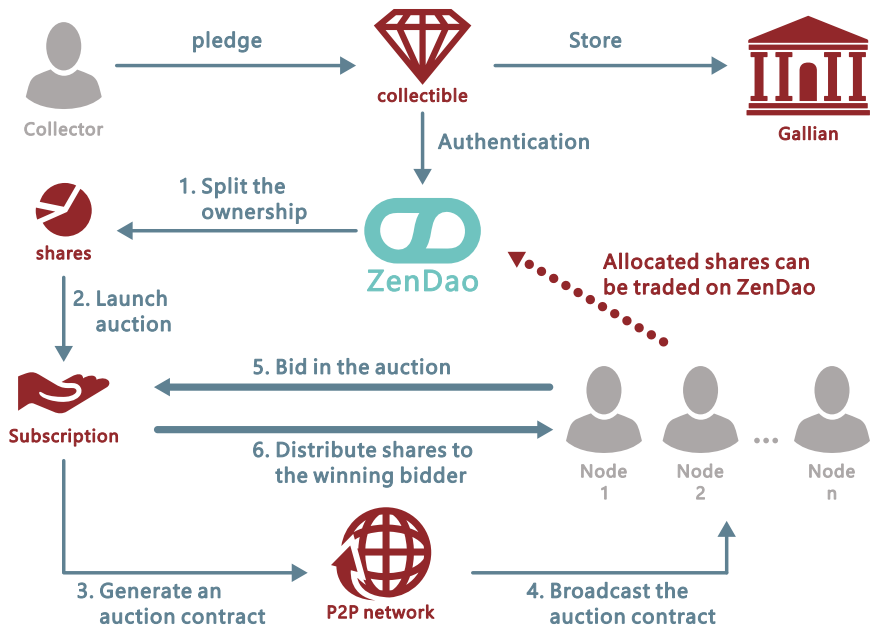
If the price of each ZenDao goes down in price (i.e. 6 USD) and Alice exercises the option, even though the painting still costs her 1000 ZDC, its value in fiat is now 6,000 USD. ¡A great deal for Alice! If the price of ZenDao goes up in price (i.e. 15 USD), the painting’ s value in fiat is now 15,000 USD. If Alice considers that the price is too expensive, she can terminate the deal and Bob keeps the premium (100 ZDC). If ZenDao price remains stable, it is up to Alice to exercise or not the option.

Initial Collectable Token Offering (ICTO)

Introducing ICTO

By digitizing the ownership of collectables in ZenDao, it is now possible to have multiple people sharing and trading the ownership of one single piece of collectable. Depending on the token amount issued on authentication of collectables, holders are able to offer the tokens to the public by meeting the certain authentication criteria. The owner needs to keep the collectable with ZenDao Gallian to launch a presale of tokens, and tokens will be offered to the public only if it is successfully presold, otherwise the smart script will return all the fund raised from public, the holder then needs to adjust the asking price or change type of smart scripted auction. There are two types of auction for token offering within ZenDao in order to meet reasonable market price.

ICTO Roadmap



Auction Methods

Distributed auction

The price of the token is decided by the seller, investors who want to purchase the token will transfer their ZDC into the auction smart script. If the total raised ZDC reached the sought amount within certain period, it is considered as a successful auction and the investors will have a relevant chance of receiving tokens purchased based on the total ZDC received, otherwise it is considered as a failed auction, the invested ZDC will be returned to investors address by the smart script.

Below is an example explaining in details:

The auction period settled is D;

The ask price settled by holder for each token is P;

The sought percentage is 70%, and the total token amount is T, thus the sought amount is 0.7T;

The total amount of ZDC raised is N{N1, N2,N3…Nn};

If the final raised amount is less than 0.7T within in D, the smart script will respond failure. If the amount is over 0.7T, the chance for every investor to get every single token is Q {N1/N, N2/N, N3/N … Nn/N}. The token will be calculated one by one until all the issued tokens are distributed.

Uniform price auction

To ensure the sought amount of token is accepted by the market within distributed chance auction, holder will need to have good understanding and accurate expectation of the market to settle a reasonable asking price, which is difficult. In order to make the process easier for holders who are not familiar with the market, the uniform price auction mode will have a better chance of selling sought amount of the tokens at a reasonable price.

Within the uniform price auction, the price of the tokens will decrease over time (after every block is created). The token price of the block at which the sale goal is reached becomes the final token price for all participants in the auction. The earlier the sale goal is reached, the greater the value of each collectible token. It is important to mention that investors should not speculate on the value of collectible tokens but instead choose the time when they believe the price of each token is representative of the value of the chosen collectible. At the time when the investor transfers her ZDC tokens, she must understand that she is committing to the maximum price per collectible token and that the tokens she will receive may be valued at this rate or lower.

The formula used to determine the evolution of token price over time will be determined for each piece of collectible prior to its ICTO. Indeed, the formula will be determined using the four following variables: the highest price set by the seller, the price recommended by experts via a decentralized autonomous organization, the estimated final deal price and the lowest deal price that the seller is willing to accept. However, smart script will be used so that all participants can see price decreasing over time.

User case for ICTO

Collector A authenticates his diamond on ZenDao and has the ownership split into 10000 pieces.

Collector A applies for pre-sale by establishing a smart script for ICTO and broadcasting this contract. The interested investors will sign the contract to participate in the pre-sale auction.

The auction winning bidder will be able to obtain the issued tokens.

After successful ICTO, the diamond ownership tokens will be listed in exchanges for trade.

Smart Monetary System

Smart Monetary System Introduction

ZenDao Coin (ZDC) is the fundamental unit of account on ZenDao platform. All assets that will be digitized on ZenDao can be purchased by ZDC. At the same time, ZDC can be freely traded on the exchanges. ZDC is constantly increasing in supply according to the smart inflation mechanism rules that are embedded in the system. ZenDao aims to create a smart inflation policy that would bring fairness and healthy economic model to the market. We acknowledge that a network without inflation but fixed amount of initially issued token is unhealthy because the participants who joined the market in the early period would have obtained the tokens with low cost, while the participants joining later would have to purchase token from the original owner at a comparatively high price, which not only is not fair to the new participants, but also would encourage people to hold the token instead of spending them, thus the market would cool down with less people selling and buying. However, an over warmed market caused by too much inflation is also not healthy, people would tend to sell tokens and keep collectable token in hands which would lead to consistently drop in price of token thus lead to loss of confidence in the market as a result. Therefore, regular self-adjusting, flexible, real-time market factor considered monetary mechanism in order to build a healthy market.

Inflation will not be applied in the beginning of launching ZenDao network. Every time there is a successful ICTO, the issued collectable valued in ZDC will be cumulated. Inflation will start as soon as this figure reaches the initial issued amount of ZDC.

Monetary mechanism

The principle of the built-in decentralized adjusting mechanism is to balance the equivalence between the tokens supply value and the assets that back them, the economic equilibrium.

Assuming:

the amount of different kind of collectables is L ;

the amount of consumers is I ;

the amount of current ZDC supply is D ;

wealth of each Consumers

$W=\{w_1,w_2,w_3,\ldots,w_m\}$

Tokeni represents the amount of token issued for every collectable, therefore we have

$T=\{t_1,t_2,t_3,\ldots,t_n\}$

Z represents the unit ZDC price of everyTokeni, therefore we have

$Z=\{z_1,z_2,z_3,\ldots,z_n\}$

therefore we have ZDC value of all collectables in ICTO

$T\times Z=T\times Z_1+T_2\times Z_2+T_3\times Z_3\ldots+T_i\times Z_i$

Assuming:

$$\frac{T\times Z}{D}=A$$

Investors are tend to invest when they have relevantly more money(D) in hand rather than token(T*Z), which is whenA≤1, so then we will need to raise more ICTO within certain period, and also increase the inflation rate for every ICTO. In order to optimize the value of A to maximize the participants in the market, we developed the utility Function of A:

Max u(I)≈Max u(T,Z,W)

$$= \sum_{j=1}^{m}\sum_{i=1}^{n}\frac{1}{1-A}\left(\frac{t_i*z_i}{w_j}\right)^{1-A} \quad \text{if } A\neq 1$$

$$= \frac{\sum_{i=1}^{n} t_i*z_i}{\sum_{i=1}^{m} w_j} \quad \text{if } A=1$$

The factors which may influence variable A are: ZDC total supply, rate of ICTO (amount of ICTO within certain period of time), price in exchange, therefore the system will observe the fluctuation in value of variable A to determine whether to increase inflation rate in order to raise ZDC total supply faster or control the rate of ICTO.

Inflation management

The inflated ZDC will be distributed to ICTO buyer and seller as bonuses in order to encourage holders with collectables and investors interested to participate. Meanwhile, certain amount of inflated ZDC will be distributed to Gallians own by ZenDao foundation in order to pay for insurance of collectables, maintenance and security services, and to establish more Gallians.

Introducing decentralized exchange

In this paragraph, we explain how we plan to operate our decentralized platform in the short and long run. In the short run, we will leverage the Openledger decentralized exchange to issue our tokens and allow customers to use their tokens to purchase shares of collectables directly on OpenLedger. In the long run, we hope to build our own decentralized platform for and will let our customer choose to use open ledger or our decentralized platform.

The artist or owner of the collectables will firstly need to determine the value and issue tokens of the collectibles on ZenDao by going through successful ICTO process and then the token will be listed on the exchange. On decentralized exchanges, all accounts and transactions of digital assets are monitored by a network of computer and not a single server and they are all recorded on a Blockchain that is publicly auditable. This allows for greater security, transparency and eliminates the risk of single node attack.

Given the structure of centralized exchanges, it is complex to understand whether or not the assets listed are actually backed by actual assets. In addition, risks of market manipulation are relatively higher on centralized exchanges as well. Finally, they tend to be more attractive targets because they hold their entire customers fund in the same place.

As opposed to centralized exchanges, decentralized exchanges bring transparency to every trade. In addition, they do not allow for high frequency trading, which provides all traders with the same opportunities and reduces the probability of market manipulation. In addition, decentralized exchanges strictly comply with 100% reserve standards, which guarantees the solvency of the market continuously. All their assets are preserved by tokens as a collateral and are kept safe because no private keys can be used to access them.

Gallian services on ZenDao

Gallian plays an important role within ZenDao as an oracle with multiple functions such as Gallery, custodian, verification facility. It is the place that connects the real world with the Blockchain, where people can see collectables under digital identities, trade would be so easy by replacing the ownership instead of physical transportation of the object. The fund raised from ICO will be partially used to build Gallians to support the ZenDao Blockchain service, and also by cooperating with existing galleries and museums to expand the scale of the market. All the collectables stored in Gallian will need to go through 3D scan process, and have the modeling file stored, therefore by applying virtual reality technology, it is possible to have users sitting at home visiting the Gallian just like they were there, either to check the collectables they tend to invest, or just to appreciate art.

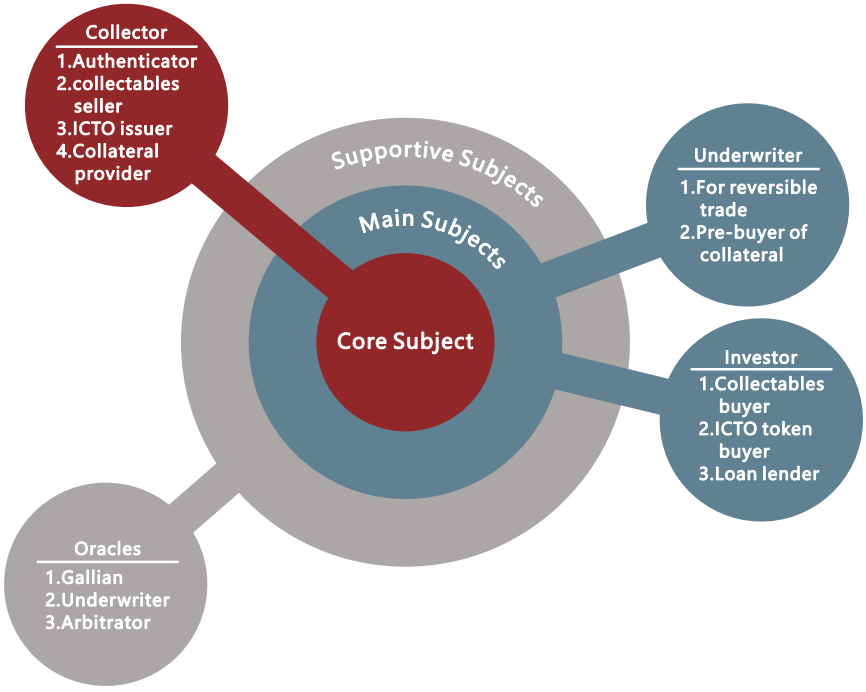
CREDIT SYSTEM

ZenDao is a decentralized system based on Blockchain technology. There is no centralized management organization, therefore it has the advantages of free handling fees, data security and free trading activities. However since there is no centralized regulation, the behavior of the participants on the ZenDao cannot be constrained, so we need to build mechanisms to guard against fraud.

ZenDao created a decentralized credit system, which allows it to record and analyze the behavior of each participant on the ZenDao. The result of the analysis of each participant's behavior shows credit score and grade.

ZenDao key participants analysis

ZenDao is a decentralized business system where collectors, investors, underwriters and oracles influence and rely on each other. The structure of the main body is shown in the following figure. Among them, the collector is the core, and the activities of other participants are carried out around the collectors.



Collector: Owns the authenticated collectables, can use the proceeds for reversible trade, token trading and collateral loans.

Investors: Participate in the reversible trade and ICTO auctions, provide loans to collateral borrowers and earn profit from it.

Underwriter: Guarantee that reversible trade occurs smoothly and compensate for the losses caused by the breach, the buyer pre-confirms the value of the collateral purchased by the borrower in the mortgage business, when the borrower loses the ability to repay the loan, and underwriter will pay the principal of the investor.

Custodian: Custody maintenance of pledged goods.

Arbitrator: Determine the effectiveness of the physical delivery process.

Credit evaluation indexes

The establishment of the credit evaluation system is an effective way to solve the problem of lack of credibility of the active principal on the ZenDao. In order to consider the credit behavior of the participants on the platform and the responsibility for performance, ZenDao builds the credit evaluation index system of the credit entity.

Data sources and reliability

The information stored on the block chain cannot be tampered and the time stamp can be traced. Therefore, the information and the transaction records stored on the ZenDao will be true and effective. By synchronizing and parsing the information in the ZenDao Blockchain, we can easily obtain the data that could be used in the credit evaluation system. For instance, by parsing the transaction information of an authentication, we can tell the owner by identifying the token receiver, hash address on distributed storage of the object, etc.; by parsing a transaction information of a reversible trade, it will show the identification of both parties, judge and underwriters, also the detailed attributes values including trading value, reversible period and reversion fee etc.

Establishment and application of credit system

Synchronization and analysis of block chain information, can be used to advise the credit system data, through large data analysis method. The basic data is filtered and processed. Based on the data obtained, a rigorous mathematical model is established and corrected.

The mathematical model is used to make credit scoring of the active participants on the ZenDao. The score can be used as an evaluation element of the reputation of the ZenDao users. Referring to this evaluation mechanism, users can avoid the loss caused by the dishonest behavior of the ZenDao's low credit level users.

ZENDAO ICO GUIDELINE

ZenDao will be using ICO as a method for fundraising. An ICO (Initial Coin Offering) is a tool for early stage Blockchain related projects to raise funds by selling part of their tokens to the early backers. An ICO can fund development of projects that are in the very beginning of their journey, while early backers receive the cryptographic tokens that come as part of the project that the ICO teams are developing. During ICO round ZenDao will allocate ZDCs to the participants of the fundraising campaign.

ZDC Features

ZenDao Coin (ZDC) is the fundamental unit of account on ZenDao platform. All assets that will be digitized on ZenDao can be purchased by ZDC. At the same time, ZDC can be freely traded on the exchanges. ZDC is constantly increasing in supply according to the smart inflation mechanism rules that are embedded in the system. This token, representing the value of the whole network, is designed in a manner to allow its holders to enjoy the high capital appreciation over time. The value of the token is derived from the value of ZenDao platform, thus every time the ownership of a new collectible is tokenized on the platform, the network effect growth maximizes the returns for ZDC holders. Thus, the investors in ZDC directly benefit from the success of ZenDao platform.

ZDC Allocation Roadmap

ZenDao ICO open date is 23rd of June, 2017. ICO round will be open for 2 weeks. The closing date of ICO is 7th July, 2017.
Investors can participate with BTC, ETH and ETP. The separate multi-signature addresses will be available for

the fundraising purposes. Those addresses will be publicly announced in order to insure the external auditability. After the closing date of the ICO campaign, ZDCs will be allocated to the fundraising campaign participants. As the price per ZDCs is predetermined and publicly available before ICO and also bonus system is set by the ICO team for the early contributors, the investors will be able to check the amount of ZDCs they are supposed to receive after the ICO round through the platform they invested in ZenDao campaign. The price of each ZDC for ICO will be available on ICO opening date on the official webpage of ZenDao.

During ICO round, 65% of ZDCs will be allocated to the public, 5% will be released through bounty program, 10% will go to ZenDao team and 20% will be assigned to ZenDao foundation.

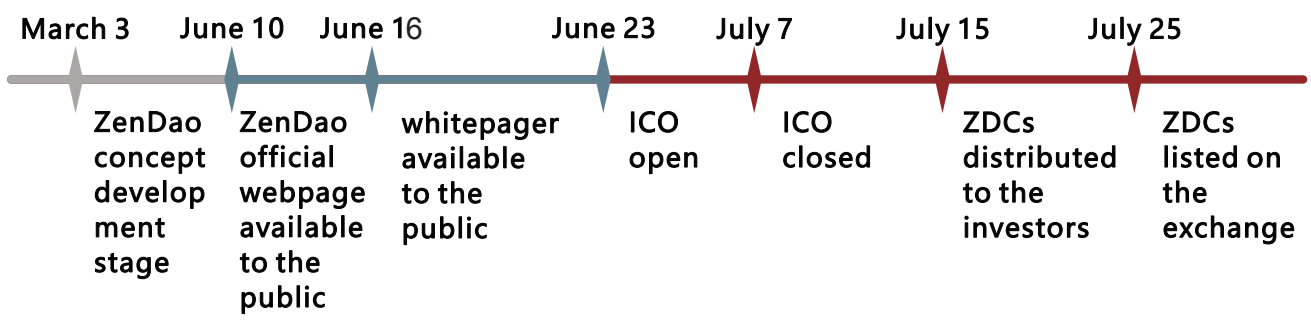
ZDC allocation plan:

Percentage of tokens	Receiver	Purpose
65%	ICO contributors	ICO participants will be able to enjoy the capital appreciation on tokens they hold, to trade within the platform with ZDC or exchange the token on different exchanges that will list ZDC tokens.
5%	Bounty program	For ZenDao supporters that will contribute to ZenDao community growth by blogging, translations, local community management and etc.
10%	ZenDao team	As a reward, ongoing research, other ICO costs.
20%	ZenDao foundation	For future development, operation and management costs of ZenDao platform.

ZDC bonus system:

STAGE	EXTRA BONUS RATE
Early bird stage (June 23 – 24)	20%
2nd Stage (June 25 – 26)	15%
3rd Stage (June 27 – 29)	5%
Last Stage (June 30 – July 7)	No extra bonus rate applied

ZenDao ICO timeline:



ZDC holder benefits:

How ZDC holders benefit from the token
Stable Capital appreciation;
Ownership of a highly liquid token that can purchase any asset on ZenDao platform or can be exchanged for other cryptocurrencies/fiat money on exchanges;
Alternative type of investment holding that allows diversification of the investor's portfolio;
Early participation and more liquidity in the community development lifecycle.

Raised Funds Management Policy

The funds raised during the ICO campaign will be spent to ensure a rapid development and growth of ZenDao community. ZenDao team is committed to provide the best level of transparency and security to the investors and ZenDao community participants.

ZenDao will be publishing periodic newsletters summarizing the fund allocation and spending plans as well as any divergence with the initial roadmap set in the Whitepaper.

The funds raised during the ICO campaign will be dedicated to:

1.Establish ZenDao foundation with the board of advisors in order to implement the best governance and decision making processes for the purposes of further development of ZenDao platform. The annual budget will be proposed and presented to the advisors board for approval and made public to the community. ZenDao foundation will be incorporated under the jurisdiction of Swiss law;

2.Establish a world-class team working on execution of the objectives set forth in the whitepaper;

3.Create global cooperation with already well positioned galleries, museums and custodian services that would allow ZenDao platform to achieve global scale and rapid expansion;

4.Create Gallian and augmented reality gallery services around the world in order to provide the platform users with convenient and safe alternative for storing and exploring the collectibles with ZenDao;

5.Cover the office and indirect costs related to employment and operation of ZenDao platform;

Cover the marketing and communication activities related to ICO campaign as well as future operation of ZenDao platform;

6.Sponsor further coding and ecosystem building and advisory fees for ZenDao platform;

7.The funds received during the ICO campaign will be kept and managed based on the public auditability principle. Raised investor contributions will be under the custody of multi-signature wallets of BTC, ETH and ETP respectively.

For the security concerns, the keys to the multi-signature wallets will be controlled by six trusted individual (two representatives from each of the following teams: ZenDao foundation, ZenDao project development team and Metaverse foundation). Six out of six signatures will be required to execute any payment from the wallets. Hereinafter are listed the entrusted individuals.

CONCLUSION

Having identified the current challenges, ZenDao aims to provide smooth solutions to the complex problems and create fair and open market standards. ZenDao is committed to be an innovative Blockchain-based platform that will successfully transform the current infrastructure of the collectibles market and the relations between the market's major stakeholders.