

# MOLD Whitepaper

The Decentralized Game Platform for The Next Generation

MOLD Team

May 1st 2018

Edition 1.0

## **Abstract**

MOLD is a fair and secure decentralized gaming platform that supports the development of new games and simplifies the transaction of valuable data such as in-game items, weapons and armors. MOLD uses tokens uniquely defined on MOLD chain to allow in-game items, weapons and gears to circulate in the market without going through a third party. Unlike previous centralized game structures, game tokens used in MOLD are not owned by the game operator. Thus, a brand-new value to the data will be applied within such virtual reality called games. With the advancement of technology and human evolution, this new value created in the virtual reality becomes more realistic and offers the possibility of gradually bringing about great economic benefits. In order to maintain fairness, MOLD allows transactions to be verified by the user, where flow of funds are visible to avoid counterfeit currency, double spending and other fraudulent acts. Previous monetary systems were based on a client-server network structure, and their centralized payment systems were vulnerable to hacking and other external attacks, resulting in a substantially high fee to implement such a complex process and adherence to regulation policies. In a decentralized monetary system with a P2P network structure, information will neither be kept in one place, nor would it depend on third parties, offering much higher security and lower burden to the system itself.

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Our Vision . . . . .	4
1.2	Operation Policy by a Decentralized Community . . . . .	4
1.3	Definition: moldcoin . . . . .	4
<b>2</b>	<b>Background</b>	<b>5</b>
2.1	Evolution of the Gaming Industry . . . . .	5
2.2	Issues Facing the Current Gaming Industry . . . . .	5
2.3	Blockchain Industry Trends . . . . .	6
2.3.1	Emergence of Blockchain Technology . . . . .	6
2.3.2	Issues Facing the Blockchain Industry . . . . .	6
<b>3</b>	<b>MOLD Principles</b>	<b>8</b>
3.1	System Benefiting the Players . . . . .	8
3.2	Simplified Game Development for Developers . . . . .	8
3.3	Proposal for Next-Generation Gaming . . . . .	9
<b>4</b>	<b>MOLD Blockchain Specialized in Games</b>	<b>10</b>
4.1	Design Goals: Creating an Exciting Future . . . . .	10
4.2	Issues to the Ethereum and the Need for TPS . . . . .	10
4.3	Token Model . . . . .	11
4.3.1	Main Currency over the MOLD platform . . . . .	11
4.4	MOLD Function . . . . .	12
4.4.1	Wallet and Account . . . . .	12
4.4.2	Tokenization . . . . .	13
4.4.3	MOLDEX and MOLD Auction . . . . .	13
4.4.4	Escrow Transactions between Players . . . . .	14
4.4.5	MOLD ICO . . . . .	15
4.4.6	MOLD SDK . . . . .	17
4.5	Block Structure . . . . .	17
4.6	Consensus Algorithms . . . . .	19
4.6.1	Problems Facing the Current Consensus Algorithm . . . . .	19
4.6.2	BFT Systems . . . . .	19
<b>5</b>	<b>Molca Project</b>	<b>22</b>
<b>6</b>	<b>Conclusion</b>	<b>24</b>
<b>7</b>	<b>Note</b>	<b>30</b>

Appendix A : Decentralized Autonomous Organization  
Appendix B : Revenue Structure over the MOLD  
Appendix C : UTXO vs Account-Base

## Glossaries

MOLD : All the system of game platform including MOLDchain

MOLD chain : Blockchain which is governed by distributed Community

moldcoin : Unit of game tokens circulating within

Community : All the network members of MOLD

User : A network member of MOLD

Player : A gamer plays on MOLD

item-token : The token which represents the ownership of an item

BFT : Byzantine Fault Tolerant

PoI : Proof of Importance

PoS : Proof of Stake

PoW : Proof of Work

validator : Those who confirm transaction data

participant : Those who using MOLD network

speaker : the person selected by random to distribute transaction data

view : The one turn to generate one block

# 1 Introduction

## 1.1 Our Vision

MOLD is dedicated to "Building a Second World" in virtual space. In particular, as a platform, MOLD supports new game development, and the establishment of a free RMT market. We aim to free the people from physical labor and create a world where revenue can be made possible through games. With the ultimate goal to create of an enormous economic value in the virtual reality world, we will support the development of a fully immersive VR game.

MOLD is a fair and secure decentralized gaming platform that supports the development of new games and simplifies the transaction of valuable data such as in-game items, weapons and armors. In-game items, weapons and armors will be protected as digital assets over the blockchain, and free for transaction between players without a third party. Unlike previous centralized game structures, game tokens used in MOLD are not owned by the game operator. Thus, a brand-new value to the data is given in the virtual reality in games. As consumer to consumer transactions becoming more prevalent in recent times, it is natural that an establishment of in-game private ownership will be born from the emergence of such a diverse economy within a game.

## 1.2 Operation Policy by a Decentralized Community

To realize MOLD's decentralized gaming platform, the operating structure will be community-based with cooperative effort between members, all of whom support the MOLD principles (detailed in Appendix A). Aim for an exciting future by establishing a next-generation gaming platform without a centralized operator, with support from a community of various stakeholders including token holders, players and developers from around the world. The contents in the whitepaper here should be construed only as a proposal made by one member of the community, the MOLD team, and should be modified accordingly through discussion within the community.

Appendix A : Decentralized Autonomous Organization

## 1.3 Definition: moldcoin

The term "moldcoin" mentioned within this whitepaper is defined as being built over the MOLD chain. A moldcoin(ERC20) compliant to a Ethereum-based ERC20 token should be called as moldcoin(ERC20), and considered separate from a moldcoin. Furthermore, moldcoin(ERC20) should be considered to be compatible with moldcoin, and possible to trade 1 moldcoin against 1 moldcoin(ERC20). In addition, moldcoin(ERC20) will be burned the moment it is exchanged into moldcoin.

## 2 Background

### 2.1 Evolution of the Gaming Industry

In recent years, starting with MOBA (Multiplayer Online Battle Arena), FPS (First Person Shooter), RPG (Role-Playing Game), and especially MMO (Massively Multiplayer Online), there has been a significant and continued growth in the PC gaming market. In addition, due to the spread of smart phones and new technological innovations, the gaming markets for both mobile and VR are rapidly growing. The international gaming market size was about 570 billion Dollars in 2014, 690 billion Dollars (up approx. 25% increase year-on-year) in 2015, and 890 billion Dollars (up approx. 29% increase year-on-year) in 2016.

Of particular note was the growth rate in the e-sports market. This market increased from 350 million Dollars in 2015 to 460 million Dollars (up approx. 30% year-on-year) in 2016, and is expected to rise to 1.1 billion Dollars in 2019. The underlying cause of which seems to be a fundamental shift in how people work. Due to advances in science and technology, physical labor and operations will be eventually substituted by AI and robot labor. Thus, most people will be freed from the majority of the labor-intensive professions and will in turn be able to pursue a higher quality of life and recreations for their careers. The development of the internet have made easy online communication, resulting in diverse communities inside of the gaming space. With AR and VR technology providing an increasingly realistic gaming experience, games continue getting closer to real life.

### 2.2 Issues Facing the Current Gaming Industry

Under conventional game structures, ownership of in-game items remained at the side of operators, and players were unable to hold these items as their assets within the game. The electronic information of an item obtained in-game could only function within its one game, and therefore were unable to pass on its value from its game to other games. The time and funding poured into a game would only hold value within the single gaming space. In addition, trading of items in-game are prohibited by the terms and conditions set forth among the majority of the game-operating companies, making it difficult for players to pass the value of any electronic information beyond that of a single gaming space. Therefore, resulting in limiting the economic activity of the player within the game world. Tradings of In-game items or electronic information are known as RMT (Real Money Trading), but the centralized structure taken by many existing games prohibited RMTs within the terms and conditions of said games. However, it has been analyzed that there is huge demand for such a concept, and the potential for such a market is estimated to be in an upwards of over several tens of billion Dollars. The conventional framework regarding game releases have been that of a paying a hefty publishing fee to a centralized third-party

company. To further promote the development and creation of an appealing next-generation virtual reality, there needs to be a gaming environment which makes possible to transfer and settle transactions of electronic value.

MOLD can convert in-game data into tokens, making possible for decentralized transactions within a virtual reality, structured as a distributed-type second-world. No player will be restricted by the limitations and other specific issues set forth by a centralized authority, making it possible to hold in-game items as digital assets, and the freedom to buy, sell and reap the benefits. Recently, there has been a push for the establishment of an RMT Exchange, but MOLD proposes to disregard a conventional centralized structure, and instead build a system enabling RMT over a decentralized network by using blockchain technology, of which will be detailed in the following chapter. Thus, as a "Game Platform of the Player, by the Player, and for the Player", will create a decentralized virtual reality for the next-generation, enabling various economic activities for all game enthusiasts.

## **2.3 Blockchain Industry Trends**

### **2.3.1 Emergence of Blockchain Technology**

In 2008, with the release of Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System"[1] whitepaper, and subsequent development of Bitcoin, the Bitcoin was hailed as a revolutionary innovation in currency and cash. Furthermore, Bitcoin was the first example of a digital currency without gold convertibility and the backing of a centralized monetary authority. The blockchain technology utilized in the basic management for the Bitcoin was made possible by adopting a simplified algorithm and computing power to enable ledger management by a decentralized network. The Open-source Ethereum[2] project supervised by the Ethereum Foundation is a next-generation smart contract and decentralized application platform. The majority of cryptocurrencies represented by Ethereum and Bitcoin all utilize blockchain technology at their core. Encryption (of electromagnetic information), Timestamp, consensus algorithm and economic incentive structures, made it possible for decentralized ledger management by P2P transaction process per nodes without trust, resolving issues in a centralized authority, such as high cost, inefficiencies and safety issues of electronic information storage. Although blockchain itself is technically not considered a new technology, the combination of P2P communication, encryption technology and data structures on the chain, can be considered as an innovation.

### **2.3.2 Issues Facing the Blockchain Industry**

The development of a decentralized governance system has attracted a large following to the blockchain project, and continues to increase worldwide, with many applications being developed. From digital currencies to applications

containing Ethereum-based smart contracts and building Ripple-based global transaction system layers, a variety of use case scenarios are born every day, posing not just further demand, but issues to the blockchain.

Unlike most software, a decentralized blockchain structure does not request users to update client and protocol, resulting in severely limiting the system due to the occurrence of "hard fork" or "soft fork", of which leads to heavy losses to the community in conjunction during protocol updates. There are still debates regarding block scalability, hindering the development of Bitcoin protocol. Due to the Bitcoin blockchain being limited in size capacity and therefore considered a factor in clogging over a million transactions, users are faced with an expensive amount of fees to accelerate such transactions. Ethereum faced a similar problem, in that by using hard fork as a remedy to The DAO problem, splintered the community, causing degradation to the user experience. In a climate with numerous hype projects that require no blockchain technology, just to cater to the ongoing speculation fervor of cryptocurrencies, a use case scenario to combat the above challenges and realize a decentralized-society will be essential.

## 3 MOLD Principles

### 3.1 System Benefiting the Players

Traditionally, ownership of items earned through billing and play in client-server type games belonged to the operating company of games, and not the players themselves. Therefore, players were unable to willingly buy or sell the in-game items, with the items becoming worthless in value when players left to play to another game. However, it must be stressed repeatedly that it was the player themselves whom had gained these items within the game and is only fair to demand ownership back to the players. Through the MOLD gaming platform, players can secure electronic information over the MOLD blockchain by tokenizing (detailed in Chapter 4) the in-game items, thereby creating a player-owned item-token economy, separate from the game companies. Through MOLDEX (detailed in Chapter 4), players can exchange item-tokens into moldcoins (the basic currency) over the MOLD platform. Upon a player leaving Game A, the player may tokenize the items gained within Game A and exchange into moldcoins. The player can then use the moldcoin for purchasing items within Game B. In this way, by utilizing the MOLD platform system, in essence, the traditionally prohibited (by game companies) act of RMT becomes possible. Through MOLD, it becomes possible for the value of items in Game A to hold its worth. In an ever-evolving gaming universe, by managing digital assets in-game, players can enjoy more freedom and a more appealing next-generation type decentralized virtual universe.

### 3.2 Simplified Game Development for Developers

Many game developers face the dilemma of having the necessary design and technology, but insufficient funds to continue developing games. Furthermore, the conventional centralized platforms used by major companies employ a business model that charges up to 30% to 50% in fees from the developer. This makes it difficult not just in retaining the skills required to develop popular games, but also making difficult for developers and technicians to raise revenue. (Better to show data here) However, within a decentralized system, not even a fee of 1% will be charged. The fee required to release a game by a developer as a decentralized gaming platform over the MOLD should of course be 0%. (Appendix: Revenue Structure over the MOLD) Regarding funding for game development over the MOLD, a system will be prepared for an ICO to be implemented over the MOLD platform (detailed in Chapter 4), making it possible for small to medium sized game companies (subcontractors of major game companies in a traditional business model) to be provided opportunities to release original games easily and at low-cost over the MOLD platform after development. In addition to all functions including tokenization of in-game items, SDK will be prepared to support conventional game developers (detailed in Chapter 4).



### 3.3 Proposal for Next-Generation Gaming

In the current game industry, players have no ownership for any in-game digital assets, and small to medium game companies and their developers act only as subcontractors for the major companies. It means that the business model is structured in a way that concentrates the revenue stream to only the major game companies and existing centralized game platforms. In addition, although with the advent of an ever-increasing number of players active in e-sports (pro-gamers), the general public regards being immersed in gaming to be unproductive and a means for escapism. One reasoning behind such a perception could be that the ownership of time and money spent and gained in games do not remain to the player as a digital asset. If time spent inside a virtual environment could influence the real world, there will be an enormous change in the way the public views gaming. Virtual space itself is expected to become increasingly more real. At this point, let us compare the state of both current and next-generation games. Next-generation games will offer players the official right to claim item ownership, making them more independent, and with the popularization of E-sports, Pro-gamers will be more familiar to general public. At the same time, for the developers working in the small and medium game companies, it will make it possible for them to raise funds, organize a project team and to develop creative games with only the skills they have without relying on the bland image of major enterprises. Due to advances in science and technology, robots and AI (Artificial Intelligence) are increasingly taking the place of human labor and workloads, while entertainment gains more importance in such a diversified future. In such a world, gaming will no longer be perceived negatively, rather, it will come to be regarded as not just entertainment, but as a form of profession. A decentralized game platform could be the new solution to the problems faced by the traditional gaming industry. A next-generation decentralized virtual reality will enable game enthusiasts to truly be immersed, in addition to providing game developers much more freedom into creating new games that will meet the needs of the players. MOLD will provide such a future of gaming to the world.

## 4 MOLD Blockchain Specialized in Games

### 4.1 Design Goals: Creating an Exciting Future

MOLD aims to a creating a decentralized next-generation gaming platform using blockchain technology that will provide an exciting and exhilarating new world for all. MOLD will provide a system for all game enthusiasts to participate in creating a "Game Platform of the Player, by the Player, and for the Player".

#### **Item-Tokens as Digital Assets**

Digital assets are a programmable asset taking the form of electronic information. By utilizing blockchain technology, the electronized assets become highly transparent and protected and trustful making possible for distribution. The user can register an object called Account over the MOLD chain to freely manage and trade the in-game items as a digital asset that have now been tokenized.

#### **Secure and Quick Transactions within a Virtual Economy**

To stimulate free Consumer to Consumer economic activity over the MOLD, adopting a blockchain customized to a game will streamline conventional billing structures, as well as bringing transparency and protection of item-token transactions over a decentralized gaming platform. In addition to a point being that in order to realize an immediate form of payment, the finality of the quickness of such a trait will be important. Furthermore, a system will be built supporting scalability of the blockchain to combat further increase in users due to the addition of new games.

#### **Availability to All: for the Games, the Players and the Developers**

In order to allow the participation of all the game enthusiasts into the next-generation gaming platform, a specialized blockchain will be developed to also support existing games and having the versatility to be implemented with various functions by the players and developers. By allowing a limited issued amount of tokenization for items with the data implemented over the smart contract in the blockchain, tokenization becomes simplified for the players, making transactions between players much freer. To realize a platform with MOLD, features such as the above will be required, including the existence of a protocol which makes possible for a better user experience.

### 4.2 Issues to the Ethereum and the Need for TPS

Ethereum made it possible to realize next-generation smart contract by filling the blockchain used in the Bitcoin with a Turing-completed expanded terms. In reality, there are numerous decentralized applications being developed that are based on the Ethereum. Unlike Bitcoin that uses UTXO (Unspent Transaction Output) to present its currency, Ethereum stores data in the state transition

inside the blockchain and its "State" is represented as an object referred as the "Account". (Appendix C: UTXO vs Account-Base) An "Account" will be classified as a Contract Account, managed by its own contract code and a secret key managed by the EOA (Externally Owned Accounts). Two types of account data will be preserved on the blockchain using a state transition function, and implementation of a smart contract executed when certain conditions are met. The Ethereum is an innovative platform as the ultimate-abstract base layer, built with a protocol able to implement various decentralized applications. However, there are issues becoming prevalent as more users enter the Ethereum network.

Because the Ethereum network is a platform that makes it possible for all decentralized applications to be implemented, various projects (besides games) are concurrently developed over the Ethereum. Therefore, there is a need for the Ethereum network to process an enormous amount of transactions, with 2018 being increasing up to a maximum of 30,000 cases of unidentified transactions, of which transaction fee will be so expensive. When looking at TPS (Transaction per Second), although it improves upon when compared to Bitcoin, Ethereum number of about 7 to 8 times is clearly insufficient to handle the anticipated increases in the network. In addition, in a gaming industry where immediate means of payment are required, this will lead to a significant decrease in quality to the user experience. Suggestions for improvement based on off chain technology have been discussed, however, the timing of implementation and feasibility are still unclear. In addition, it should be noted that systems rolled back when dealing with the problems to the DAO, and that certain parts of the community broke down due to hard fork. Using Ethereum contains the several issues and risks as various projects becoming intertwined, and in order to realize a free virtual world aimed by MOLD, an innovative framework that specializes in a high-quality user experience will be important.

### **4.3 Token Model**

#### **4.3.1 Main Currency over the MOLD platform**

On the MOLD, users can freely trade their item-tokens they own as digital assets. It is at this time that moldcoin be suggested being used as the main currency. When users buy and sell their item-tokens, trading can be made possible with moldcoin owners. Trading through moldcoin as a main currency can take place in the DEX built over the MOLD platform. For example, when the user leaves Game A, the player may tokenize the items gained within Game A and exchange into moldcoin. The player can then use the moldcoin to purchase items within Game B. In addition, due to state transition of smart contract occurring during the transceiving/receiving of item-tokens and tokenization in-game, moldcoin can be used as a "Gas". Furthermore, by preparing SDK for a payment structure with moldcoin, game developers can easily use moldcoin as a way to settle an account, creating a free-economy within the game world based

around moldcoin.

The term "moldcoin" mentioned within this whitepaper is defined as being built over the MOLD chain. A moldcoin(ERC20) compliant to a Ethereum-based ERC20 token should be called as moldcoin(ERC20), and considered separate from a moldcoin. The amount of moldcoin (ERC20) issued is 2.5 billion MLD, of which 300 million MLD will be devoted to the development team, and the remaining 2.2 billion MLD all being distributed by January 2018. For details regarding moldcoin(ERC20), information is available through our contract address (0x52E30201f31283dc5F7928b4198896083F604416). Furthermore, moldcoin(ERC20) will be considered to be compatible with moldcoin, and possible to trade 1 moldcoin against 1 moldcoin(ERC20). In addition, a moldcoin(ERC20) will be burned the moment it is exchanged into moldcoin. moldcoin will come to be used by the various stakeholders involved in games to help usher the growth and development of the MOLD gaming platform.

Appendix B: Revenue Structure over the MOLD

## 4.4 MOLD Function

### 4.4.1 Wallet and Account

Currently, cryptocurrency transaction by users are typically processed by using specialized wallets. But it involves many complicated processes and when concurrently using existing services over the gaming platform, it significantly decreases the quality of the user experience. However, wallets used over the MOLD are associated by in-game IDs and transactions between players will be implemented as fast and simple as possible.

MOLD wallets can support all tokens issued over the MOLD platform, and it can also secure and safeguard not just moldcoin, but item-tokens from various other games as well. In addition, like that of conventional wallet services, aside from sending moldcoin and item-tokens to the address of a third party with a MOLD wallet, it can access MOLDEX (detailed in 4.4.3) to buy and sell item-tokens between users.

To play the games on the MOLD platform, the user first creates a MOLD wallet. Upon creating the wallet, a MOLD ID will be assigned per user. By logging into the wallet using the MOLD ID and the password generated when creating the wallet, users can simultaneously manage the account balance of moldcoin and item-tokens, in addition to setting up the registered game account. The wallet and the game account are associated by the MOLD ID, whereupon by logging into the wallet, the user has simultaneously logged into the game account, making possible to switch to playing the game at the one tap. By integrating the game account and wallet features through association by the MOLD ID, users are free from the conventional hassles of having to separately manage your game account and wallet (separately login to both wallet and game accounts, or login to the wallet account only when transactions of item-tokens

and purchasing items become necessary), which enhances the user experience. Regarding existing games, by having the game companies incorporate SDK (detailed in 4.4.6) to tokenize items, this will make it possible for items managed over the MOLD chain to appear in existing games, making . At such time, conventional users still not registered to the MOLD wallet can participate in item transactions just by generating a new MOLD wallet. Furthermore, by including features such as chats, friends and group functions, there will be more active exchange between players, blurring the line between games.

#### **4.4.2 Tokenization**

In a next-generation decentralized gaming platform, players hold ownership to their in-game items as digital assets, and are free to actively engage in transactions. In such an environment, tokenization is a feature that most characterizes this platform. In-game items secured in the servers by conventional operators can be managed, traded, bought and sold by the users through the utilization of blockchain technology, which in turn, creates an enormous economy within the virtual space as a second world.

There are two types of tokens. Fundible (can be substituted) and Non-Fundible (cannot be substituted) tokens. The former, of which can be exemplified as a potion common throughout the game, supports the ERC-20 token over the Ethereum. A game item as a Fundible token could each be substituted, an example being 1 token owned by Molca holding the same value as 1 token owned by Molna. However, most games include unique items with variables in value to make such in-game universes more exciting. For such in-game items with unique Levels, attack powers and skill sets, these status parameters will each be stored in-game as meta data and be turned into Non-Fundible tokens. This, corresponding to the ERC-721 token over the Ethereum, becomes an irreplaceable kind of a token. In this case, if 1 token owned by Molca and 1 token owned by Molna were to be exchanged, it could not be considered as having an equivalent value. In either case regarding any item tokens, the user has ownership as a digital asset over the MOLD, making it possible to simplify the transaction using MOLDEX, etc (detailed in next chapter). In addition, MOLD will facilitate SDK (detailed in Chapter 4.4.6) as a system for easily allowing both tokens to be issued by the game developers.

#### **4.4.3 MOLDEX and MOLD Auction**

Most current cryptocurrency transactions are processed through an Exchange operator. A centralized approach is made by the Exchange admin side, regarding the decision-making process hence such an Exchange is called the Centralized Exchange. Users will send assets via their wallet to the Exchange 's wallet, where the user 's account balance will be managed within the database at the

Exchange. With the assets itself being stored within the Exchange. Therefore, users are forced to trust the Exchange and their digital assets completely held by a third party (Exchanges). In a centralized Exchange, there are an abundance of cases where the Exchanges themselves make off with user assets or have hacking incidents where customer information is leaked. Due to a single point of failure, there are also risks of access concentration and DDoS attacks. Under the such situations, secure transactions are threatened not because of the blockchain itself, but because of the Exchange server which goes down. On the other hand, an Exchange running on smart contracts without a central operator is called Decentralized Exchanges. Users are responsible to manage their own assets and during an exchange, users are able to deposit by sending their tokens to the contract address via their wallet, making transactions possible without trusting a third party. However, compared to a Centralized Exchange, due to low user numbers and lacking in fluidity, it is not practical yet.

With the above in mind, in order to realize a distributed market of item-tokens without going through a third party, in the MOLD, a MOLDEX will be built to establish an environment where players can freely buy and sell item-tokens. With a MOLDEX, various item-tokens can be exchanged over the MOLD platform using the moldcoin as the basic currency. Therefore, Bob can sell off the item-tokens from Game A to purchase item-tokens from Game B, and then itemize it to use as an item within Game B. The exchange rate between item-tokens and moldcoin will depend on the market, with market pricing being equated to match the supply and demand. With scarcity becoming the template for how high in value an item will be, as more economic activity by the players becomes prevalent in the virtual space, a virtual economy through the transaction of item-tokens over the MOLDEX will be established. Even MOLDEX, because of its impracticality without fluidity, an ongoing project to adopt a mechanism to automatically determine the token price and fluidity, thereby making it possible for an immediate payment method called the Bancor protocol[3], are being discussed to introduce.

In addition, regarding rare item-tokens of which only a small amount are issued, the selling and buying at DEX will not be sufficient, so instead a system called a MOLD Auction will be adopted, and auctioned off by bidding within a restricted time. Since based on smart contract, players seeking to sell item-tokens can sell off to the highest bid by only setting the submission deadline.

#### **4.4.4 Escrow Transactions between Players**

If wishing to directly have a transaction with a third party you have become familiar through the gaming community, dishonest transactions can be avoided by using the escrow transaction established over the MOLD. Consider the following simple example. Alice and Bob became friends through the chat feature and they both agree to exchange an item she owns from Game A with an item

that he owns from Game B. Now although it is possible for Alice to send the item-token to Bob, if Bob held malicious intent, there is the possibility that Alice may send her item to Bob, but Bob may not in turn send his item to Alice. Then, Alice will become victim of fraud. Escrow transactions over the MOLD make it possible to use smart contracts. After both sending the item-token to their respective escrow address, the smart contract automatically sends the item-tokens, so that Alice will receive the item from Game B, and Bob will receive an item-token from Game A. In addition, in case Bob fails to send an item-token from Game B to the escrow address within the time limit, Alice can prevent wrongdoing by setting the limit time in the smart contract to make a rule to have her item-token from Game A to be returned.

#### 4.4.5 MOLD ICO

Currently, many of the development for MMORPGs and SMS games are being done by small to medium scale companies under subcontract from the major game companies. Even applications such as mobile games can now be developed by individuals, so the conventional method of having to be affiliated with a major game company in order to create games have been steadily changing.

Over the MOLD, an ICO (Initial Coin Offering) will be established, aimed at placing a system for anyone, including freelance developers and small to medium scale companies short on funding, to freely recruit a project team and/or attract funding. Game developers who provide ICOs can propose whitepapers and game designs to the community that clearly indicates the ideas and merits to the patrons of new games. Users can then decide whether or not to invest in such a project after strict scrutiny and discussion within the community. Investors can transfer moldcoin to the contract address provided by the game developer hosting the ICO, and receive the native tokens. Owners of native tokens will be the recipient of various merits provided by the host of these ICOs, such as preferential acquisition of rare items at the launch of a game, or receive X% of the game sales in moldcoin automatically based on smart contract. This ICO model, from the side of investors will not only support new games, but will allow developers to solicit funding and smooth out the development process. This will create a cycle leading to more and more new games over the MOLD, and with the advent of an increase in games, lead to an increase of new users and contribute to the further growth of the MOLD platform.

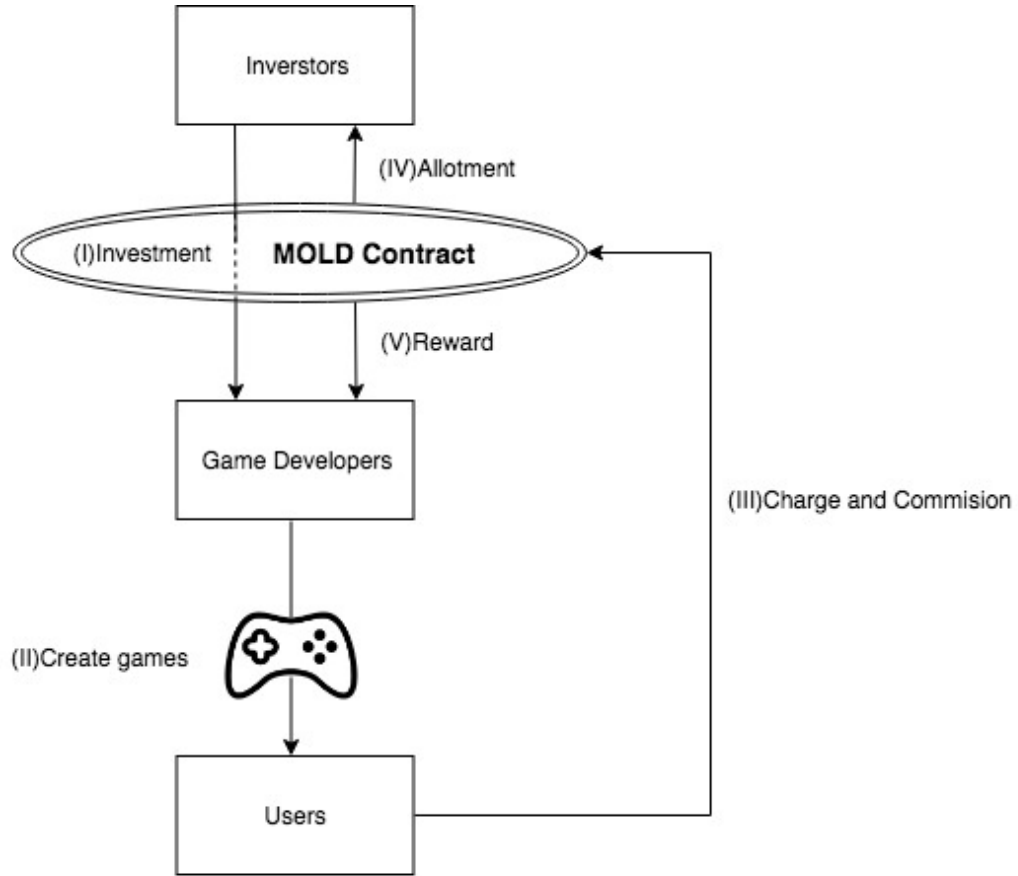


Figure 1: MOLD ICO System

The following will demonstrate a simple flow of the MOLD ICO.

- (I) Investors can invest in moldcoin against an ICO issued over the MOLD platform.
- (II) Game Developers can use the moldcoin raised in the MOLD ICO as funding to advance game development.
- (III) When users play the game, at which point the fees paid by the users to purchase or tokenize items will be sent to the MOLD smart contract address of the game.
- (IV) Based on smart contract, out of the sales generated, a predetermined portion will be immediately returned back to the investors.
- (V) after deducting the dividends for investors (IV), the remains becomes the revenue for the Game Developer.

Traditionally, when establishing game funding, funding could only receive back a dividend that were of a prescribed percentage after the closing of an account. Gaming companies had incentive to increase expenses to reduce the profit margins to the investors as much as possible. In addition, dividends took several months to actually be returned to the investor, further hindering po-



tential investors into entering the game industry. In using the MOLD ICO, game developers can efficiently raise the funds and build teams to concentrate on developing games. Due to a “trustless” system employing a smart contract, investors too can actively invest in game projects without worrying about any wrongdoing from the developer side. At the same time, a portion of the native token issued in the MOLD ICO are considered as security tokens, and risks conflicting with international law. For this reason, game developers must be compliant to the laws per region. For example, when hosting an ICO, implement it under cooperation with a traditionally licensed funding organization.

#### 4.4.6 MOLD SDK

Provide an SDK so that any game developer, conventional or not, can easily participate into the MOLD community, and create a decentralized gaming platform. For example, many games today are created using software such as the Unity and Unreal Engine. By tokenizing the game items created by these software, and providing an SDK making possible for an instantaneous payment system, these will allow developers of conventional game designs to easily adjust into the MOLD. When adopting payment systems over existing platforms, fees of up to 30% to 70% were required. However a transaction using a SDK on the MOLD, various languages such as Java will be supported from time to time, and regarding SKD support per programming language, a suitable language for game development such as C# will be provided.

### 4.5 Block Structure

Referring to the Ethereum block structure[4], Blocks over the MOLD blockchain are comprised of a block header known as information aggregation, and transaction. Within the block header contains information, such as in the following figures. Block header contains

- PreviousHash : hash value of one previous block header
- Txn Root : hash value of the root node of the transactions tree
- StateRoot : hash value of the root node of the state tree
- ReceiptsRoot : hash value of the root node of the receipts tree
- TimeStamp : a suitable UNIX time during block formation
- Height : the number of blocks at 0 Genesis blocks
- Nonce : a random 64bit number or string of characters
- NextMiner : contract address of the next miner

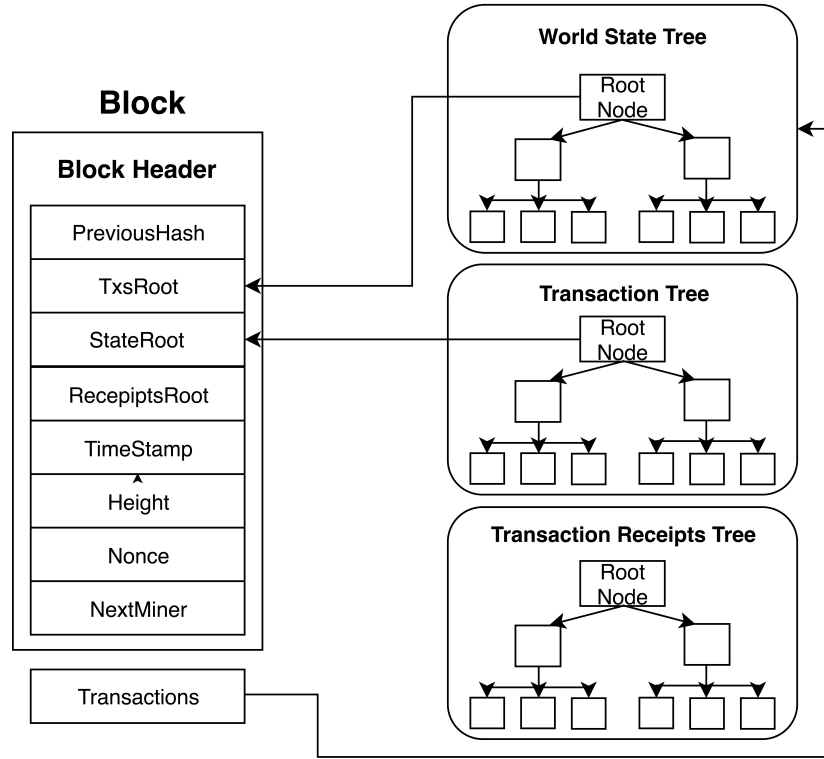


Figure 2: MOLD Block Structure

There are 2 types of transactions, transmission of actual moldcoin, or transmission/publishing of item-tokens. Both are clearly distinguished over the MOLD blockchain. Regarding the transmission of moldcoin, it will be done through the UTXO method adopted by bitcoin and the balance calculated based per transaction. Since it is based on the UTXO method, parallel processing can be done simultaneously, which in turn, makes it possible for one person to send to multiple people. Each transaction by UTXO will be hashed using encryption technology such as the SHA256 function, and a TxRoot is generated based on the Merkle tree concept. The part stored in the block header will be this part of the TxRoot. On the other hand, during the generation of the item-token, contract for issuing a token will be generated and then saved to each account as Account State. In addition, the Account status, or the Account State that shows information such as the kind of item-tokens being owned, will be hashed in accordance to the Mackle Patricia Tree, whereby all account information compiled by the hash will be stored within a block as a State Hash. Within the Contract Account, an account-based way to record the kind of item-tokens contained within the account at a certain point is taken.

## 4.6 Consensus Algorithms

### 4.6.1 Problems Facing the Current Consensus Algorithm

The consensus algorithms widely used today cannot be said to have the sufficient algorithms in achieving the Design Goals mentioned in Chapter 4.1. PoW consensus algorithms are zero-sum games, and executes authorization processes based on the computational power of miners. Specifically, it provides authorization to the initial node that finishes computing the enormous load required in the hash computation. Due to current increases in transaction loads, Difficulty requires super computers and large servers, leading to the consumption of a heavy amount of power, and vulnerability to 51% attacks. In addition, massive Miners hold advantage due to economies of scale. Economies of scale meaning, a miner able to raise a cost of 100 million Yen will be able to profit 100 times the amount compared to a miner only able to raise a cost of a million Yen. This is due in part to cost reductions stemming from large-scale productions and mining in favorable geographical positions in the network. Furthermore, there are an unspecified number of authorization process in PoW, inevitably leading to a time-consuming approval process, of which are not favorable to games requiring an immediate means of payment.

PoS is a system providing authorization rights dependent on coin age and volume amount in ownership, and do not have problems such as massive power consumption faced by PoW. However, there is the possibility that due to investors with plenty of capital having a preferential initiative to generate blocks, thus leading to an oligopoly and lower the circulation of the currency. In addition, since in a PoS, it is generating blocks are relatively easy, and it faces the “Nothing at Stake” problem of being able to generate blocks without risk.

### 4.6.2 BFT Systems

BFT[5] solves the uncertainties of finality and performance problems which were the demerits faced by PoW and PoS. Unlike PoW and PoS, blocks are generated after decision made by the validator, which in effect do not generate branching in the blockchain. Therefore, as confirmed blocks are not overturned, it ensures finality in addition to no longer needing calculations until meeting a criteria like the PoW, making such a system extremely fast performance-wise. To realize a smart economy, NEO adopts dBFT, while the Linux Foundation, of whom is pushing Hyperledger Fabric is adopting PBFT. In case the validator, of which will become a tentative leader to the DBF, holds malicious intent, other validators will monitor the movements of the leader and when determined that it has acted fraudulently, another new leader can be replaced after application by majority decision, making it fault-tolerant and strong algorithm. When a validator is found to have malicious intent (including validators with faulty functionality), such a validator will be excluded from the validator pool, as well as confiscating any moldcoin it had deposited [refer to Punitive Algo-

rithm]. Byzantine Fault Tolerance, in regard to consensus systems by N amount of nodes, provides the  $f = (n-1) / 3$  fault-tolerance. This guarantees the functionality and stability of the system by not having a node error consensus exceed past “ $(n-1) / 3$ ”. Blockchain’s general ledger are maintained by the bookkeeper node, and by having the node usually not participating in the consensus, simplifies the process of consensus-building. This tolerance capacity ensures the security and usability, and is suitable for any environment.

Blockchain is a decentralized ledger system that connects participants through the P2P network, broadcasting all messages within. Nodes have 2 types of roles, a normal and a bookkeeper role. Normal nodes transfer and exchange via the system to receive ledger data. Whereas the bookkeeper node provides accounting work to the entire network to maintain the ledger. The authenticity and integrity of the transferred information will be guaranteed by encryption, along with requiring the sender to attach their signature to the hash value in the message they have sent.

In a consensus algorithm of the MOLD, an N amount of people selected as validators from a node [refer to Selection Method of Validators] pool with validator-qualifying criteria, are all provided a certain amount in moldcoin to validate them as suitable validators to participate in the bookkeeping. Each validators are provided pseudo random numbers from 0 to n-1, and provide authentication work per period (epoch). Upon finishing authentication work per epoch, each validators are free whether or not to continue or to quit the next authentication work. Validators are supplemented by being chosen from the top of a node pool, in accordance with having high contribution to the MOLD.

### **Selection Method of Validators**

MOLD rankings are placed in accordance to the amount of moldcoin owned and used in the MOLD wallet. The parameters for the MOLD rankings correlate with the amount of moldcoin owned and used in the wallet. A node wanting to become validators are registered in the node pool, of which is a preliminary list for potential validators. Out of the nodes registered into the node pool, the top-ranking N amount of people will be granted rights as validators.

### Block Generation Procedure

The process of block generation under normal circumstances are shown in the below.

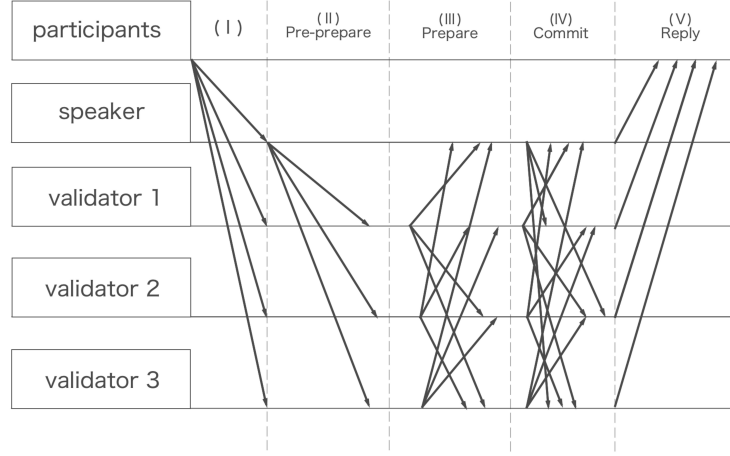


Figure 3: MOLD Block Structure

Validators are given numbers from 0 to  $n-1$  using pseudo random functions.

- (I) participants deliver transaction data signed by the sender across the network. All validators store the data in their memory.
- (II) the validator assigned number 0 from the pseudo-random function will send the Pre-prepareRequest as speaker.
- (III) validator will send Prepare to ensure proper receipt of transaction data by the other validators.
- (IV) validator will examine the data within the block, and send to all other validators only if the data is valid, whereupon reaching  $n-f$  consensus within the validators, a new block is generated.
- (V) finally, after signage by validator, the blocks are connected to the chain.

The role of speaker will then change to the number 1 validator by pseudo-random function, and the process (I) through (V) will be repeated. Within the epoch, an  $N$  amount of validators will have opportunity to become a speaker at least once, but in case a speaker cannot operate successfully, the view will be changed and the next speaker will be selected.

If there are illegal transactions amongst validators, a validator will send a Change View. If in case  $n-f$  consensus cannot be reached, the next validator chosen by the pseudo-random function will play the role of speaker.

Transaction data from the participants contain signage by the sender, making it impossible for validators with malicious intent to tamper with the transaction data.

#### **Punitive Algorithm and Validator Reward**

To actually have a proper functioning validator, a certain amount of moldcoin as a deposit need to be locked up, and in case of any malicious action to the network, a system is setup for validators to lose their privilege, in addition to a fixed amount from their deposit. The MOLD network fees (transmission fees, deploying smart contracts, summoning calls) act as rewards to the Validator. By burning the deposit of validators with malicious intent, of which will raise the rarity and value of moldcoin, this will act as incentive as denouncement towards any validators with malicious intent.

## **5 Molca Project**

The Molca Project is a project voluntarily started within the community around November of 2017, to utilize a humanoid interface named "Molca" as a guide to the decentralized platform MOLD. Molca, aside from functioning as a medium for public relations activities for the MOLD project, have become an iconic character to users within the MOLD gaming platform. In the future, with working as the MOLD public relations representative as a Virtual YouTube Star, Molca is planned to freely travel back and forth between the MOLD platform to provide assistance such as game tutorials and user support.

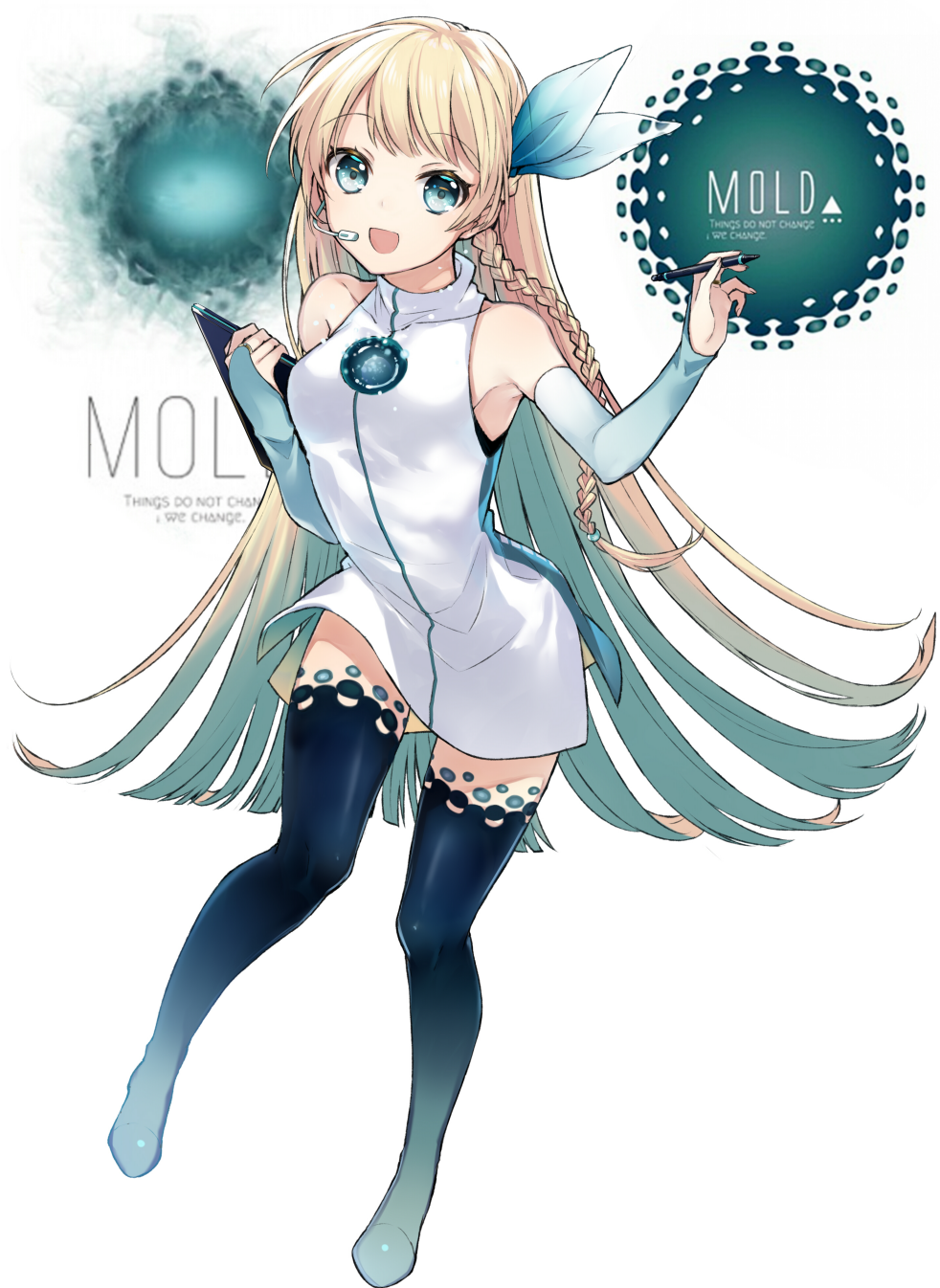


Figure 4:

## 6 Conclusion

Blockchain, as technology to authenticate transactions P2P (Peer to Peer) without the need for a centralized third party have evolved through the emergence of Bitcoin, and with it has attracted attention in various industries as revolutionary in tamper-resistant and highly available technology that allows significant savings to operation costs. Aside from aspects such as money transfers and means for payment, there have been efforts to apply it to international money transfers and IoT, with many empirical studies being done in various fields. In any case however, the practicality of such are still far from being realized, and the reality being that they are all still in the developmental phases. In 2017, various blockchain project were launched, with an enormous surge in finance activities through ICO. However, in certain circles, there were many fraudulent cases of projects that raised enormous funding through ICO by quite literally associating with blockchain terminology, when in fact there were no need to use blockchain. As "trustless" and "permissionless" being the core values of blockchain, any projects ignoring such values are in effect no different to conventional systems, and not revolutionary in creating anything next-generation. In fact, it is not so far off to say that the key to the blockchain project are to fundamentally understand key concepts of the blockchain, the community supporting the project, the significance of tokens, and the product itself. Communities are, in essence, open sourced and a bottom-to-top ecosystem with a nonprofit belief, of which are different from existing top-to-bottom business ecosystems. Tokens represents value in ownership, and though merely electronic data, holds an important role as incentive in creating a new economy within the virtual world. Products are technological deliverables itself using blockchain. If there were no value to the existence of communities and tokens, having only a product cannot be appealing enough towards the blockchain project. As there are still very few use case scenarios of blockchain, establishing a use case scenario, will realize the potential of any blockchain projects in the future.

As MOLD has aspects of a blockchain project, in the world that various attempts to implement blockchain technologies, in order to establish a presence regarding use case scenarios in gaming, there is a need to build a blockchain based in practicality and associated extension applications. In order to achieve this, MOLD will establish item ownership to the user, focus on the tokenization of in-game items, and develop MOLDEX to foster easy trade between users, and an ICO system and SDK within the MOLD for game developers. Aside from a community-based operation, MOLD will treat moldcoin as its main currency and hold value to tokens, creating a decentralized gaming platform that will change conventional games in order to realize a token economy within the virtual world.

On the other hand, MOLD will act as ambassadors to the general public, in order to change the perception of games and how it has changed. If at any time a player feels "bored" with a game, it may be that they cannot see purpose of



the game and what lies ahead. Perhaps they are under the preconceived notion that games are a form of entertainment, and that it has no relevance to the real world. However, with the evolution of e-sports, conventional concepts regarding games are starting change around the world. In addition, by using blockchain technology, though still in developmental phase, will make it possible to store digital data in a decentralized way, all the while being tamper-proof and highly available. The days of game playing amounting to nothing in the real world is rapidly closing. We are now at the forefront of the game industry where game play will lead to impressive, accolades and accomplishment in the real world. Reflecting on such a time, MOLD as a decentralized gaming platform, will understand the point of view by the player and provide new value to games. There may be diversity in the feel, the accolades and the accomplishments felt per player, but MOLD will aim to re-clarify such vague notions and promise to build a "Completely Free and Realistic" virtual reality. We believe our young generation to be the creators of the new era.

MOLD: For all the games enthusiasts

## References

- [1] Satoshi Nakamoto. "Bitcoin: A Peer-to-peer Electronic Cash System." <https://bitcoin.org/bitcoin> October 2008
- [2] Ethereum.<https://ethereum.org>
- [3] Eyal Hertzog. "Bancor Protocol Continuous Liquidity for Cryptographic Tokens through their Smart Contracts " <https://about.bancor.network/>
- [4] DR. GAVIN WOOD. "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BYZANTIUM VERSION " <https://ethereum.github.io/yellowpaper/paper.pdf>, April 2018.
- [5] Castro M, Liskov B. "Practical Byzantine fault tolerance" <http://pmg.csail.mit.edu/papers/osdi99.pdf> ,february 1999.
- [6] SECURITIES AND EXCHANGE COMMISSION, July 25, 2017 "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO" <https://www.sec.gov/litigation/investreport/34-81207.pdf>
- [7] Hyper Ledger <http://hub.digitalasset.com/blog/retiring-hyperledger-beta-re-opensourcing-soon-and-other-changes>

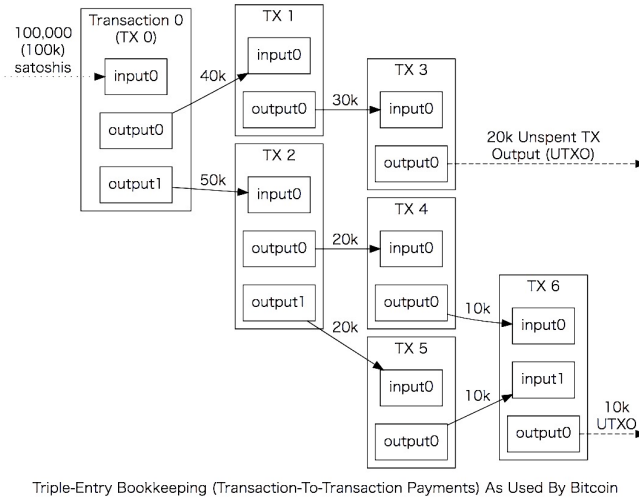
## Appendix A: Decentralized Autonomous Organization

One reason behind blockchain technology becoming greatly appreciated today is the elimination of a centralized operator through blockchain protocol and realizing a decentralized autonomous organization (DAO). Concepts of a decentralized autonomous organization have existed prior to the advent of blockchain. Generally, organization structures that use majority decisions of 67% or higher made by members or shareholders to agree to contract modifications and joint materials can be thought of being similar in concept. But a concept realizing blockchain technology based on encryption theories was a first. With the flourish in the cryptocurrency market, there have been many various projects all claiming to be "blockchain technology". However, the essence of the blockchain technology is advocating for a new form of organization management, made by changing the decision-making process and incentive structures. Since the MOLD, in accordance with encryption theory, is a decentralized platform that organically continues growing using blockchain technology, fees to release games are 0%, promoting further economic activity within the game world. Gaming platforms based on the MOLD chain, instead of a centralized operator, will take the operation form of a decentralized community overlapping improvements made by contributions from game enthusiasts, all act voluntarily.

## Appendix B: Revenue Structure over the MOLD

As MOLD aims to be a easy and low cost platform for game enthusiasts to contribute to, fees for game developers to use the platform are 0%. Therefore, since the operational structure of MOLD will adopt a community-based cooperative effort by those approving of the principles set forth by MOLD, there will be no structure in place for the operator to benefit financially. The main reasoning behind MOLD not adopting a revenue structure is to encourage the entry of many users due to the low cost, but discussion regarding the legality will be important as well. As a use case scenario, in 2016 there was a revenue distribution structure incorporated into a decentralized autonomous organization called the "The DAO". Regarding "The DAO", in July 25th 2017, the United States Securities and Exchange Commission (SEC) published a paper indicating that "The DAO" fell under "Securities" and will be subject to United States securities regulations[6]. Since revenue distribution structures can be subjected to security regulations by the government, there should be consideration that there is the likelihood of damage caused to the operation of the platform.

## Appendix C : UTXO vs Account-Base



Many cryptocurrencies including bitcoin and that are derived from this, are managed based on the UTXOs (an Unspent Transaction outputs) model. By collecting UTXOs from past transaction histories, and then creating other new UTXOs, such UTXOs will be used in future transactions as continuous forms of currency. At this time, each UTXO can be considered similar in concepts to existing coins. As this method is supported by numerous projects after bitcoin, the following has been stated as reasoning for Hyperledger to adopt UTXOs[7].

”We are also switching from our simplistic notion of accounts and balances to adopt to de facto standard of the Bitcoin UTXO model, lightly modified. While Hyperledger does not use Bitcoin in any way, the Bitcoin system is still extremely large and innovative, with hundreds of millions of dollars invested. By adopting the Bitcoin transaction model as standard, users of Hyperledger will benefit from innovation in Bitcoin and vice versa, as well as making Hyperledger more interoperable.”

Regarding the consensus system of the blockchain network, it is crucial that all nodes participating will process transactions in equal order to reach a comparable conclusion. Therefore, in order to gain consensus from the participants, execution of a parallel process and scale expansion will be required, at which time the basic structure of transaction taking place will be crucial. In contrast to the UTXOs model adopted by bitcoin, Ethereum adopts the account state transition model, and understanding the advantages and disadvantages of these models will be necessity. Unlike the UTXOs model, Account model is closer in concept to managing a bank account, and presents its currency by simply saving

the state transition of the currency balance per user account. There are disadvantages however, such as his system leaks the account balance information. Further discussion regarding UTXOs and Account models can be summarized in the below.

## **Advantages of the UTXO model**

### **Parallel Processing**

Though dependent on how owners manage their coin, users can make it difficult to associate the account to the address by using a new wallet per UTXOs. This is a suitable characteristic of currency. In an Account model, privacy management using this method will be difficult, so a system such as a zero-knowledge proof will be required.

### **High Level of Privacy**

Though dependent on how a owner manages the coins, users can make it difficult to associate the account to the address by using a new account per UTXOs. This is a suitable characteristic of currency. In an Account model, privacy management using this method will be difficult, so a system such as a zero-knowledge proof will be required.

### **Potential Scalability**

UTXOs models have characteristics suitable solving scalability problems regarding certain perspectives. For example, in a UTXOs model, if a part of the data from the Merkle tree is lost, only the owner of the currency suffers damage. In an Account model, in addition to the owner, all other accounts who had association by such as messaging through their accounts, will suffer losses as well.

### **Reentrant to Reentrancy**

Due to UTXO being simply managed by boolean, it does not face the problem of deterioration due to unexpected reentrancy. This is a big problem raised during The DAO attacks at the initial stages of Ethereum.

## **Advantages of the Account Model**

### **Simplicity**

In a UTXOs model, when managing multiple UTXOs using the wallet, it requires to think of appropriating all UTXOs. But in an Account model, it only requires to simply read the balance from the database.

### **Fungibility**

As each set of coins does not preserve the block chain at the code level,

substitution possibilities of each coin remain intact, and does not store specific information.

### **Ease of Reference by Light Client**

Although the light client on the other hand can gain all information pertaining to a single account by following the state tree in an Account Model, from the perspective of the UTXO, each transaction differs per reference point, making it a complicated system. In addition, integrating services such as wallets becomes relatively easy. When executing a smart contract for the above data structure, the workload will be heavy.

## 7 Note

The information contained herein is only to stimulate discussion amongst the community, and not intended to induce any sales of MOLD or the related company's share or securities. Any such solicitation will be made in accordance to the relevant legal terms. The information and analysis provided in this document shall not be used as basis for judgement on investment and shall not include specific recommendations. Therefore, this document does not offer views or suggestions related to or leading to investment. The purpose of this document is not to market or induce securities. MOLD will not be responsible for any loss or damage of any kind, whether directly or indirectly caused by errors, omissions or inaccuracies recorded in this document. In addition, the information recorded in this document shall be subject to change without notice. Please note the possibility of modifications to this document (edition 1.0) in the future, and any such modifications shall be specified. Please refer to the MOLD webpage (<https://moldproject.org>) for the updated version of the document.

### **1. Moldcoin Access Risk Due to Loss of Credential Information**

The buyer's moldcoin is associated with the Ethereum wallet address before it is allocated. The address of the Ethereum wallet is the information that managed by the buyer himself. If the information is lost, the loss of the authority to login may cause loss of moldcoins. The buyer must keep the information of private key safely in more than one, or in physically work-independent place with backup.

**2. Risk Associated with Buyer Eligibility** Users with their account information or any third party with access to secret keys can perform moldcoin-related operations. To mitigate this risk, users should use electronic devices to prevent unauthorized access.

### **3. Risk Associated with Regulatory Measures and Legal**

**Amendment** Block chain technology is the subject reviewed by regulators around the world. MOLD and moldcoin may also be affected by any investigation, regulatory measures or amendments to the law, which may hinder or restrict MOLD.

### **4. Risk Associated with Lack of Attention to Games or Distributed**

**Applications** It is possible that the attention to MOLD and moldcoin is only limited to people who care about the production and development of decentralized applications and those who are interested in games, but not used in most businesses, individuals and other organizations that are unrelated to games. The lack of attention by people other than the limited population above may have an impact on the development of MOLD and the potential value of moldcoin.

**5. Risk Associated with Buyer ' s Dissatisfaction with MOLD upon Completion** MOLD is still in the planning stage, and substantial changes to the contents will still be possible before launch. Due to changes to planning

and implementation at the designing period, or other reasons including the running of MOLD, it is possible that the forms or features of the moldcoin or MOLD that buyers purchased fall short of their expectations.

**6. Risk Associated with Theft and Hacker Attacks** Hackers and other groups or organizations may damage the usability of MOLD or moldcoin by various means such as Denial of Service, Sybil attack, Spoofing, Smurf, malware and protocol-based attacks.

**7. Risk Associated with Weakness and Vulnerabilities in Encryption**

With advances in the encryption technology and quantum computer, more risks may emerge in the field of encryption and MOLD, resulting in moldcoins being stolen or lost.

**8. Risk Associated with Insufficient Use or Utilization of MOLD**

While moldcoin should not be seen as an investment, it has the potential to have values over time. If MOLD is not fully utilized or used, moldcoin values may be limited. If the above becomes true, the platform will start with almost no market, which may limit the value of moldcoin.

**9. Risk Associated with Uninsured Loss** Unlike bank accounts or accounts associated with other financial institutions, funds held with MOLD are not insured. When a loss or loss of value occurs, no public insurance company such as Federal Depository Insurance Corporation or a private insurance company will provide any relief measures.

**10. Risk Associated with Dissolution of the MOLD Project** The MOLD project may dissolve if it is unable to implement out of reasons including but not limited to: unfavorable changes in the values of Bitcoin, Etherthe and/or moldcoin or the lack of business relationships.

**11. Risk Associated with MOLD Malfunction** MOLD may be subject to system failure due to the low value of moldcoin.

**12. Unforeseen Risks** Encrypted token is a new technology that is not encrypted. In addition to the risks described above, the MOLD development team will face unforeseen risks. Unanticipated risks may emerge as result of unexpected combinations or changes of the risks described above.