CERES TRUST FUND

WHITE PAPER

-SOCTF-

BLOCKCHAIN BASED DIGITAL STOCK

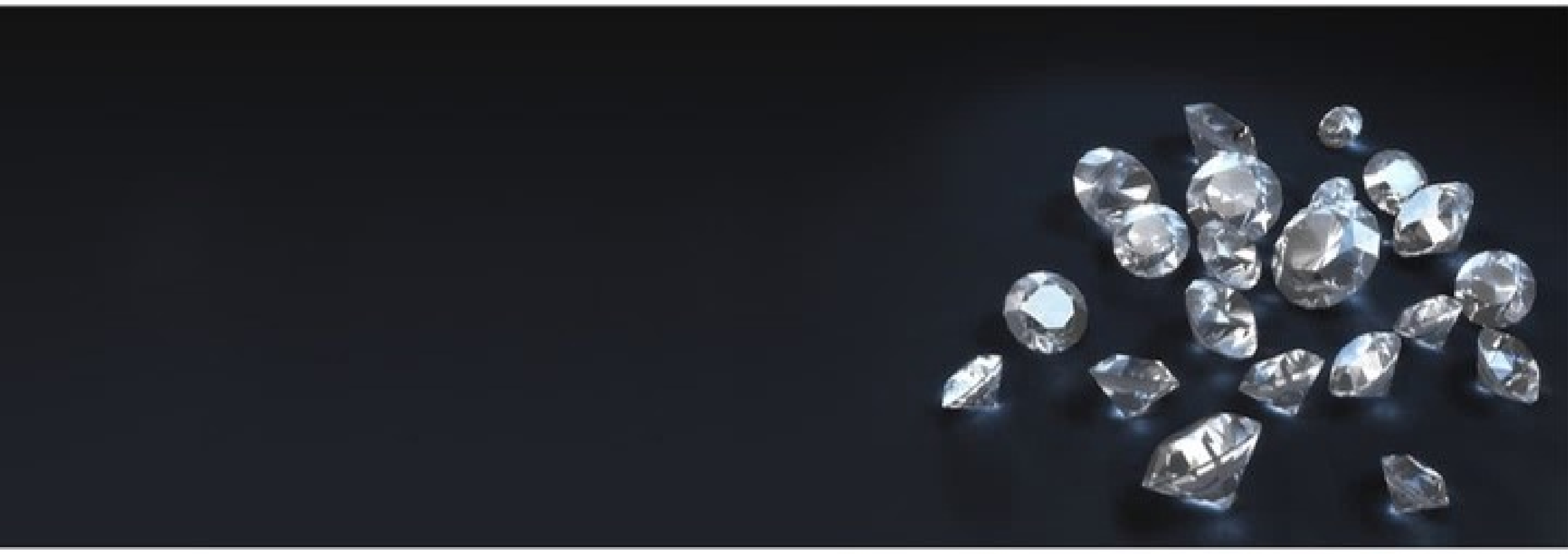
IMPORTANT NOTICE

Please read this section and the following sections entitled, "NO REPRESENTATIONS AND WARRANTIES", "REPRESENTATIONS AND WARRANTIES BY YOU", "MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS", "NO FURTHER INFORMATION OR UPDATE", "RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION", and "NO OFFER OF SECURITIES OR REGISTRATION" carefully. If you are in any doubt as to the action you should take, you should consult your legal, financial, tax or other professional advisor(s).

The SOCTF are not intended to constitute securities in any jurisdiction. This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

No regulatory authority has examined or approved of any of the information set out in this Whitepaper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

This Whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this Whitepaper is prohibited or restricted.



No part of this Whitepaper is to be reproduced, distributed or disseminated without including this section and the following sections entitled "NO REPRESENTATIONS AND WARRANTIES", "REPRESENTATIONS AND WARRANTIES BY YOU","MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS","NO FURTHER INFORMATION OR UPDATE", "RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION","NO OFFER OF SECURITIES OR REGISTRATION"

NO REPRESENTATIONS AND WARRANTIES

Ceres Global does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), you represent and warrant to Ceres Global and/or the Distributing Agency as follows:

a) You agree and acknowledge that the SOCTF do not constitute securities in any form in any jurisdiction;

b) You agree and acknowledge that this Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities in any jurisdiction or a solicitation for investment in securities and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper;

c) You agree and acknowledge that no regulatory authority has examined or approved of the information set out in this Whitepaper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;

d) The distribution or dissemination of this Whitepaper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to Ceres Global;

e) You agree and acknowledge that in the case where you wish to own any SOCTF, the SOCTF are not to be construed, interpreted, classified or treated as:

i. Any kind of currency other than cryptocurrency;

ii. Debentures, stocks or shares issued by any person or entity (whether Ceres Global)

iii. Rights, options or derivatives in respect of such debentures, stocks or shares;

iv. Rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

v. Units in a collective investment scheme;

vi. Units in a business trust;

vii. Derivatives of units in a business trust; or

f) Any other security or class of securities. you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology; and

g) All of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession this Whitepaper or such part thereof (as the case may be).

MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS

This Whitepaper includes market and industry information and forecasts that have been obtained from internal surveys, reports and studies, where appropriate, as well as market research, publicly available information and industry publications. Such surveys, reports, studies, market research, publicly available information and publications generally state that the information that they contain has been obtained from sources believed to be reliable, but there can be no assurance as to the accuracy or completeness of such included information.

Save for Ceres Global and their respective directors, executive officers and employees, no person has provided his or her consent to the inclusion of his or her name and/or other information attributed or perceived to be attributed to such person in connection therewith in this Whitepaper and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information by such person and such persons shall not be obliged to provide any updates on the same.

While Ceres Global have taken reasonable actions to ensure that the information is extracted accurately and in its proper context, Ceres Global have not conducted any independent review of the information extracted from third party sources, verified the accuracy or completeness of such information or ascertained the underlying economic assumptions relied upon therein.

Consequently, neither Ceres Global, nor their respective directors, executive officers and employees acting on their behalf makes any representation or warranty as to the accuracy or completeness of such information and shall not be obliged to provide any updates on the same

NO FURTHER INFORMATION OR UPDATE

No person has been or is authorized to give any information or representation not contained in this Whitepaper in connection with Ceres Global and their respective businesses and operations, the SOCTF, and, if given, such information or representation must not be relied upon as having been authorized by or on behalf of Ceres Global.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION

The distribution or dissemination of this Whitepaper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this Whitepaper or such part thereof (as the case may be) at your own expense and without liability to Ceres Global.

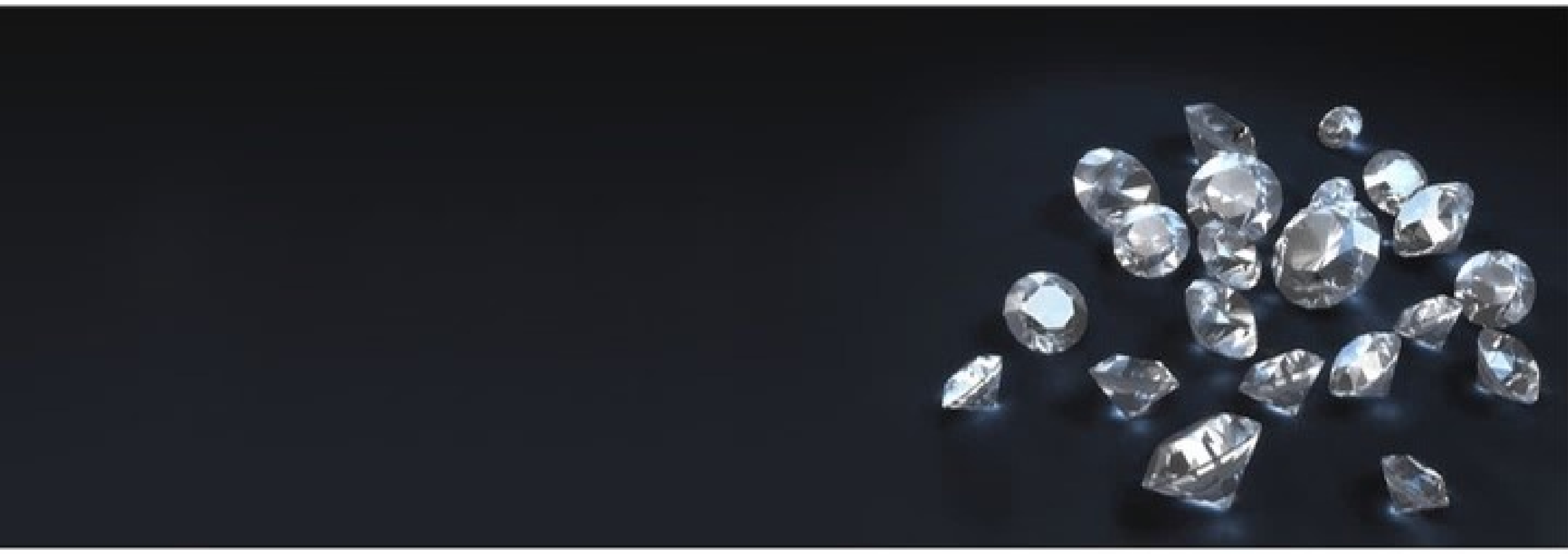
Persons to whom a copy of this Whitepaper has been distributed or disseminated, provided access to or who otherwise have the Whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

NO OFFER OF SECURITIES OR REGISTRATION

This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper.

No regulatory authority has examined or approved of any of the information set out in this Whitepaper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

CONTENTS:



1

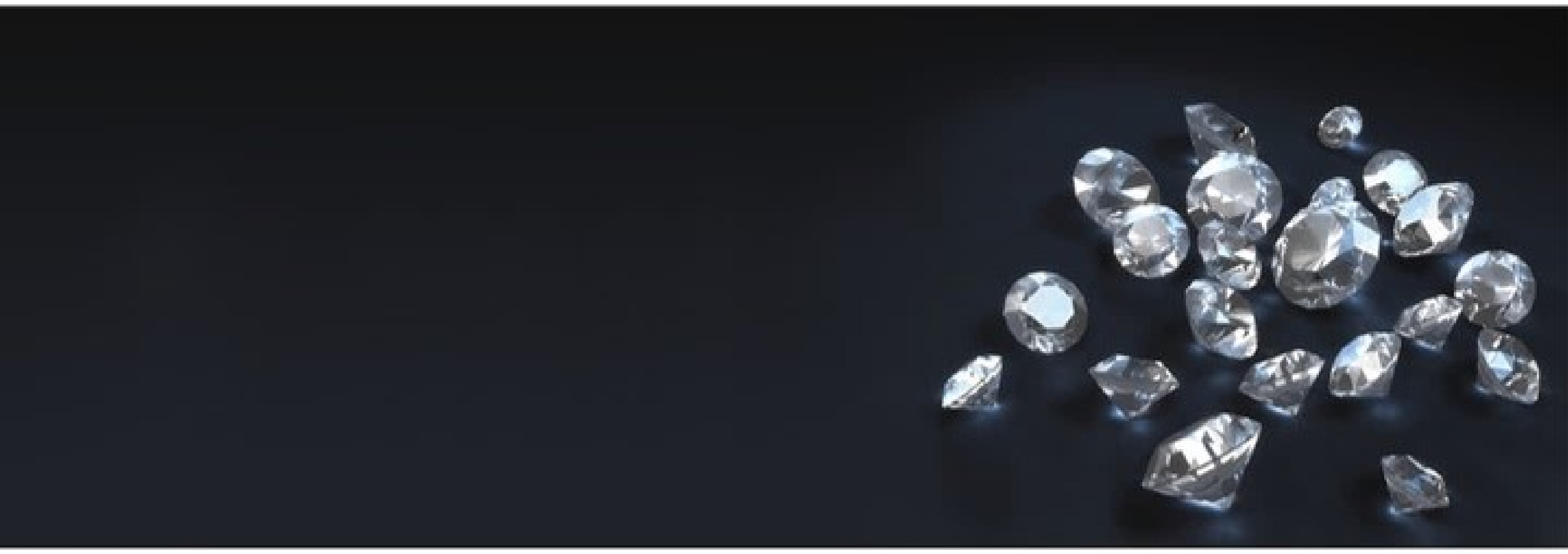
INTRODUCING CERES GLOBAL

CERES GLOBAL is a global startup that uses the latest technology including blockchain, smart contracts and machine learning to support reducing risks and frauds for banks, insurance companies and open markets in the industry, Diamond and gemstone industry. We provide a full ecosystem for the diamond industry from supply chain solutions, to diamond tracking and certification, and finally decentralized exchange for diamond trading and related services.

Block chain technology and cryptocurrencies are changing the world, and the diamond industry is no exception. Despite some new efforts, none of the blockchain ecosystems focused on the diamond industry have been designed to cover the various issues facing the industry.

The need for transparency, visibility and objectivity in the diamond industry was felt decades ago. The need for person-to-person contact when dealing with buying or selling diamonds limits the size of the market. CERES GLOBAL focuses on integrating the best features of the conventional diamond industry with the utility and functionality of the latest blockchain technology.

CERES GLOBAL builds an open blockchain-based consumer and ownership ecosystem for the diamond industry, where all diamond transactions can be conducted and coordinated with the CERES INVESTMET stock exchange trust team.



CERES TRUST FUND

Ceres Trust Fund was established in 2005 as a group specializing in providing trust services, trading authorizations, and investment management in the field of foreign exchange.

Ceres Trust Fund was founded by Ceres Global and a Wall Street group of individuals, along with analysts in the stock market such as Nasdaq, S&P500, etc. They are knowledgeable about the psychology and behavior of individual investors. as well as having seniority in the field of securities analysis in the most dynamic market in the world. With many years of experience in researching market movements, especially the changes in Wall Street from the market crash in 1929, the change of the gold standard system during World War II. US Dollar position. Until the real experience in the 90s when Asian financial markets collapsed, Gulf wars, 9/11 terrorist attacks, Iraq wars ... they accumulated a treasure for themselves. massive knowledge. The CEO of Ceres Trust Fund was also a member of the advisory team for the IMF to activate emergency monetary mechanism to help the world financial market escape the crisis in 2003.

2

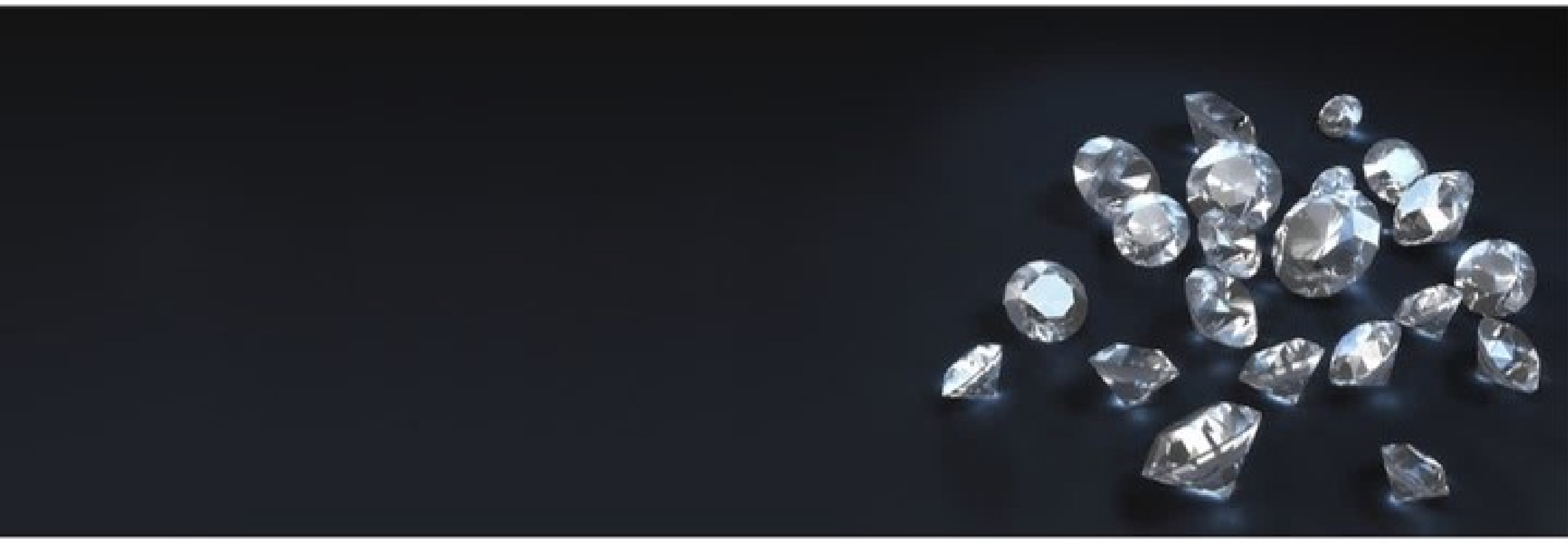
BLOCKCHAIN TECHNOLOGY OVERVIEW

National Institute of Standards and Technology Interagency has a very clear article on Blockchain Technology, document number NISTIR 8202, which ritten by Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone. In this document, we will take out some key information related to the subject of Blockchain Technology. For complete information, we encourage you to study document NISTIR 8202.

1. Introduction

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.

This technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. In Bitcoin, and similar systems, the transfer of digital



information that represents electronic cash takes place in a distributed system. Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin blockchain is independently maintained and managed by a distributed group of participants. This, along with cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later (modifying blocks or forging transactions). Blockchain technology has enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum1. Because of this, blockchain technology is often viewed as bound to Bitcoin or possibly cryptocurrency solutions in general. However, the technology is available for a broader variety of applications and is being investigated for a variety of sectors.

The numerous components of blockchain technology along with its reliance on cryptographic primitives and distributed systems can make it challenging to understand. However, each component can be described simply and used as a building block to understand the larger complex system. Blockchains can be informally defined as:

> Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

[1] Bitcoin and Ethereum are mentioned here since they are listed as the top two cryptocurrencies on market capitalization websites

1.1 Background and History

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The Part-Time Parliament [2] to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed [3]. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System [4], which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto's paper contained the blueprint that most modern cryptocurrency schemes follow (although with variations and modifications). Bitcoin was just the first of many blockchain applications.

Many electronic cash schemes existed prior to Bitcoin (e.g., ecash and NetCash), but none of them achieved widespread use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted third party. It also enabled the issuance of new cryptocurrency in a defined manner to those users who manage to publish new blocks and maintain copies of the ledger; such users are called miners in Bitcoin. The automated payment of the miners enabled distributed administration of the system without the need to organize. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain.

In Bitcoin, the blockchain enabled users to be pseudonymous. This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible. This has effectively enabled Bitcoin to offer pseudo-anonymity because accounts can be created without any identification or authorization process (such processes are typically required by Know-Your-Customer (KYC) laws).

Since Bitcoin was pseudonymous, it was essential to have mechanisms to create trust in an environment where users could not be easily identified. Prior to the use of blockchain technology, this trust was typically delivered through intermediaries trusted by both parties. Without trusted intermediaries, the needed trust within a blockchain network is enabled by four key characteristics of blockchain technology, described below:

- **Ledger** – the technology uses an append only ledger to provide full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.
- **Secure** – blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered with, and that the data within the ledger is attestable.
- **Shared** – the ledger is shared amongst multiple participants. This provides transparency across the node participants in the blockchain network.
- **Distributed** – the blockchain can be distributed. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors.

For blockchain networks that allow anyone to anonymously create accounts and participate (called permissionless blockchain networks), these capabilities deliver a level of trust amongst parties with no prior knowledge of one another; this trust can enable individuals and organizations to transact directly, which may result in transactions being delivered faster and at lower costs. For a blockchain network that more tightly controls access (called permissioned blockchain networks), where some trust may be present among users, these capabilities help to bolster that trust.

1.2 Purpose and Scope

This document provides a high-level technical overview of blockchain technology. It looks at different categories of implementation approaches. It discusses the components of blockchain technology and provides diagrams and examples when possible. It discusses, at a high-level, some consensus models used in blockchain networks. It also provides an overview of how blockchain technology changes (known as forking) affect the blockchain network. It provides details on how blockchain technology was extended beyond attestable transactions to include attestable application processes known as smart contracts. It also touches on some of the limitations and misconceptions surrounding the technology. Finally, this document presents several areas that organizations should consider when investigating blockchain technology. It is intended to help readers to understand the technologies which comprise blockchain networks.

1.3 Notes on Terms

The terminology for blockchain technology varies from one implementation to the next – to talk about the technology, generic terms will be used. Throughout this document the following terms will be used:

- Blockchain – the actual ledger
- Blockchain technology – a term to describe the technology in the most generic form
- Blockchain network – the network in which a blockchain is being used
- Blockchain implementation – a specific blockchain
- Blockchain network user – a person, organization, entity, business, government, etc. which is utilizing the blockchain network
- Node – an individual system within a blockchain network
    - Full node – a node that stores the entire blockchain, ensures transactions are valid
        - Publishing node – a full node that also publishes new blocks
    - Lightweight node – a node that does not store or maintain a copy of the blockchain and must pass their transactions to full nodes

2. Blockchain Categorization

Blockchain networks can be categorized based on their permission model, which determines who can maintain them (e.g., publish blocks). If anyone can publish a new block, it is permissionless. If only particular users can publish blocks, it is permissioned. In simple terms, a permissioned blockchain network is like a corporate intranet that is controlled, while a permissionless blockchain network is like the public internet, where anyone can participate. Permissioned blockchain networks are often deployed for a group of organizations and individuals, typically referred to as a consortium. This distinction is necessary to understand as it impacts some of the blockchain components discussed later in this document.

2.1 Permissionless

Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority. Permissionless blockchain

platforms are often open source software, freely available to anyone who wishes to download them. Since anyone has the right to publish blocks, this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain (through including those transactions within published blocks). Any blockchain network user within a permissionless blockchain network can read and write to the ledger. Since permissionless blockchain networks are open to all to participate, malicious users may attempt to publish blocks in a way that subverts the system (discussed in detail later). To prevent this, permissionless blockchain networks often utilize a multiparty agreement or 'consensus' system (see Section 4) that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system. Examples of such consensus models include proof of work (see Section 4.1) and proof of stake (see Section 4.2) methods. The consensus systems in permissionless blockchain networks usually promote non-malicious behavior through rewarding the publishers of protocol-conforming blocks with a native cryptocurrency.

2.2 Permissioned

Permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority (be it centralized or decentralized). Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions. Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals. They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals. Permissioned blockchain networks may be instantiated and maintained using open source

or closed source software.

Permissioned blockchain networks can have the same traceability of digital assets as they pass through the blockchain, as well as the same distributed, resilient, and redundant data storage system as a permissionless blockchain networks. They also use consensus models for publishing blocks, but these methods often do not require the expense or maintenance of resources (as is the case with current permissionless blockchain networks). This is because the establishment of one’s identity is required to participate as a member of the permissioned blockchain network; those maintaining the blockchain have a level of trust with each other, since they were all authorized to publish blocks and since their authorization can be revoked if they misbehave. Consensus models in permissioned blockchain networks are then usually faster and less computationally expensive.

Permissioned blockchain networks may also be used by organizations that need to more tightly control and protect their blockchain. However, if a single entity controls who can publish blocks, the users of the blockchain will need to have trust in that entity. Permissioned blockchain networks may also be used by organizations that wish to work together but may not fully trust one another. They can establish a permissioned blockchain network and invite business partners to record their transactions on a shared distributed ledger. These organizations can determine the consensus model to be used, based on how much they trust one another. Beyond trust, permissioned blockchain networks provide transparency and insight that may help better inform business decisions and hold misbehaving parties accountable. This can explicitly include auditing and oversight entities making audits a constant occurrence versus a periodic event.

Some permissioned blockchain networks support the ability to selectively reveal transaction information based on a blockchain network users identity or credentials. With this feature, some degree of privacy in transactions may be obtained. For example, it could be that the blockchain records that a transaction between two blockchain network users took place, but the actual contents of transactions is only accessible to the involved parties.

Some permissioned blockchain networks require all users to be authorized to send and receive transactions (they are not anonymous, or even pseudo-anonymous). In such systems parties work together to achieve a shared business process with natural disincentives to commit fraud or otherwise behave as a bad actor (since they can be identified). If bad behavior were to occur, it is well known where the organizations are incorporated, what legal remedies are available and how to pursue those remedies in the relevant judicial system.

3. Consensus Models

A key aspect of blockchain technology is determining which user publishes the next block. This is solved through implementing one of many possible consensus models. For permissionless blockchain networks there are generally many publishing nodes competing at the same time to publish the next block. They usually do this to win cryptocurrency and/or transaction fees. They are generally mutually distrusting users that may only know each other by their public addresses. Each publishing node is likely motivated by a desire for financial gain, not the well-being of the other publishing nodes or even the network itself.

In such a situation, why would a user propagate a block that another user is attempting to publish? Also, who resolves conflicts when multiple nodes publish a block at approximately the same time? To make this work, blockchain technologies use consensus models to enable a group of mutually distrusting users to work together.

When a user joins a blockchain network, they agree to the initial state of the system. This is recorded in the only pre-configured block, the genesis block. Every blockchain network has a published genesis block and every block must be added to the blockchain after it, based on the agreed-upon consensus model. Regardless of the model, however, each block must be valid and thus can be validated independently by each blockchain network user. By combining the initial state and the ability to verify every block since then, users can independently agree on the current state of the blockchain. Note that if there were ever two valid chains presented to a full node, the default mechanism in most blockchain networks is that the 'longer' chain is viewed as the correct one and will be adopted; this is because it has had the most amount of work put into it. This happens frequently with some consensus models and will be discussed in detail.

The following properties are then in place:

- The initial state of the system is agreed upon (e.g., the genesis block).
- Users agree to the consensus model by which blocks are added to the system.
- Every block is linked to the previous block by including the previous block header's hash digest (except for the first 'genesis' block, which has no previous block and for which the hash of the previous block header is usually set to all zeros).
- Users can verify every block independently.

In such a situation, why would a user propagate a block that another user is attempting to publish? Also, who resolves conflicts when multiple nodes publish a block at approximately the same time? To make this work, blockchain technologies use consensus models to enable a group of mutually distrusting users to work together.

When a user joins a blockchain network, they agree to the initial state of the system. This is recorded in the only pre-configured block, the genesis block. Every blockchain network has a published genesis block and every block must be added to the blockchain after it, based on the agreed-upon consensus model. Regardless of the model, however, each block must be valid and thus can be validated independently by each blockchain network user. By combining the initial state and the ability to verify every block since then, users can independently agree on the current state of the blockchain. Note that if there were ever two valid chains presented to a full node, the default mechanism in most blockchain networks is that the 'longer' chain is viewed as the correct one and will be adopted; this is because it has had the most amount of work put into it. This happens frequently with some consensus models and will be discussed in detail.

The following properties are then in place:

- The initial state of the system is agreed upon (e.g., the genesis block).
- Users agree to the consensus model by which blocks are added to the system.
- Every block is linked to the previous block by including the previous block header's hash digest (except for the first 'genesis' block, which has no previous block and for which the hash of the previous block header is usually set to all zeros).
- Users can verify every block independently.

4.1 Proof of Work Consensus Model

In the proof of work (PoW) model, a user publishes the next block by being the first to solve a computationally intensive puzzle. The solution to this puzzle is the “proof” they have performed work. The puzzle is designed such that solving the puzzle is difficult but checking that a solution is valid is easy. This enables all other full nodes to easily validate any proposed next blocks, and any proposed block that did not satisfy the puzzle would be rejected.

A common puzzle method is to require that the hash digest of a block header be less than a target value. Publishing nodes make many small changes to their block header (e.g., changing the nonce) trying to find a hash digest that meets the requirement. For each attempt, the publishing node must compute the hash for the entire block header. Hashing the block header many times becomes a computationally intensive process. The target value may be modified over time to adjust the difficulty (up or down) to influence how often blocks are being published.

For example, Bitcoin, which uses the proof of work model, adjusts the puzzle difficulty every 2016 blocks to influence the block publication rate to be around once every ten minutes. The adjustment is made to the difficulty level of the puzzle, and essentially either increases or decreases the number of leading zeros required. By increasing the number of leading zeros, it increases the difficulty of the puzzle, because any solution must be less than the difficulty level – meaning there are fewer possible solutions. By decreasing the number of leading zeros, it decreases the difficulty level, because there are more possible solutions. This adjustment is to maintain the computational difficulty of the puzzle, and therefore maintain the core security mechanism of

the Bitcoin network. Available computing power increases over time, as does the number of publishing nodes, so the puzzle difficulty is generally increasing.

Adjustments to the difficulty target aim to ensure that no entity can take over block production, but as a result the puzzle solving computations require significant resource consumption. Due to the significant resource consumption of some proof of work blockchain networks, there is a move to add publishing nodes to areas where there is a surplus supply of cheap electricity.

An important aspect of this model is that the work put into a puzzle does not influence one’s likelihood of solving the current or future puzzles because the puzzles are independent. This means that when a user receives a completed and valid block from another user, they are incentivized to discard their current work and to start building off the newly received block instead because they know the other publishing nodes will be building off it. There is currently no known shortcut to this process; publishing nodes must expend computation effort, time, and resources to find the correct nonce value for the target. Often the publishing nodes attempt to solve this computationally difficult puzzle to claim a reward of some sort (usually in the form of a cryptocurrency offered by the blockchain network). The prospect of being rewarded for extending and maintaining the blockchain is referred to as a reward system or incentive model.

Once a publishing node has performed this work, they send their block with a valid nonce to full nodes in the blockchain network. The recipient full nodes verify that the new block fulfills the puzzle requirement, then add the block to their copy of the blockchain and resend the block to their peer nodes. In this manner, the new block

the Bitcoin network. Available computing power increases over time, as does the number of publishing nodes, so the puzzle difficulty is generally increasing.

Adjustments to the difficulty target aim to ensure that no entity can take over block production, but as a result the puzzle solving computations require significant resource consumption. Due to the significant resource consumption of some proof of work blockchain networks, there is a move to add publishing nodes to areas where there is a surplus supply of cheap electricity.

An important aspect of this model is that the work put into a puzzle does not influence one's likelihood of solving the current or future puzzles because the puzzles are independent. This means that when a user receives a completed and valid block from another user, they are incentivized to discard their current work and to start building off the newly received block instead because they know the other publishing nodes will be building off it. There is currently no known shortcut to this process; publishing nodes must expend computation effort, time, and resources to find the correct nonce value for the target. Often the publishing nodes attempt to solve this computationally difficult puzzle to claim a reward of some sort (usually in the form of a cryptocurrency offered by the blockchain network). The prospect of being rewarded for extending and maintaining the blockchain is referred to as a reward system or incentive model.

Once a publishing node has performed this work, they send their block with a valid nonce to full nodes in the blockchain network. The recipient full nodes verify that the new block fulfills the puzzle requirement, then add the block to their copy of the blockchain and resend the block to their peer nodes. In this manner, the new block

gets quickly distributed throughout the network of participating nodes. Verification of the nonce is easy since only a single hash needs to be done to check to see if it solves the puzzle.

For many proof of work based blockchain networks, publishing nodes tend to organize themselves into "pools" or "collectives" whereby they work together to solve puzzles and split the reward. This is possible because work can be distributed between two or more nodes across a collective to share the workload and rewards. Splitting the example program into quarters, each node can take an equal amount of the nonce value range to test:

- Node 1: check nonce 0000000000 to 0536870911
- Node 2: check nonce 0536870912 to 1073741823
- Node 3: check nonce 1073741824 to 1610612735
- Node 4: check nonce 1610612736 to 2147483647

This is a completely new nonce, but still one that solved the puzzle. It took 90,263,918 guesses (completed in 10 minutes, 14 seconds). Dividing up the work amongst many more machines yields much better results, as well as more consistent rewards in a proof of work model.

The use of a computationally difficult puzzle helps to combat the "Sybil Attack" – a computer security attack (not limited to blockchain networks) where an attacker can create many nodes (i.e., creating multiple identities) to gain influence and exert control. The proof of work model combats this by having the focus of network influence being the amount of computational power (hardware, which costs money) mixed with a lottery system (the most hardware increases likelihood but does not guarantee it) versus in network identities (which are generally costless to create).

4.2 Proof of Stake Consensus Model

The proof of stake (PoS) model is based on the idea that the more stake user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it. Stake is often an amount of cryptocurrency that the blockchain network user has invested into the system (through various means, such as by locking it via a special transaction type, or by sending it to a specific address, or holding it within special wallet software). Once staked, the cryptocurrency is generally no longer able to be spent. Proof of stake blockchain networks use the amount of stake a user has as a determining factor for publishing new blocks. Thus, the likelihood of a blockchain network user publishing a new block is tied to the ratio of their stake to the overall blockchain network amount of staked cryptocurrency.

With this consensus model, there is no need to perform resource intensive computations (involving time, electricity, and processing power) as found in proof of work. Since this consensus model utilizes fewer resources, some blockchain networks have decided to forego a block creation reward; these systems are designed so that all the cryptocurrency is already distributed among users rather than new cryptocurrency being generated at a constant pace. In such systems, the reward for block publication is then usually the earning of user provided transaction fees.

The methods for how the blockchain network uses the stake can vary. Here we discuss four approaches: random selection of staked users, multi-round voting, coin aging systems and delegate systems. Regardless of the exact approach, users with more stake are more likely to publish new blocks.

When the choice of block publisher is a random choice (sometimes referred to as *chain-based proof of stake*), the blockchain network will look at all users with stake and choose amongst them based on their ratio of stake to the overall amount of cryptocurrency staked. So, if a user had 42% of the entire blockchain network stake they would be chosen 42 % of the time; those with 1 % would be chosen 1 % of the time.

When the choice of block publisher is a multi-round voting system (sometime referred to as *Byzantine fault tolerance proof of stake* [12]) there is added complexity. The blockchain network will select several staked users to create proposed blocks. Then all staked users will cast a vote for a proposed block. Several rounds of voting may occur before a new block is decided upon. This method allows all staked users to have a voice in the block selection process for every new block.

When the choice of block publisher is through a coin age system referred to as a *coin age proof of stake,* staked cryptocurrency has an age property. After a certain amount of time (such as 30 days) the staked cryptocurrency can count towards the owning user being selected to publish the next block. The staked cryptocurrency then has its age reset, and it cannot be used again until after the requisite time has passed. This method allows for users with more stake to publish more blocks, but to not dominate the system – since they have a cooldown timer attached to every cryptocurrency coin counted towards creating blocks. Older coins and larger groups of coins will increase the probability of being chosen to publish the next block. To prevent stakeholders from hoarding aged cryptocurrencies, there is generally a built-in maximum to the probability of winning.

When the choice of block publisher is through a delegate system, users vote for nodes to become publishing nodes – therefore creating blocks on their behalf. Blockchain network users' voting power is tied to their stake so the larger the stake, the more weight the vote has. Nodes who receive the most votes become publishing nodes and can validate and publish blocks. Blockchain network users can also vote against an established publishing node, to try to remove them from the set of publishing nodes. Voting for publishing nodes is continuous and remaining a publishing node can be quite competitive. The threat of losing publishing node status, and therefore rewards and reputation is constant so publishing nodes are incentivized to not act maliciously. Additionally, blockchain network users vote for delegates, who participate in the governance of the blockchain. Delegates will propose changes, and improvements, which will be voted on by blockchain network users.

It is worth noting that a problem known as "nothing at stake" may arise from some proof of stake algorithms. If multiple competing blockchains were to exist at some point (because of a temporary ledger conflict as discussed in Section 4.7), a staked user could act on every such competing chain – since it is essentially free to do so. The staked user may do this as a way of increasing their odds of earning a reward. This can cause multiple blockchain branches to continue to grow without being reconciled into a singular branch for extended periods of time.

Under proof of stake systems, the "rich" can more easily stake more of the digital assets, earning themselves more digital assets; however, to obtain the majority of digital assets within a system to "control" it is generally cost prohibitive.

4.3 Round Robin Consensus Model

Round Robin is a consensus model that is used by some permissioned blockchain networks. Within this model of consensus, nodes take turns in creating blocks. Round Robin Consensus has a long history grounded in distributed system architecture. To handle situations where a publishing node is not available to publish a block on its turn, these systems may include a time limit to enable available nodes to publish blocks so that unavailable nodes will not cause a halt in block publication. This model ensures no one node creates the majority of the blocks. It benefits from a straightforward approach, lacks cryptographic puzzles, and has low power requirements.

Since there is a need for trust amongst nodes, round robin does not work well in the permissionless blockchain networks used by most cryptocurrencies. This is because malicious nodes could continuously add additional nodes to increase their odds of publishing new blocks. In the worst case, they could use this to subvert the correct operation of the blockchain network.

4.4 Proof of Authority/Proof of Identity Consensus Model

The proof of authority (also referred to as proof of identity) consensus model relies on the partial trust of publishing nodes through their known link to real world identities. Publishing nodes must have their identities proven and verifiable within the blockchain network (e.g., identifying documents which have been verified and notarized and included on the blockchain). The idea is that the publishing node is staking its identity/reputation to publish new blocks. Blockchain network users directly affect a publishing node's reputation based on the publishing node's behavior.

Publishing nodes can lose reputation by acting in a way that the blockchain network users disagree with, just as they can gain reputation by acting in a manner that the blockchain network users agree with. The lower the reputation, the less likelihood of being able to publish a block. Therefore, it is in the interest of a publishing node to maintain a high reputation. This algorithm only applies to permissioned blockchain networks with high levels of trust.

4.5 Proof of Elapsed Time Consensus Model

Within the proof of elapsed time (PoET) consensus model, each publishing node requests a wait time from a secure hardware time source within their computer system. The secure hardware time source will generate a random wait time and return it to the publishing node software. Publishing nodes take the random time they are given and become idle for that duration. Once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network, alerting the other nodes of the new block; any publishing node that is still idle will stop waiting, and the entire process starts over.

This model requires ensuring that a random time was used, since if the time to wait was not selected at random a malicious publishing node would just wait the minimum amount of time by default to dominate the system. This model also requires ensuring that the publishing node waited the actual time and did not start early. These requirements are being solved by executing software in a trusted execution environment found on some computer processors (such as Intel's Software Guard Extensions5, or AMD's Platform Security Processor6, or ARM's TrustZone7).

Verified and trusted software can run in these secure execution environments and cannot be altered by outside programs. A publishing node would query software running in this secure environment for a random time and then wait for that time to pass. After waiting the assigned time, the publishing node could request a signed certificate that the publishing node waited the randomly assigned time. The publishing node then publishes the certificate along with the block.

4.6 Delegated Proof of Stake (DPoS)

The earliest consensus mechanism is the Proof of Work (PoW) consensus mechanism. This protocol is currently implemented in Bitcoin and Ethereum. In PoW systems, transactions broadcast through the network are grouped together into nascent blocks for miner confirmation. The confirmation process involves hashing transactions using cryptographic hashing algorithms until a merkle root has been reached, creating a merkle tree:

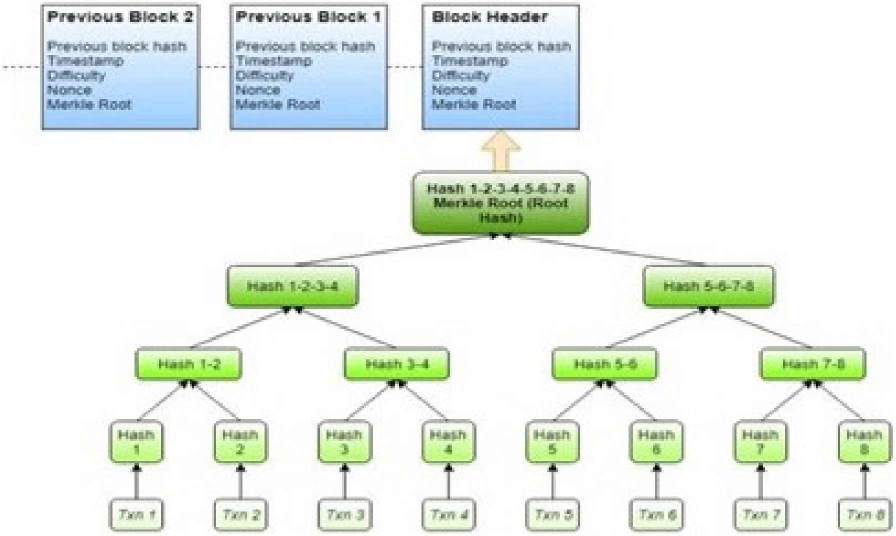


Figure 1: 8 TRX transactions are hashed into the merkle root.

This merkle root is then included in the block header, which is attached to the previously confirmed blocks to form a blockchain. This allows for easy and transparent tracking of transactions, timestamps, and other related information.

[5] Intel SGX - https://software.intel.com/en-us/sgx

[6] AMD Secure Technology - https://www.amd.com/en/technologies/security

[7] ARM TrustZone - https://www.arm.com/products/silicon-ip-security

Cryptographic hashing algorithms are useful in network attack prevention because they possess several properties:

- **Input/Output length size** - The algorithm can pass in an input of any length in size, and outputs a fixed length hash value.
- **Efficiency** - The algorithm is relatively easy and fast to compute.
- **Preimage resistance** - For a given output z, it is impossible to find any input x such that h(x) = z. In other words, the hashing algorithm h(x) is a one-way function in which only the output can be found, given an input. The reverse is not possible.
- **Collision resistance** - It is computationally infeasible to find any pairs x1 ≠ x2 such that h(x1) = h(x2). In other words, the probability of finding two different inputs hashing to the same output is extremely low. This property also implies second preimage resistance.
- **Second preimage resistance** - Given x1, and thus h(x1), it is computationally infeasible to find any x2 such that h(x1) = h(x2). While this property is similar to collision resistance, the property differs in that it is saying an attacker with a given x1 will find it computationally infeasible to find any x2 hashing to the same output.
- **Deterministic** - maps each input to one and only one output.
- **Avalanche effect** - a small change in the input results in an entirely different output

These properties give the cryptocurrency network its intrinsic value by ensuring attacks does not compromise the network. When miners confirm a block, they are rewarded tokens as a built-in incentive for network participation. However, as the global cryptocurrency market capitalization steadily increased, the miners became centralized

Cryptographic hashing algorithms are useful in network attack prevention because they possess several properties:

- **Input/Output length size** - The algorithm can pass in an input of any length in size, and outputs a fixed length hash value.
- **Efficiency** - The algorithm is relatively easy and fast to compute.
- **Preimage resistance** - For a given output z, it is impossible to find any input x such that h(x) = z. In other words, the hashing algorithm h(x) is a one-way function in which only the output can be found, given an input. The reverse is not possible.
- **Collision resistance** - It is computationally infeasible to find any pairs x1 ≠ x2 such that h(x1) = h(x2). In other words, the probability of finding two different inputs hashing to the same output is extremely low. This property also implies second preimage resistance.
- **Second preimage resistance** - Given x1, and thus h(x1), it is computationally infeasible to find any x2 such that h(x1) = h(x2). While this property is similar to collision resistance, the property differs in that it is saying an attacker with a given x1 will find it computationally infeasible to find any x2 hashing to the same output.
- **Deterministic** - maps each input to one and only one output.
- **Avalanche effect** - a small change in the input results in an entirely different output

These properties give the cryptocurrency network its intrinsic value by ensuring attacks does not compromise the network. When miners confirm a block, they are rewarded tokens as a built-in incentive for network participation. However, as the global cryptocurrency market capitalization steadily increased, the miners became centralized

and focused their computing resources on hoarding tokens as assets, rather than for network participation purposes. CPU miners gave way to GPUs, which in turn gave way to powerful ASICs. In one notable study, the total power consumption of Bitcoin mining has been estimated to be as high as 3 GW, comparable to Ireland's power consumption. This same study projected total power consumption to reach 8 GW in the near future.

To solve the energy waste issue, the Proof of Stake (PoS) consensus mechanism was proposed by many new networks. In PoS networks, token holders lock their token balances to become block validators. The validators take turns proposing and voting on the next block. However, the problem with standard PoS is that validator influence correlates directly to the amount of tokens locked up. This results in parties hoarding large amounts of the network's base currency wielding undue influence in the network ecosystem.

The TRON consensus mechanism uses an innovative Delegated Proof of Stake system in which 27 Super Representatives (SRs) produce blocks for the network. Every 6 hours, TRX account holders who freeze their accounts can vote for a selection of SR candidates, with the top 27 candidates deemed the SRs. Voters may choose SRs based on criteria such as projects sponsored by SRs to increase TRX adoption, and rewards distributed to voters. This allows for a more democratized anddecentralized ecosystem. SRs' accounts are normal accounts, but their accumulation of votes allows them to produce blocks. With the low throughput rates of Bitcoin and Ethereum due to their PoW consensus mechanism and scalability issues, TRON's DPoS system offers an innovative mechanism resulting in 2000 TPS compared to Bitcoin's 3 TPS and Ethereum's 15 TPS.

The TRON protocol network generates one block every three seconds, with each block awarding 32 TRX to Super Representatives. A total of 336,384,000 TRX will be awarded annually to the 27 SRs. Each time an SR finishes block production, rewards are sent to a sub-account in the super-ledger. SRs can check, but not directly make use of these TRX tokens. A withdrawal can be made by each SR once every 24 hours, transferring the rewards from the sub-account to the specified SR account.

The three types of nodes on the TRON network are Witness Node, Full Node, and Solidity Node. Witness nodes are set up by SRs and are mainly responsible for block production and proposal creation/voting. Full nodes provide APIs and broadcast transactions and blocks. Solidity nodes sync blocks from other Full Nodes and also provide indexable APIs.

4.7 Ledger Conflicts and Resolutions

As discussed previously, for some blockchain networks it is possible that multiple blocks will be published at approximately the same time. This can cause differing versions of a blockchain to exist at any given moment; these must be resolved quickly to have consistency in the blockchain network. In this section, we discuss how these situations are generally handled.

With any distributed network, some systems within the network will be behind on information or have alternative information. This depends on network latency between nodes and the proximity of groups of nodes. Permissionless blockchain networks are more prone to have conflicts due to their openness and number of competing publishing nodes. A major part of agreeing on the state of the blockchain network (coming to consensus) is resolving conflicting data.

For example:

- node_A creates block_n(A)with transactions #1, 2 and 3. node_A distributes it to some nodes.
- node_B creates block_n(B)with transactions #1, 2 and 4. node_B distributes it to some nodes.
- There is a conflict.
  - block_n will not be the same across the network.
    - block_n(A) contains transaction #3, but not transaction #4.
    - block_n(B) contains transaction #4, but not transaction #3.

Conflicts temporarily generate different versions of the blockchain, which is depicted in Figure 2. These differing versions are not "wrong"; rather, they were created with the information each node had available. The competing blocks will likely contain different transactions, so those with block_n(A) may see transfers of digital assets not present in block_n(B). If the blockchain network deals with cryptocurrency, then a situation may occur where some cryptocurrency may both be spent and unspent, depending on which version of the blockchain is being viewed.

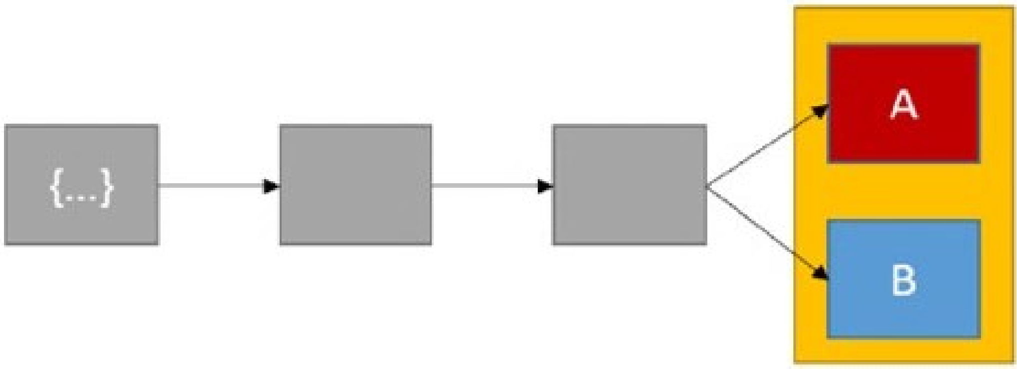


Figure 2 Ledger in Conflict

Conflicts are usually quickly resolved. Most blockchain networks will wait until the next block is published and use that chain as the "official" blockchain, thus adopting the "longer blockchain". As in Figure 3, the blockchain containing block_n(B) becomes the "official" chain, as it got the next valid block.

Any transaction that was present in block_n(A), the orphaned block, but not present in the block_n(B) chain, is returned to the pending transaction pool (which is where all transactions which have not been included within a block reside). Note that this set of pending transactions is maintained locally at each node as there is no central server in the architecture.

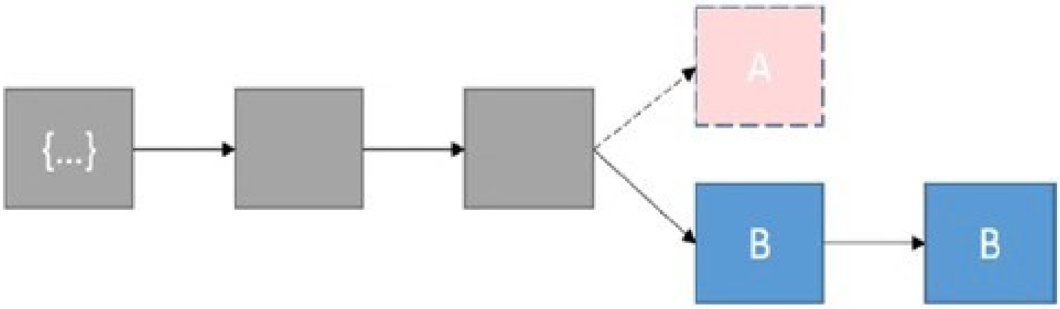


Figure 3: The chain with block_n(B) adds the next block, the chain with block_n(A) is now orphaned

Due to the possibility of blocks being overwritten, a transaction is not usually accepted as confirmed until several additional blocks have been created on top of the block containing the relevant transaction. The acceptance of a block is often probabilistic rather than deterministic since blocks can be superseded. The more blocks that have been built on top of a published block, the more likely it is that the initial block will not be overwritten.

Hypothetically, a node in a proof of work blockchain network with enormous amounts of computing power could start at the genesis block and create a longer chain than the currently existing chain, thereby wiping out the entire blockchain history. This does not happen in practice due to the prohibitively large amount of resources that this would require. Also, some blockchain implementations lock specific older blocks within the blockchain software by creating checkpoints to ensure that this can never happen.

3

THE EVOLUTION OF BLOCKCHAIN

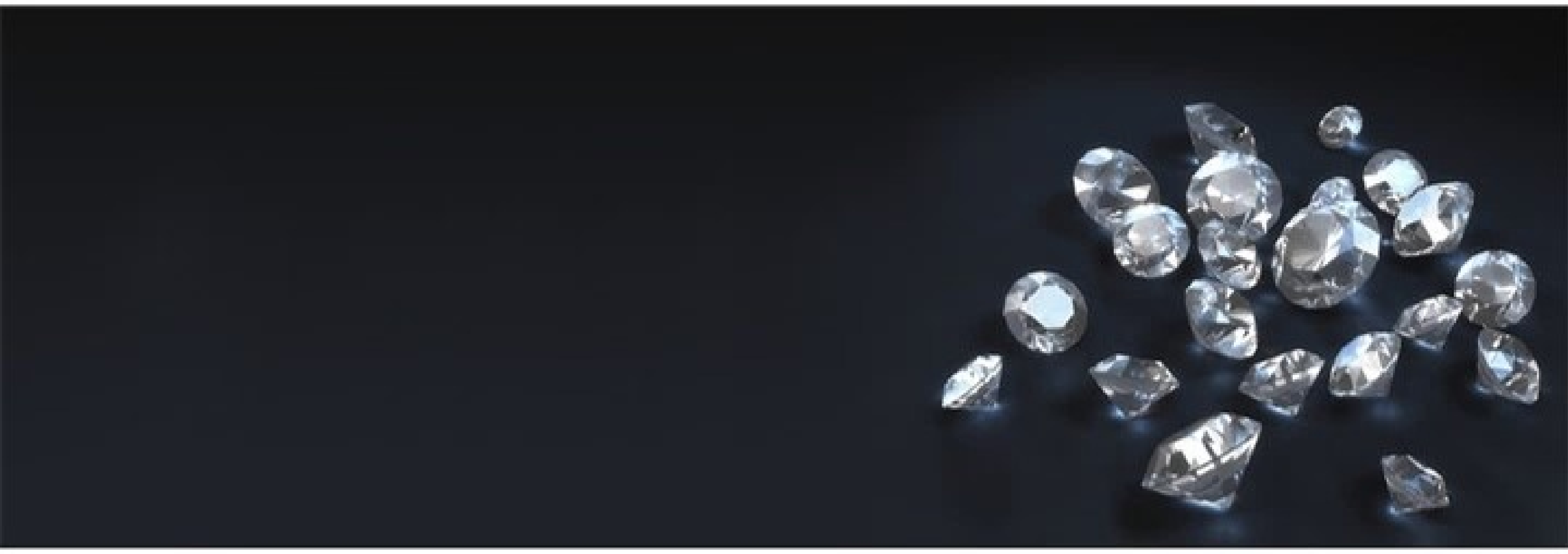
Started to be noticed by the world in 2009, through the emergence of a digital currency called Bitcoin, blockchain technology has become very popular today, and it marks the end of an era, and usher in a new era, the era of the Internet of Things, also known as the Industrial Revolution 4.0

With the applications that blockchain brings, many business opportunities have opened up, significant changes have occurred in the flow of finance, and many young millionaires have emerged.

Not stopping there, blockchain technology also opens a door of enormous potential, which experts have affirmed that what blockchain technology can do is likely to have a greater impact than what the internet has brought to the world economy.

Unlike fiat money, Bitcoin digital currency is limited, and it is not controlled by any authority or government. Besides, the transparency and security which Bitcoin offers to its users, that makes Bitcoin believer treat it as an potential "asset" that will grow in high value and Bitcoin is truly people-money.

But Bitcoin is merely a single product of many applications that Blockchain has to offer to the world. And every time the knowledge of blockchain is exploited to a deeper level, cash flow moves, and new millionaires appear.



THE DEVELOPING STAGES OF A TECHNOLOGY

The same as many other predecessor technologies, Blockchain will go through its evolution stages phases:

- **Primitive Stage:** When the idea is new, and difficult to accept.
- **Developing Stage:** When believers and adopters start to make some impact through proven results
- **Acceptance Stage:** When the technology is widely used, and many people talk about it in almost every conversation
- **Booming Stage:** When there is no more talk about it, people just cannot live without it

There are some debates about the 3rd and 4th stage, when there are many who believe the definition of a Booming Stage should be: When the technology is widely used, and the Acceptance Stage should be: when people just cannot live without it. They may be right. However, with a prospective of a business solution consultant and investors, we believe we are now in the Acceptance Stage and the Booming Stage is just around the corner.

At difference stage, one who realize and adapt it quickly, will control the game of market and will gasp the biggest piece of money. There are some indicators that we all been through but some of us have never noticed.

Primitive Stage:

Remember in 2009, when the idea of buying IPhone and Video Cards to build Bitcoin Mining Rigs sounded stupid and waste of time and money. Fast forward to this day, everyone realize that idea, at that period of time is genius.

Early Bitcoin believers who at time might be student, investors, mechanic, IT guys and some idiots now live a very okay life with couple of hundred Bitcoin in their wallet, humbly speaking.

Developing Stage:

When people start to understand more about blockchain, they are seeking a way to make Cryptocurrency more useable, more applicable and more accessible. Then the idea of POS and Smart Contract emerged. The number of companies and projects are pop up like mushroom.

There are some people who make a lot of money and there are also a lot of people who lose some money. The one who have knowledge about technology and hold as much as ERC20 based Tokens, keep them in the wallet, and stake out more of them, seem to be very happy today. The concept of dApps and Smart Contract seems to open up many million dollar ideas.

- **ERC20 Cryptography Algorithm**
  - An ERC20 token is a blockchain-based asset with similar functionality to bitcoin, ether, and bitcoin cash: it can hold value and be sent and received. The major difference between ERC20 tokens and other cryptocurrencies is that ERC20 tokens are created and hosted on the Ethereum blockchain, whereas bitcoin and bitcoin cash are the native currencies of their respective blockchains. ERC20 tokens are stored and sent using Ethereum addresses and transactions, and use gas to cover transaction fees.
  - ERC20 is an official protocol for proposing improvements to the Ethereum (ETH) network. ERC stands for Ethereum Request for Comment, and 20 is the proposal identifier. This is a common standard for creating tokens on the Ethereum blockchain. This token standard defines a set of rules that apply to all ERC20 tokens that allow them to interact seamlessly with one another. Wallets and exchanges use the standard to integrate various ERC20 tokens onto their platforms and facilitate exchanges between ERC20 tokens and other cryptocurrencies.

- **Smart Contract**
    - A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.
    - Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.
- **Decentralized Application**
    - Decentralized applications (dApps) are digital applications or programs that exist and run on a blockchain or P2P network of computers instead of a single computer, and are outside the purview and control of a single authority.

Acceptance Stage:

The key fundamental of this Stage is the number of the people who believe in the movement of their group is also the movement of cash flow. The one who have the network of people is the controller of the digital financial game. For the reason, they have the large group of promoters, consumers, networkers and affiliates. Once they speak, their group listens. The groups are seeking the leader's knowledge, tips, and guidance to make something or become someone in this Blockchain worlds. Companies are willing to collaborate with those leaders in order to shape the markets.

Last but not least, the Booming Stage

The start of the Booming Stage is when everyone is using the technology without talking about it anymore. They just cannot live without it. They play, shop, enjoy, connect and making money with it. We believe this stage is just around the corner, and we are on the way moving toward it.

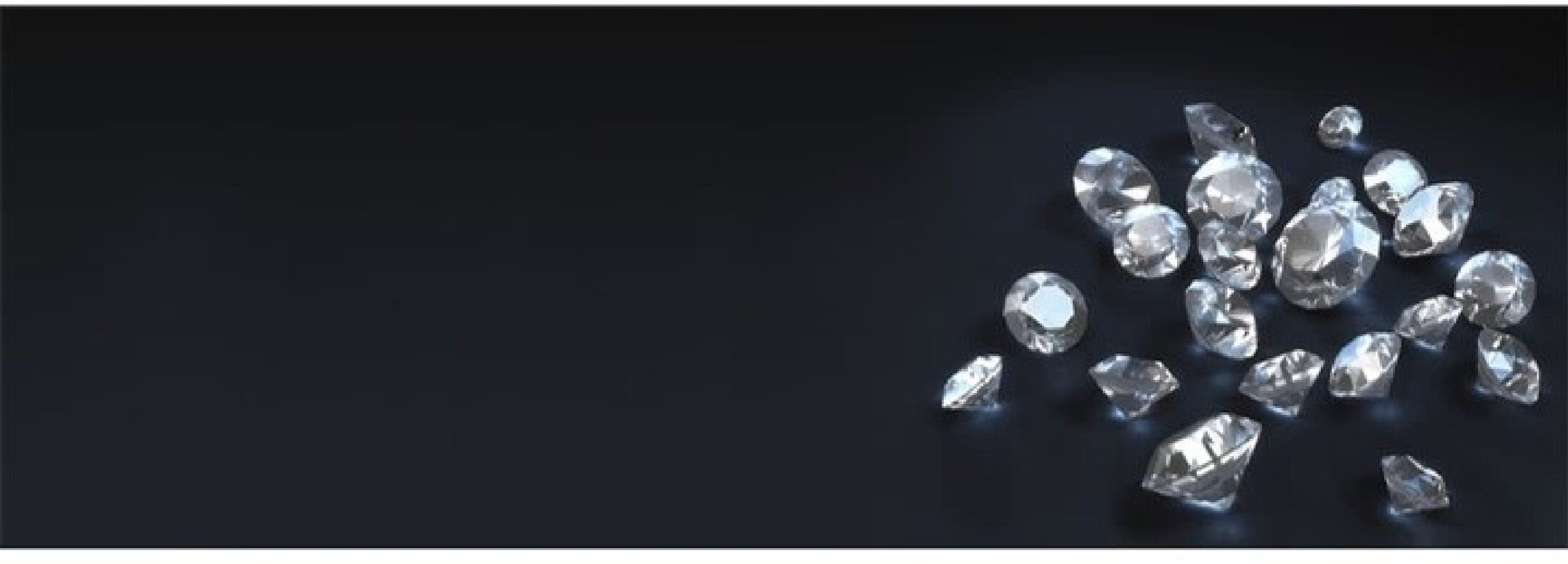
4

OUR VISION ON THE DIAMOND INDUSTRY

We incorporate the latest blockchain technology into the supply chain of the diamond industry. This opens up a new platform for conducting global trade in diamonds. In addition to reducing transaction-related costs, CERES GLOBAL eliminates the inherent inefficiency of paper transaction processing. A set of advanced functions are implemented to provide sophisticated and detailed diamond tracking and tracking. The goal is to decentralize the market for diamonds, which will open up lot of access for diamond buyers and sellers. The diamond trade does not require ancillary services such as transportation, finance and insurance. These services will be provided by separate service providers. The CERES GLOBAL project will only integrate them within the platform and not charge commissions or brokers for such third party services.

MARKET TRENDS AND POTENTIAL

There is no doubt that the implementation of CERES GLOBAL, will increase the market scope of the diamond industry. The increased visibility of the products and the adoption of a cryptocurrency will help diamond dealers at all levels to increase their market share. At the same time the transparency of the entire process and the authenticity of diamonds will instill confidence in both the first and the first diamond investor. The absence of middlemen and reduced transportation and other related costs, will allow for more competitive prices.



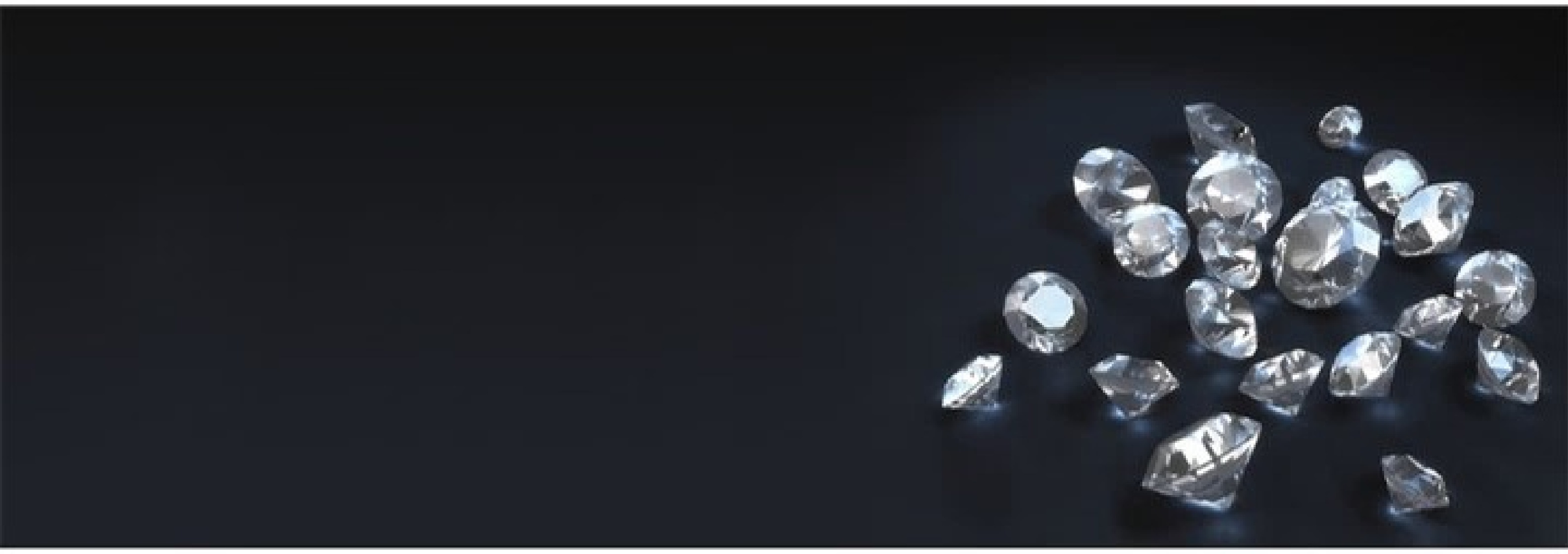
5

CERES DIAMOND DIGITAL STOCK

With the development of cryptocurrencies for the past few years, many have even come to believe 2021 as the year of the Bitcoin as this topic has been at the forefront of discussions worldwide are it on global media. Naturally, with the increased interest that this topic has been sparking many have decided to jump on the super speed train and learn how to trade and invest online. Therefore, at Ceres Global we have plant the seed of Digital Stock for the past 5 years and have been developing this idea in to reality.

Essentially, the Digital Stock along with our trading platform is software that brings traders and investors together in one place and allows them to buy and sell their currencies and other financial instruments. Our Digital Stock offer many benefits when compared to traditional brokers and financial dealers. For one, it’s quick and easy to use and secondly, they offer a number of educational opportunities to help investors learn more about dealing and trading a number of commodities, shares and currencies.

The added convenience of being able to access your online broker whenever you wish, be it day or night, is also another great feature allowing for more flexibility. Further advantages of online trading platforms include:



Essentially, the Digital Stock along with our trading platform is software that brings traders and investors together in one place and allows them to buy and sell their currencies and other financial instruments. Our Digital Stock offer many benefits when compared to traditional brokers and financial dealers. For one, it's quick and easy to use and secondly, they offer a number of educational opportunities to help investors learn more about dealing and trading a number of commodities, shares and currencies.

The added convenience of being able to access your online broker whenever you wish, be it day or night, is also another great feature allowing for more flexibility. Further advantages of online trading platforms include:

1. EASE OF DEALING

Gone are the days when trading involved calling a broker to arrange for purchases or sales. With online trading it's all done in just a few clicks and it's rare that traders need to speak directly with their broker.

2. AFFORDABILITY

Online trading is very affordable, as more and more brokers are offering online trading, the costs of dealing has decreased considerably, thus allowing traders to benefit from greater income when successful trades are made.

3. GREATER CONTROL

As previously mentioned, online trades can be conducted at any time day or night, allowing traders to choose when they choose to trade. Additionally, trading can take place via mobile device or laptop, allowing for even more flexibility and freedom and trading on the go.

4. REAL TIME TRADING

Online brokers offer real time prices and an advanced interface, so traders can keep an eye on their deals at any time and get the most up-to-the-minute prices.

5. FASTER TRANSACTIONS

Online trading is extremely fast. As soon as an account has been set up with an online broker, trading can take place immediately as long as sufficient capital is in the account. There are numerous online trading platforms out there, trading with IG offers all the above, plus the knowledge that you're trading with one of the most popular and trusted online brokers on the internet. Make sure to spend enough doing due diligence and familiarizing yourself with online trading in general including the different trading strategies that are available to help make the most of your trades and have a better overall knowledge of the industry.

STOCK OF CERES TRUST FUND (SOCTF) STATISTIC

Valuation Measures

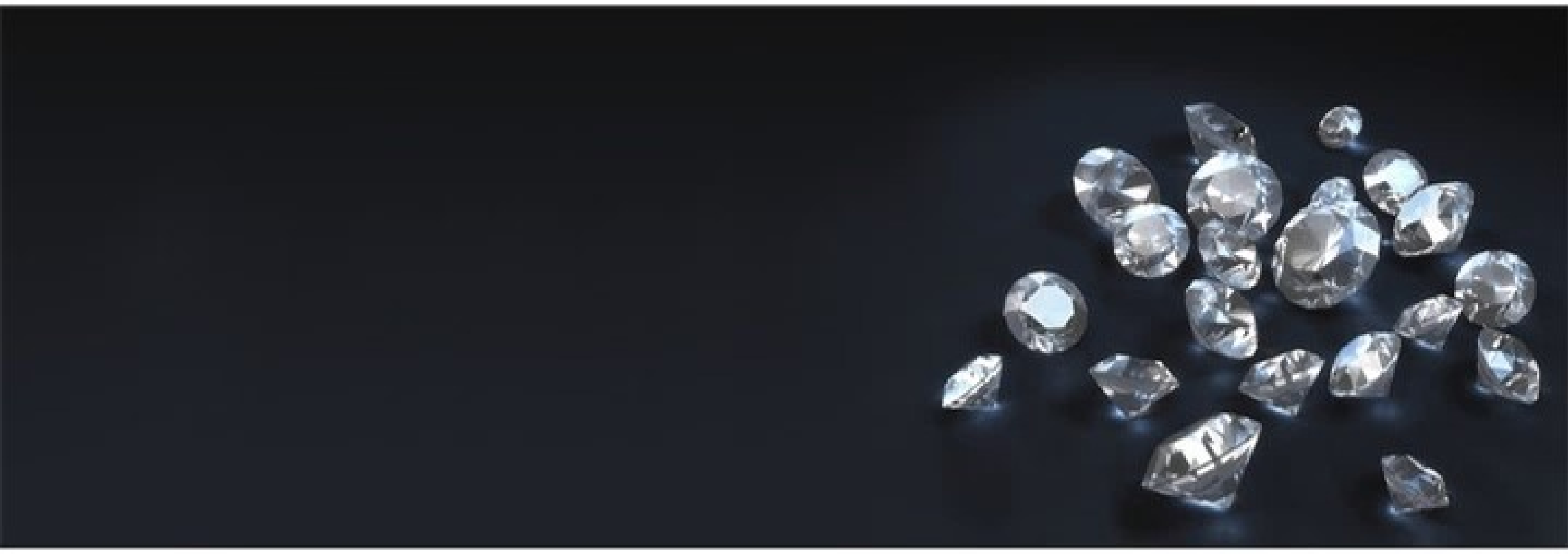
Total Supply of SOCFT	5,980,000,000
VIP Investor Value	3,097,640,000 (51.8%)
Regional Leader Value	621,920,000 (10.4%)
Public Value	2,260,440,000 (37.8%)
Market Cap.	$29,900,000,000
Initial Price/Sales	$5.00
Expected PEG Ratio	2.0

6

REFERENCES

I. Blockchain Technology Overview, document #8202 by National Institute of Standards and Technology Interagency.

1. Clarke, A.C., "Hazards of Prophecy: The Failure of Imagination," from Profiles of the Future: An Inquiry into the Limits of the Possible, 1962.
2. Lamport, Leslie. "The Part-Time Parliament." ACM Transactions on Computer Systems, vol. 16, no. 2, Jan. 1998, pp. 133-169., https://dl.acm.org/citation.cfm?doid=279227.279229.
3. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.
4. Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf
5. National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. https://doi.org/10.6028/NIST.FIPS.180-4
6. National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions
7. "Hash per Second." Bitcoin Wiki, http://en.bitcoin.it/wiki/Hash_per_second.
8. National Institute of Standards and Technology, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Federal Information Processing Standards (FIPS) Publication 202, August 2015. https://doi.org/10.6028/NIST.FIPS.202



9. National Institute of Standards and Technology (NIST), Digital Signature Standard, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013. https://doi.org/10.6028/NIST.FIPS.186-4
10. "LDAP.com." LDAP.com, https://www.ldap.com.
11. "How Is the Address of an Ethereum Contract Computed?" Ethereum Stack Exchange, 29 Jan. 2016, 22:14, https://ethereum.stackexchange.com/questions/760/how-is-the-address-of-an-ethereum-contract-computed.
12. Bahsoun, J.P., Guerraoui, R., and Shoker, A., "Making BFT Protocols Really Adaptive," 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, pp. 904-913, 2015. https://doi.org/10.1109/IPDPS.2015.21
13. Lamport, L. "Time, Clocks, and the Ordering of Events in a Distributed System." Communications of the ACM, vol. 21, no. 7, January 1978, pp. 558-565., doi:10.1145/359545.359563. https://amturing.acm.org/p558-lamport.pdf.
14. Todd, P. Bitcoin Improvement Protocol (BIP) 65, "OP_CHECKLOCKTIMEVERIFY," October 1, 2014. https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki
15. Wong, J. and Kar, I., "Everything you need to know about the Ethereum 'hard fork,'" Quartz Media, July 18, 2016. https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/
16. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D., Report on Post-Quantum Cryptography, National Institute of Standards and Technology Internal Report (NISTIR) 8105, April 2016. https://doi.org/10.6028/NIST.IR.8105

II. What is an ERC-20 Token Blockhchain.com

III. Ake Frankenfield, "What is Smart Contract?"

- https://www.investopedia.com/terms/s/smart-contracts.asp

IV. Paramita (Guha) Ghosh "The Future of Blockchain"

- https://www.investopedia.com/terms/s/smart-contracts.asp

V. Forbes Technology Council "What does the future of blockchain hold 10 Predictions From Tech Experts"

- https://www.forbes.com/sites/forbestechcouncil/2018/09/06/what-does-the-future-of-blockchain-hold-10-predictions-from-tech-experts/#22edd72c301a

VI. Matt Perez "Top Earning Video Gamers: The Ten Highest-Paid Players Pocketed More Than $120 Million In 2019" https://www.forbes.com/sites/mattperez/2020/01/29/top-earning-video-gamers-the-ten-highest-paid-players-pocketed-more-than-120-million-in-2019/#9b63b4880b4a

VII. Brendan Sinclair, "Global Games market hit $137.9 Bilion this year" https://www.gamesindustry.biz/articles/2018-04-30-global-games-market-to-hit-usd137-9-billion-this-year-newzoo

GLOSSARY

Address

A short, alphanumeric string derived from a user's public key using a hash function, with additional data to detect errors. Addresses are used to send and receive digital assets.

Assets

Anything that can be transferred.

Asymmetric-key cryptography

A cryptographic system where users have a private key that is kept secret and used to generate a public key (which is freely provided to others). Users can digitally sign data with their private key and the resulting signature can be verified by anyone using the corresponding public key. Also known as Public-key cryptography.

Block

A data structure containing a block header and block data.

Block data

The portion of a block that contains a set of validated transactions and ledger events.

Block header

The portion of a block that contains information about the block itself (block metadata), typically including a timestamp, a hash representation of the block data, the hash of the previous block's header, and a cryptographic nonce (if needed).

Block reward

A reward (typically cryptocurrency) awarded to publishing nodes for successfully adding a block to the blockchain.

Cryptocurrency

A digital asset/credit/unit within the system, which is cryptographically sent from one blockchain network user to another.

Double spend (attack)

An attack where a blockchain network user attempts to explicitly double spend a digital asset.

Double spend (problem)

Transacting with the same set of digital assets more than once. This is a problem which has plagued many digital money systems, and a problem that most blockchain networks are designed to prevent.

-SOCTF-

BLOCKCHAIN BASED

DIGITAL STOCK

Published by
CERES TRUST FUND