# TALAN TECHNOLOGY

Talan is a decentralized public blockchain and permissionless project and is fully open source. Talan is developing a powerful and genius contract platform which seeks to deliver more advanced features than any protocol developed previously. It is the first blockchain platform to evolve out of a scientific philosophy and a research-first driven approach.

# CONTENTS

01

*Part One*

# DEVELOPMENT RATIONALE

# The financial industry of FinTech:

It can be said that fintech has had three major successes. Its first success was mobile payments like Apple Pay, WeChat, Ali Pay and Google Pay. The next one was achieved by Chinese brands like Ant Xiaodai, Jingdong Baitiao and Huabai by providing P2P loaning services. The final success which has enabled an entire new section of ventures and has been the subject of a lot attention recently, is blockchain. Instant communication, credit scoring, dynamic data and fast updates are the driving force behind such successes. The reason for FinTech’ s obsession with blockchain technology is that it has made trusting other parties easier and it has the potential to revolutionize financial infrastructures as we know them. As its name suggests, blockchain is comprised of blocks of data which are connected to each other by a proverbial chain. In it, each block contains an encrypted hash which points to the previous block, a timestamp and transaction information. However, blockchain is still in its infancy. Challenges like scalability, security, privacy and delay in integration are still points of concern.

In order to lead blockchain into the future and to bring about a free and truly decentralized economy in a world where wealth is not distributed equally and rapid inflation has created an even deeper social gap between people, a team which has a correct understanding of the current financial situations is needed.

# Talan and Bitcoin's idea

The idea of Bitcoin was grate, and it was that by solving the problem of double spending, it would let people to transfer money without the need for financial intermediaries. While Bitcoin sought to eliminate intermediation of financial institutions, it now targets the potential of the blockchain industry far beyond. Any asset or data can be transferred on a peer-to-peer basis without the need for a "trusted" intermediary. Such processes are processed and managed by a series of scripts called **smart contracts**. Talan is a hybrid solution combining Bitcoin' s blockchain and Ethereum' s technology.

# Talan and Bitcoin’s idea

A smart contract between two parties can be considered as a computer code. This contract is executed on the blockchain network and its code, which cannot be changed, is saved and replicated. The transactions regrading a smart contract are processed by blockchain which means that they can be automatically executed without the need for a third party.

Smart contracts play the governing and legislative role in Talan blockchain. Its most important role is to manage blockchain parameters through smart contracts implemented in genesis block.

Talan’ s codebase is Bitcoin. But in Talan's platform a layer has been added which allows the Ethereum Virtual Machine to execute Bitcoin's smart contracts. This means that Talan contains the best of the Bitcoin and Ethereum features.

Bitcoin introduced a blockchain based on UTXO. In a UTXO based blockchain each transaction is a link between inputs and outputs.

**The decentralized Talan blockchain has been created for the following purposes:**

- Issues of trust
- Decentralizing the economy
- Improper planning in developing countries for using blockchains in businesses
- Entering the world of IOT
- Limited and fair distribution of original coins

# 1. Issues of trust:

Many analyzers believe that the financial crisis of 2008 where the biggest financial firm declared bankruptcy was caused because of short term liquidity which can be traced back to the mortgage bubble and credit scoring systems. Many bankers were arrested for reselling low value assets in the course of multiple years which shows that the firm’ s finical statements were not being maintained based on what was really happening. This shows that the current banking accounting practices are old and are in need of change.

The Talan blockchain aims to provide transparency and trust which in the current financial global economy are among the biggest assets.

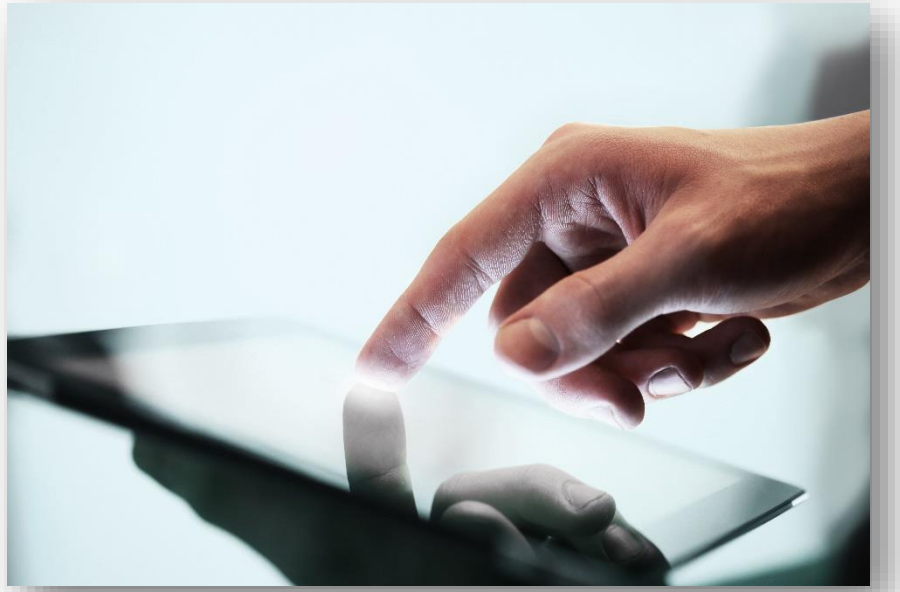
# 2. Decentralizing the economy:

Since the technology behind bitcoin is decentralized and is not controlled by any single institution, each party can keep a record of previous transactions. The Talan blockchain, as a decentralized platform, allows business owners to recreate traditional financial tools.

Before Talan, multiple blockchain technologies such as Ethereum were created for this purpose as well. However, being slow, having a high running cost, low transaction rates, not being in line with real world principles and wrong policies adopted by the founders for integrating this technology in quotidian lives of users has squandered the potential of these technologies becoming stable and reliable tools.

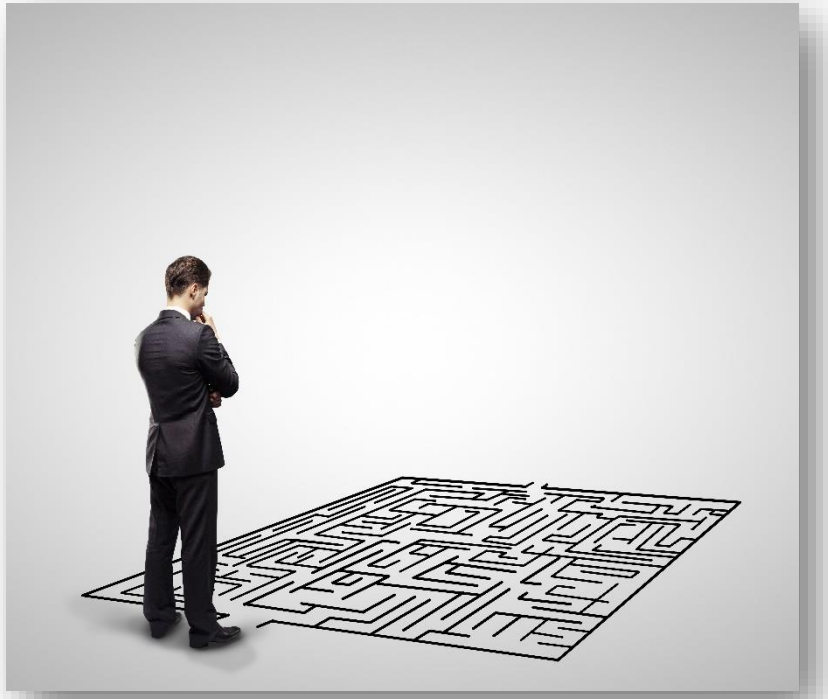
Talan aims to solve the aforementioned problems so that it can bridge the digital world and the real one in order to support the vision of decentralization and providing an infrastructure for businesses.

# 3 .Improper planning in developing countries for using blockchains in businesses:



It is evident that till now blockchain and the idea of decentralized economy has been mostly used in developed countries. Europe, United States, China, Japan, Malta, Switzerland and Estonia are among the countries which have enabled the usage and advancement of blockchain. The Talan institute will try its best to negotiate with developing countries in order to enable the use of blockchain in such countries.

# 4 – Entering the world of IOT



Since the Talan platform uses the UTXO blockchain model from bitcoin, it is light, entirely decentralized and uses a real proof of stake system. Additionally, it has high speed, short transaction time and it uses smart contracts. All these features make Talan’ s platform ideal for IoT devices.

# 5. Limited and fair distribution of original coins:

One of the main problems of many current blockchains is the distribution of a large number of original coins. This means that these blockchains pre-mine millions and even billions of coins and then distribute them in the market to gather a large amount of capital. This act, defeats the purpose of decentralization because even though that these systems use the latest decentralization techniques, in truth the majority of the coins are owned by a few which itself creates a centralized system. Since Talan stands by blockchain’ s main objectives which are limited distribution and expansion by its community, only a limited number of coins with real proof of stake have been created.

02 *Part Two*

# Technical Characteristics

# Technical Characteristics

The Talan system is based on Bitcoin and its most integral part is transactions. These transactions are data structures which encrypt the transfer of value between Talan’ s participants. The life cycle of a deal begins with a transaction known as the "origin” . Then, the deal is authenticated with either one or multiple signatures which indicate the deal’ s valid transfer of funds. After that, the transaction is broadcast across the Bitcoin network, where each node (participant) confirms the transaction and broadcasts it further until it has reached almost all the nodes in the network. Finally, the transaction is confirmed by an extraction node and is registered in a blockchain transaction block.

After registration in the blockchain and some further confirmations, a transaction is considered valid by the entirety of Talan and the funds assigned to the new owner can be spent in another transaction to further the ownership chain and begin the transaction’ s lifecycle anew.

# Output of a transaction

- A transaction can be considered as an address (which can be locked) and a value. Keeping with our analogy, the key for opening this lock, is the signature associated with it and after doing so, the value can be accessed. New transactions spend the output of previous transactions and their output can be used in future transactions. Each UTXO can only be used once.

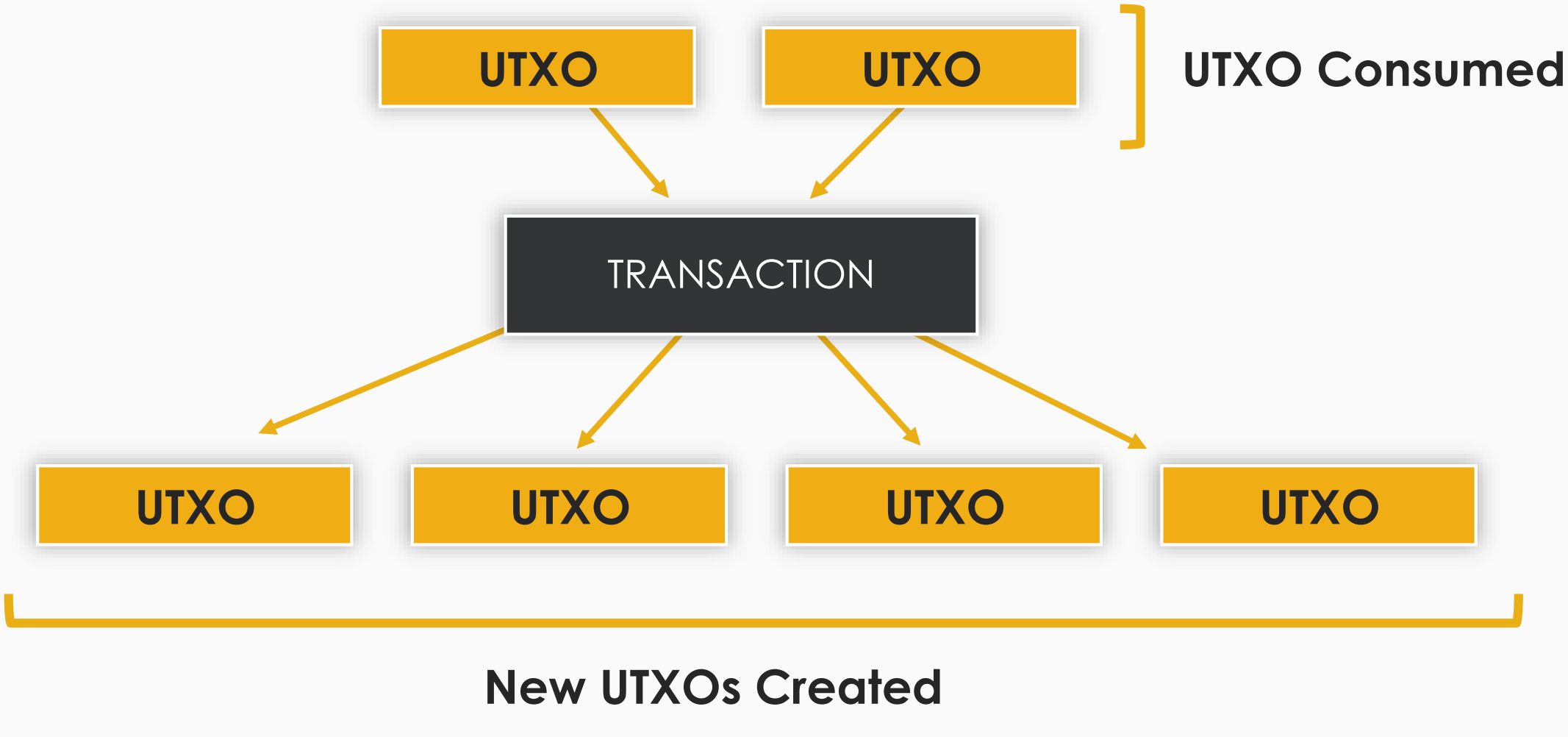
# Input of a transaction

- The input of a transaction is the output of a previous transaction. This input, is a pointer which points to the output of a previous transaction and an encrypted signature which acts as a key to unlock the aforementioned lock. When a signature "unlocks" a transaction's output, blockchain will consider that output as "spent" which can be used as inputs for other transactions. The new outputs which have not been unlocked yet are called UTXOs.

# Input of a transaction

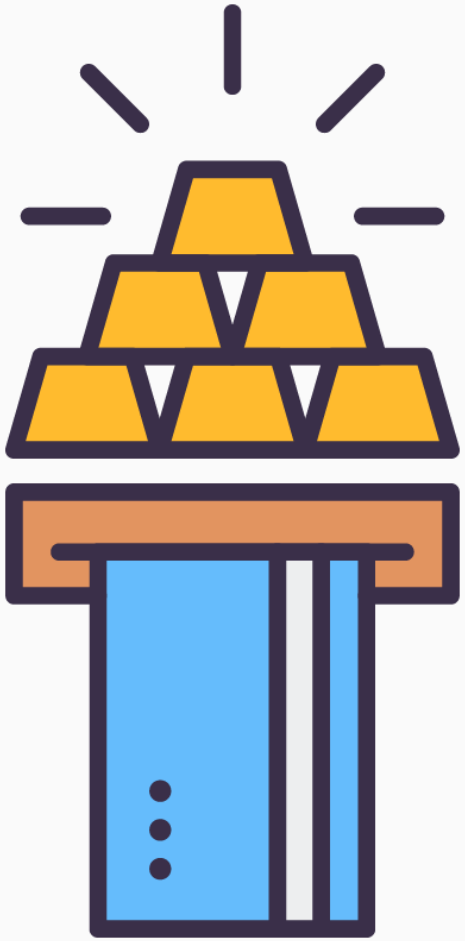
- With UTXOs it's more straightforward to validate transactions, and you can process multiple transactions at the same time regardless of sequence. This makes UTXOs more secure and scalable.
- In a UTXO accounting model, transactions use the unused output of the previous transactions to create new outputs for future transactions.

# New UTXOs Creation process



# New UTXOs Creation process (cont.)

Each user's wallet manages their UTXOs and their related transactions. Each blockchain node, keeps a record of all the UTXOs of all time. This body is called UTXO. From a technical point of view, this is a chain which is stored in each node’ s data list. Whenever a new block is added to the chain, the entire block is updated to reflect this change. The new block contains a list of the latest transactions (including, a history of spent UTXOs and new transactions created since the latest chain status update). Each node maintains an exact copy of the chain status.



# Creating transactions

From certain points of view, a transaction is like a cheque. Each transaction is a tool which describes an action for transferring funds and until it is not used, it is not visible to the financial system. Like a cheque, the one doing the transaction does not have to necessarily be the one who signs it.

Transactions can be created online or offline by anybody even if that person is not the one who is authorized to sign the transaction. For example, an employee can create transactions and have them digitally signed by the firm' s CEO for authorization. Unlike a cheque which uses a specific account to use the funds from, a Talan transaction uses a previous transaction as its origin.

After a transaction' s creation, and after obtaining the authorization and digital signature of the funds' owner (or owners), the transaction is regarded as valid and will contain all the information needed for transferring the funds. Finally, a valid transaction needs to be propagated through the bitcoin network until it reaches a miner so that it can be registered in the public ledger.

# Account abstract layer

The account abstract layer describes methods for hiding the internal mechanics of code through abstraction. AAL is a technique used in Talan to abstract account level information. it’ s a serious technical challenge to deploy the EVM on the Bitcoin blockchain. This challenge is solved with an Account Abstraction Layer that converts the blockchain’ s outputs into account balances and facilitates the transfer of information between the EVM and the UTXO-based blockchain. From a more technical point of view, Talan’ s AAL is added to the bitcoin’ s transaction code to enable Ethereum-like smart contracts on top of bitcoins UTXO model. This method was used by the Quantum blockchain.

# Account abstract layer

Currently, this feature exists in the Talan blockchain and all smart contracts are executed using this method. AAL in Talan allows the account model used in **Ethereum** to be abstracted or being transferred to work on top of the UTXO model. Talan’ s AAL is like a pivotal computing that allows UTXO to interact with account models. As the name states, abstracts the concept of Accounts away from the implementation, allowing virtual machines like the EVM to run atop the UTXO model that powers Talan. In the UTXO model, we often have lots of public and private key pairs as change is generated and transactions move coins around. A wallet maintains a list of public keys which hold your coins and your 10 Bitcoins or Talan might be split among 10 different UTXOs. In an Accounts model, all of that is simplified to an Account Address Balance in the database, so that contracts can just check the end balance to send/receive funds from.

# We can summarize the technical characteristic of Talan blockchain as follow

- Transaction model: UTXO (Unspent Transaction Output) from Bitcoin
- Smart contract architecture: EVM (Ethereum Virtual Machine)
- Block size: 4 million bytes, scalable using on-chain DGP (Decentralized Governance Protocol) up to 32 million bytes
- Average block spacing: 32 seconds
- Smart contract token protocol: TLRC20, based on Ethereum ERC20; TLRC721 non-fungible tokens, based on Ethereum ERC721
- Consensus algorithm: Proof of Stake, version 3.0, upgraded from Blackcoin
- Theoretical maximum TPS (Transactions Per Second): 400 to 500
- Block reward: 4 TALAN per block and it is decreasing by 32% every year, plus a share of transaction fees and gas
- Dev fund: 700,000 TALAN
- Maximum supply: 14 million in 23 years

# Proof of stake model

Proof of Stake's security has proven itself over years of testing. Advances in this technology in Blackcoin's Proof-of-Stake 3.0 have solved the issues faced with Coin-Age, Block Reward and Blockchain Precomputation. The protocol is robust and keeps nodes connected to the network. It disincentives inactive nodes. In this paper we will highlight and outline the advantages and perform a security analysis of the system.

# Security, Coinage and Attacks

The whole purpose of holding competitions for coins is to avoid attacks. Confirmation of transactions is an honor given to the winner of a block. However, if this system can be gamed, then it is flawed. In Proof of Stake, you first prove you have access to coins and from that point you can compete to win blocks randomly. The more people competing the more secure the block. Coin age is the idea that the longer you hold coins the higher the probability you can win a block. It's original intention was to incentive dormant holders of coins. However, this does not encourage a node to stay connected to the network in practice since they can wait for the reward to increase. Also, shareholders can disconnect from the network for long periods of time, then reconnect and win enough blocks to risk a 50% attack on the network. The time calculation will effect payouts discouraging connectivity. Also, the fewer the nodes that are connected, the easier it is to gain a majority of the blocks forging consensus. Also, stakes can be computed in advance to make the attack more effective. Timestamps are used in Proof of Stake to get a general idea of time. Drift calculations are used to prevent forging erroneous timestamps. In Proof of Work, a difficulty increase or decrease is made depending on how quickly a block was produced. However, as a precautionary method to prevent any sort of "Timing Attacks" Proof of Stake coins use centralized checkpoints.

# The Ethereum Virtual Machine(EVM)

Talan basically runs an EVM (Ethereum Virtual Machine) which makes smart contracts possible on top of Bitcoin’ s blockchain. If you’ ve tried developing a smart contract on the Ethereum blockchain, or have been in the space for a while, you might have come across the term “**EVM**”, short for **E**thereum **V**irtual **M**achine. Virtual machines are essentially creating a level of abstraction between the executing code and the executing machine. This layer is needed to improve the portability of software, as well as to make sure applications are separated from each other, and separated from their host.

# The Ethereum Virtual Machine(2)

The EVM’ s physical instantiation can’ t be described in the same way that one might point to a cloud or an ocean wave, but it does exist as one single entity maintained by thousands of connected computers running an Ethereum client.

The Ethereum protocol itself exists solely for the purpose of keeping the continuous, uninterrupted, and immutable operation of this special state machine; It's the environment in which all Ethereum accounts and smart contracts live. At any given block in the chain, Ethereum has one and only one 'canonical' state, and the EVM is what defines the rules for computing a new valid state from block to block.It allows smart contract code to run by compiling to EVM bytecode. EVM plays a core role in blockchain to ensure a trustless mechanism without having any central administrator. EVM keeps each node systemically isolated from others in order to avoid security risks. Even if one node is compromised, it does not influence any other nodes and blockchain network.

# The Ethereum Virtual Machine(3)

EVM enables smart contract(solidity) to be executed on any computer(OS agnostic). EVM is installed on the computer(operating system) and works as a middle layer between a smart contract and operating system. Once Solidity code is compiled to bytecode, EVM can read to execute.

If we do not have EVM, we need to develop respective compilers for each operating system. EVM makes Ethereum ecosystem compatible and efficient. In computer science, “bytecode” is a computer language which is compiled from source code and run on Virtual Machine. Bytecode is not human-readable but computer-readable.EVM byte code is compiled from Solidity and executed on EVM.

# The Ethereum Virtual Machine(4)

AAL adds a couple of new opcodes to the Bitcoin opcodes to add support for smart contracts.

**OP_CREATE:** Used to create new smart contracts

**OP_CALL:** Used to execute code inside an existing smart contract

**OP_SPEND:** Used to spend the value in a smart contract

During the block creation process, the validator’ s software will parse the script in the Talan transactions, and when it comes across transactions using these opcodes, it’ ll set them aside to be processed through the EVM. The EVM contract transactions are then processed into a special “Expected Contract Transaction List” which is executed by validator nodes. These transactions are then run against the EVM, with the resulting output being converted into a spendable Talan tx. If during the execution of a contract, the contract calls another contract with a value, that transaction is also turned into an explicit Talan tx and attached to the current block.

# Blockchain Precomputation

The block timestamp is key to the Proof of Stake system. It is possible in theory to fork a coin by changing previous timestamps. The stake modifier does not obfuscate the hash of sufficiently to prevent knowing future proofs. So an attacker can attempt to compute all of the blocks in advance and run a higher probability to forge multiple consecutive blocks. Solution from Proof of Stake 2.0: The stake modifier is changed at every modifier interval to better obfuscate any calculations that would be made to pinpoint the time for the next proof-of-stake.

# Block Reward

The Block Reward in most Proof of Stake systems is unfortunately based on Coin Age. In theory, this is to distribute interest fairly by allowing nodes to receive latent payments due. It is an attempt to keep a common APR. However, this system does not work because nodes can stay disconnected and with many split inputs, reconnect to the network and game the reward system. Also, it does not give nodes any incentive to stay connected. In a decentralized system, the more nodes connected the better the security since it shifts trust from a single entity to the network itself. Solution from Proof of Stake 3.0

# Security Analysis

The elimination of Block Reward based on time was an obvious improvement. Thus, if the amount of nodes staking drops, yearly interest would increase proportional to the disconnected nodes. For example, if only 1/5th the network was Staking, you can expect up to 5 times the reward! Since many coins do not have enough nodes, this is a great advantage even to smaller shareholders. Although statistical data on all relevant coins would be time consuming to obtain, it is self-evident that there is usually a lot less than 20% of the shareholders staking. We think this increase in incentive will certainly keep the nodes more competitive. The change in granularity was useful to prevent "Stake Grinding". A good analysis of the probability of this attack was done in Neucoin. Their claim is that even with all the hashing power of the Bitcoin network, the attack would not be possible. However, a rollback of a few minutes could cause new users to the network unsure of which chain to join.

# Security Analysis

Therefore, Proof of Stake systems use "Checkpointing" which is basically centralized control of the main developer to choose chains that attempt to do this. Of course, this is not an ideal solution. There was a good proposal made in Ethereum for this. They proposed that a new node to the network asks other nodes "off-band" if they are indeed on the correct chain. Using our decentralized markets, it is possible we can get nodes to share this information periodically. The solution will require further investigation. The additional removal of Coin age in general is a secure decision. It is possible to perform a hybrid system of checking popular time servers as well to help calculate drift and require nodes to keep closely synchronized with a general consensus of time. Addition of other random factors based on the blockchain itself may also be a consideration.

# Offline staking

Offline staking allows users to keep their cryptocurrencies in an offline wallet and gain interest on them. The offline wallet is also referred to as hardware or cold wallet to indicate that it is not connected to the internet.

Receiving rewards gives users the opportunity to earn profits from staking their coins. They do not necessarily have to use a valid node under proof of stake model.

Talan’ s offline staking does not need an internet connection. That’ s why it is called offline staking. In it, instead of tokens, the owners delegate their wallet’ s addresses. The coins themselves remain in the owner’ s wallet and can be used at any given time. Like all blockchain networks, the stakers are divided into two groups: the superstakers and the UTXO representatives which are called Delegators. To participate in offline staking, the representative’ s wallet address is sent to a super staker.

# Offline staking

The super stakers then can act on behalf of the delegators and take a cut from the profits for doing the staking. However, after delegation of the wallet, the owner doesn’ t have to be online at all times which means that the owners will receive interests even if they are not participating directly. The time windows for receiving the rewards is directly related to amount of delegated talans. The more coins that you have for staking, the sooner you will receive the block’ s rewards.

# How does offline staking work?

There are several ways to participate offline. Like any POS blockchains, the user can decide to participate in the network as a Superstaker (as a validator) or delegate to a validator.

In case that a user does not want to participate as superstaker, they can delegate their coins to a user that is a superstaker. This method allows such users to put their coins in a large pool and do staking by paying a part of their gained rewards.

This can be configured through the staking network interface using their offline wallet address. The user can choose any of the options, can get their staking rewards and deposit them to their wallet address. This means that they can continue to enjoy the benefits of offline staking at all times without risking their online funds.

# 03 *Part Three* Economic Model

# Economic Model

At first Talan will release 700,000 coins in block number 1.

Out of these 700000, 25 percent of it will go to the developers and the needed software infrastructure. Talan’ s main goal is to create a fair, unbiased, equal and innovative financial ecosystem to help integrate blockchain technology with the real world especially in developing countries in which the users will not partake in raising the price falsely with approaches such as fakecoins. Unlike other blockchains which create millions and even billions of coins at launch, we have decided to start with a relatively small number of coins to allow the community to grow fairly and without any discrimination. Also, unlike the fiat money created by central banks of countries, Talan’ s coins are limited and will cap at 14 million in 23 years. Such a limit means that Talan’ s value will always be on the rise and will result in lowering the cost of staking year by year. In the first year, each 20 or 30 seconds, 1 Talan will be created and each year going forward, this number will be reduced by 32 percent until it reached the final amount of 14 million TALANs in 23 years.

# Economic Model

We have initiated negotiations with industries, enterprises, and companies to introduce and integrate Talan in the economy. To incentivize various industries, we have distributed 500,000 Talan' s among them. This enables these industries to have a more meaningful entrance to the Talan world. Talan will be used in numerous applications such as various bill payments, tourism, purchasing plane tickets, cryptocurrency exchange where one can buy and sell Bitcoins, Ethereum and other cryptocurrencies, sending money, NFT' s and many more. Investing in stocks and websites which sell their products in TALAN will be ready and offered in time.

The leadership of Talan institution will closely follow up these applications. As stipulated in the contract between Talan and these institutions, 2/3 of the staked coins will be transferred to an address to be sold to the users and proceedings will be invested in the related projects.

Last but not the least Talan institution will be able to use %20 of the available Talans at the address to developed the Blockchain even further and must present a list of expenditure after every project. The institution will provide a report of the expenditures to the Talan community. The collected coins will be spent on incentives and staking on tokens which follow Talan' s standards and are acceptable by the

# 04 *Part Four* Talan Off-chain Management

# Talan Off-chain Management

The Talan institution was founded in 2016 under the name Talan technology LLC in Georgia, a crypto friendly country.

The ecosystem and business model were designed in 2019 and became operational by **Isaac Yaqub** in second half of 2020. Currently more than eight experts are assigned to develop the Talan blockchain based on the roadmap.

# This roadmap for 2021 is:

- **Expediting block production as well as reducing the production time to under 20 seconds.**
- **Providing support for usernames so that users do not need to use long addresses for transactions.**
- **Creating confidential assets.**
- **Updating and maintaining the Bitcoin kernel of Talan to the latest version.**

# We summarize again the technical characteristic of Talan blockchain as follow

- Transaction model: UTXO (Unspent Transaction Output) from Bitcoin
- Smart contract architecture: EVM (Ethereum Virtual Machine)
- Block size: 4 million bytes, scalable using on-chain DGP (Decentralized Governance Protocol) up to 32 million bytes
- Average block spacing: 32 seconds
- Smart contract token protocol: TLRC20, based on Ethereum ERC20; TLRC721 non-fungible tokens, based on Ethereum ERC721
- Consensus algorithm: Proof of Stake, version 3.0, upgraded from Blackcoin
- Theoretical maximum TPS (Transactions Per Second): 400 to 500
- Block reward: 4 TALAN per block and it is decreasing by 32% every year, plus a share of transaction fees and gas
- Dev fund: 700,000 TALAN
- Maximum supply: 14 million in 23 years

# T A L A N
TECHNOLOGY