**Evoca and Ethem**

**Asynchronous offstate Recursive Governance model for a global state shared Ledger in achieving a cyclic Block Production through Gift Economy.**

1. **Abstract**
2. **Previous Work**
3. **Introduction**
4. **Account System in Evoca**
5. **Cuisine Cylinder Function**
6. **Trust Scores**
7. **Overview of global level scalable consensus**
8. **Quorums**
   1. **Eligibility**
   2. **Formation of Quorum**
   3. **Rules**
   4. **Parts**
   5. **Slot Dynamics**
   6. **Economics**
      1. **Quorum Payouts**
      2. **Quorum Dynamics**
   7. **Cold Staking**
9. **Role of Ghost Nodes**
   1. **Liquid Democrat**
   2. **Local Governance**
      1. **Monitoring**
      2. **Trail Call System**
10. **Mimeo Twins Consensus Protocol**
    1. **Core Objective**
    2. **Inner Consensus or zero phase**
    3. **Phases**
11. **Governance**
12. **Ethem Shell**
13. **String Swap & Hot Staking**
14. **Cold vs Hot Staking**
15. **Conclusion**
16. **References**
17. **Evocapedia** 
    1. **Paradox of Thrift**
    2. **Paradox of Value**
    3. **Paradox of Choice**
    4. **Account**

**Abstract**

Evoca an DLT enabled platform which mainly focuses on solving the core issues of fair stake distribution through variant capped account system and the performance of the public ledger through an alternative block production and incentive at the lowest level of the network peers through gift economy so, that there would be a constant higher motivation among the peers across the network to behave honestly for a better economy so, that it can reach unto billions of user’s across the globe for their daily commerce.

**Keywords**

1. **Previous Work**

Bitcoin from an abstract Satoshi’s whitepaper to a small group of computer enthusiasts experiments to a widely accepted currency and a most prominent and important innovation since the Digital Age**.** Most recently the variants in Bitcoin so called as Altcoins are created everyday with their own approach in a specific Domain. To ranging concepts from Privacy to Stable to Prediction Tokens adding up an entire foundational disciplines in to the formation of an industry of concepts such as **DEX’s ,Mining Pools** etc in a stiff competition in replacing the existing centralized Legacy System’s into a new form of Decentralized Governance mechanism.

Most of Altcoins bring about their own solution in addressing a centralized problem into a completely decentralized form through their own core governance model which gets directly corresponds to their community chosen consensus model ,which might be flawed in some case such as **POW**in terms of performance to scale to millions of people where as in **BITCOIN** the global commitment and the governance is achieved through a environment which has highly competitive miners performing the memory intense computation solvable and easily verifiable Hash Puzzle which in turn is highly cost and resource consuming. Due to this reason Industry as a whole in a ***crypto sphere*** needed an alternative scalable solution which in turn guaranties the same level of security as that of ***Nakamoto’s Consensus***, which in turn lead to the innovative introduction of POS Block chains to achieve the general global standard consensus through a process of transforming stakeholders to validators using a secure coin age function. But most often these POS Blockchains are faced with a fundamental core problem of wealth distribution at a very initial stage of economic construction.

Unfortunately the entire POS Ledger setting depends on the coin age function which in turn acts as a scarce resources and can only be achieved through holding and Locking up these tokens, this in turn clearly depicts that these POS networks are more effectively designed to encourage only Hoarding a large portion of wealth for an wealthy individuals which rises up into a **Paradox of Thrift**, than to spend it on a long run. And for those who are not investors and Speculators it can simply be a deep pocketing scheme which in turn leads up to a larger stake on the network transforming its nature into more of a speculative source of value than a real form of currency which rises an entire corrupted mafia's in the interior part of the network called as **Crypto Whales**. Who in turn can single handedly control and manipulate the price of an asset and potentially increase the security risks of the network.

Well, other alternative consensus models such as **pBFT, vBFT, dBFT, FBA** are good enough to achieve global level throughputs. But subjecting them to a highly centralized network design which in turns leads them to suffer from the failure of technical viewpoint of design rather than a economical viewpoint because they are just the variants of same inherent function **BFT** of stake hoarding and to a widely criticized topic of limited honesty subscribers to validate or even a closed membership to a widely distributed peers in across a open public network in a permission less ledger. Causing it **Highly Centralized** Both in terms of Economy and Network stability, leading up to controlling the entire economy, market manipulation and network security.

1. **Introduction**

### EVOCA vs. ETHEM

*“Evoca & Ethem are the two native tokens of a Evoca Blockchain Platform, serving different purposes with* ***Evoca*** *in short Xpc being a primary asset token following inflationary model in which the total target supply cap of circulating tokens would reach in a long run with an upward motion of a steady flow of circulating supply and* ***Ethem*** *in short Ehm a network resource token showing up a Deflationary economic model which would ultimately decline as the time progress in its monetary circulating phase.”*

* EVOCA tokens represent the ownership of the EVOCA Blockchain. They are used to create blocks and manage the network, and when you hold EVOCA in your wallet you’ll be rewarded with ETHEM tokens.
* ETHEM tokens give you the right to use the EVOCA Blockchain. Much like Ether to the Ethereum network, ETHEM is the fuel that powers transactions in the EVOCA system*.*

Evoca aims to build an asynchronous payment network which could initially have zero confirmations from the originator of the block orbit and later get revalidated from the other ordinate, with a notion of cashback system because a simple transaction on a network to a recipient it only involves a simple 1 event of transfer which is synchronous in a real time, but in order to build a industries level standard of asynchronous communication i.e., payments in terms of public ledger well asynchronous payments are only possible through cashback System because in case of cashback there is an notion of 2 independent events in which the 2nd transaction happens only based on the confirmation of 1st transaction validation.

**Account System in Evoca**

**An account in Evoca platform would simply be a function of these two different addresses i.e., XPC and EHM in which a state of any active account would simply respond to their personal wealth both in terms of XPC and EHM holdings in their respective address as**

**accounting in Evoca would function with a simple notion of an address which gets created on the network would simply represents personal wealth holding by a network peer.**

**Any active account created on the Evoca platform would simply responds to their personal wealth in terms of their address holdings**

**To begin any account created in the Evoca platform i.e., irrespective of XPC or EHM would simply behaves as of their hard coded monetary policy.**

Accounts created in Evoca are just same as off any bank to hold ones wealth, in its technical design philosophy created using public key cryptography, maintaining a fixed minimum Base Balance provides a greater resistance to Sybil attack. In which a user tries to generate a massive bulk address in order to spam the network.

Blockchains provide a greater anonymity for its participation in context to their asset's transition pattern. An account in Evoca platform is an address which is coupled with user’s asset holdings. Well in order to have a fair distribution of tokens at a very initial stage and also later during the economic progression at different stages of positive fixed inflation

Address in Evoca ledger to have inflation model of storage capacity of maximum limit holding wealth per single address, Well the limit can be increased through a regular gain of trust score by regularly involving in the process of trust score or spending of tokens. [4] Maximum trust score which a user can gain simply be a variant based on M1, M2, M3....Mn etc .In case of Evoca the native token.

In case of Ethem address the max cap holding per single address wealth would be deflationary, as Ethem corresponds to resource on network.

By this variant the Maximum capital addressing account system, along with the fairly awarded trust score One can never achieve a over flow of well concentrated wealth in a short time period. As every account gets created on network simple bounds to the core quasi protocol enabling global fair distribution of wealth.

**Skull Address:**

Skull address are the special type of address which are generated in Evoca Blockchain which is actually wealth variable capped so that one individual potential investor cannot hold up number tokens. Well that variable cap is actually analyzed with the help of a special metering parameter called as cylinders.

Address 🡪 1XcbVnJ49aKrEsAF987

Notice: Account Holdings 🡪 Evoca + Ethem holdings

……………………………………………………………………………………………………………………………………………………………………………

The cylinder function for any individual account is based on the various parameters. [Wealth Variable]

{Birth 🡪20000} + {Inflation 🡪72 hrs} [“Cylinder Expander”] + {Trust Scores🡪 variable}

Trust Scores🡪 Velocity of the stake

Eigen++ 🡪 Trust Pattern

Envy Cutting Cake Problem 🡪Ethem Ownership

1. **Trust Score**

Trust Scores for an account is accounted from a various standard ranking parameters such as,

“In terms of prioritized percentages between various parameters” :

Coin age function in POSV 🡪[Duration of Asset Staking, 50%]

Eigen++ in NEM 🡪 behavioural patterns of the account, 25%]

Cuisine Cylinder Function 🡪“CuCy Expander can only effect 10% of Cyfu “

Notice: Total Tokens🡪 “toTo function”

…………………………………………………………………………

Cuisine Cylinder Function & CuCy Expander

The Quorums stake all their newly created tokens in a special contract called as “CuCy Expander “for a period of 72 hrs. In order to avoid a sudden effect on an individual CuCy function due to the inflation of new tokens which are born out of a fresh consensus.

“CuCy Expander “helps in avoiding Self Looping Transaction for 72 hrs.

Cuisine Cylinder Function:

Cuisine Cylinder Function is a hypothetical measuring the meter which is pegged to an account which primary functions is to define the quality of a transaction and also to set a wealth variable a max capped address to hold up the wealth.

**Concepts like \***

**Refill-->** the total filling of Ethem in cylinder leads to the triggering action of the leak function

**Unlock-->** the process of updating a cylinder, in order to increases its maximum holding capacity.

**Leak -->** If an address accumulates more the number of Ethem than a max which it can hold, based on trust scores which it gained in order to increase its Reputation. It simply starts to Leak.

**Meter scale-->**

**Partial (Unconfirmed) -->** If the Ethem produced during the cashback process is less than a cylinder max holdings. It needs a minimum withdraw able balance to unlock.

**Full (Instant) -->** if the Ethem produced during the cashback process is more than cylinder max holdings, a user can only withdraw a max cap of a cylinder and the left out balance is restored inside the cylinder to get filled again.

1. **Overview of global level scalable consensus**

Well for a distributed state shared ledger to achieve a user base of millions and even billions of users across the wide verity of communities then it simply needs to be scaled up to a global level presences with a effective coordinated commitment from the vast majority of honesty peer’s among the network . With the recent innovation and improvement techniques such as side chains, secure sharding, fesilating the network to perform and scale at its peak limit level performance .But with most of the consensus mechanism built with a core philosophy approaching coordination or competitive method to achieve global consensus either of these both provide a great solution in achieving the classical Decentralized Governance.

Competitive approach seems to provide a greater intuition of motivation across the peer’s which leads to a highly Reputable state model with pure form decentralized well in turn consuming the resources highly in terms of pure computation resulting in its performance declining over the time with its ability failing to scale up on a long run.

But with an alternative coordinated approach it provides a best way to overcome those performance issues in the previous form, But these coordinated approach in achieving the global consensus due to various reasons ranging from closed membership access to other being a complete premined wealth which in turns leads to a less motivated peers across the network, causing a greater centralized control of command in to the hands of few of centralized authorities or even there foundation itself.

1. *Quorums*
   1. *Eligibility*

Any node with a good reputation score can be included in an orbits quorum with a fixed lockup amount of 10,000 Ethem.

* 1. *Formation of Quorum*

Ever Quorum consists of a predetermined two mulitpools called as Slots with one slot having N and N-1 peer nodes along with the ghost node which participate in the consensus process.

* 1. *Rules*

A chosen node on the network can participate in the consensus process with fixed lockup tokens of 10,000 Ethem. And Evoca platform has enabled a standard Outfit Layout for ordinates i.e., there can only be 100 Quorums on both sides of ordinates with two individual orbits in a single ordinate. Resulting in 2 ordinates with 4 multipool orbits.

* 1. *Economics*
     1. *Quorum Payouts*

Each quorum gets a fixed block reward as its payout in teams of XPC and Ehm by Gonos

XPC on producing successful Block on to a global chain and Ehm on Revalidating the Tips of a Block produced by XPCs Block Producer.

* + 1. *Quorum Dynamic*

Dynamic nature of the Quorums is directly based on the circulating supply of tokens which would exist in the market. Due to which the number of peer nodes eligible in a Quorum is strictly limited based on the circulating supply of token which would exist in the market and the number of slot peers to be included in the Quorum might also vary due to inflation.

Quorum contains 2 slots with a majority of the pool’s agreeing upon the Slot1 & Slot2 series i.e., 4-5,6-7,8-9,10-11,12-13,14-15.., of Slot1 and Slot2 respectively can have these pattern set of nodes in them.

Ex: Let say out of 200 consensus Quorums of either 0dd or Even Producers we chose Quorum31 from 0dd Producers

Slot1 might contain 7 individual nodes

Slot2 might contain 6 individual nodes

With a fixed Initial lock up of 10000 Evoca Token’s for Delegation a peer meets up the initial eligibility criteria out of many.

In terms of economics,

Example: Q31 which contains total 13 individual nodes which leads up to 130000 (13\*10000) per single quorum.

Then for 200 quorums from both ordinates (0dd & Even Producers) which makes up about ~26 million (130000\*200) Evoca in creating a single valid block.

With an each Quorum getting a chance of ~ 8 times to produce a block for a period of 24hrs, If a consensus time of creating a new block is ~ 1 minute for both Support and Delegation consensus.

i.e., 1 minute of global consensus yields about 60 blocks per hour than with a rate of 1440 (24h\*60min) blocks per day i.e., 720blocks for each 0dd & Even Producers as the block production in a standard chain format is simultaneous between the 0dd & Even Producers.

Conclusion, the summation of 9 Slot1 nodes and 8 Slot2 would lead to different economic delegation pattern as it is directly proportional to the slot series.

1. **Mimeo Twins Consensus Protocol**
   1. **Core Objective**

Evoca aims to provide a scalable effective consensus model which in turn guaranties higher decentralized network by combining the best practice of both coordinated and competitive approaches in creating a Hybrid Governance model to achieve higher success rate in terms of performance and security. Well in a Evoca the entire network in whole is partitioned into a two segments of ordinates trying to coordinate in processing entirely two different blocks asynchronously at the same time but with one ordinate said not publish the processed ledger without it including the other ordinate’s processed ledger and vice versa. Due to its simple hypothetical design philosophy of odd and even sequence of a chain format ledger in a global asynchronous commitment ledger, it simply follows an analogy of copycats.

**Example:**

When **X** ordinate computes pool performs and **Y** ordinate copy the result and vice versa providing a greater stability and also ensuring mathematical trade fairness. But when **Y** ordinate is off state it copies **X** ordinate by reconsidering in providing the tips equivalent to the fee spent by user when performing a transaction. The process can be divided into several phases as explained below.

Let’s say assume that out of 100 Quorum’s, there are only 99 Quorum’s are active and 1 Quorum is inactive (Pre Published) even before the block generation. Now, Out of those active full synchronized 99 Quorum, A single Quorum is chosen randomly to present its viewpoint about the transaction to the other Quorums.

Let’s say Quorum31 is selected from the above proceedings.

Result of Quorum31’s with its view point about the transaction is gossiped across the network with the help of Q31’s associated Ghost node to the other active 98 Quorums. But those nodes who failed to agree with the viewpoint of the other quorums with a Byzantine failure i.e., 98-17=81.

If Quorum31’s view point about the transaction is accepted with a super majority by the other Quorums of different ordinate, then Quorum31 gets a Right to push the Block on to the global state chain and those 18 nodes (17+1) who, failed to agree upon the new state change during (Pre or Post published) will simply store the globally accepted Block.

Those, Failure Nodes (Byzantine + Pre Published (inactive nodes)) are under serious observation by the community.

**6.2 Phases involved in consensus building:**

**Phase 0 (Pre Published)**

Those nodes that are not full synchronized with the current state of the Blockchain are considered to be inactive and they would be eliminated from the consensus round, and the remaining active nodes take part in the consensus round.

***Phase 1***

When a Transaction is broadcasted on to the network it gets assigned to an active on chain orbit ordinates based on the pre determined sequence of Block height to perform the validation and verification

***Phase 2***

Every quorum on an active on chain goes through the transaction producing its own viewpoint based on its verification and validation analysis.

***Phase 3***

A quorum is chosen securely through random process.

***Phase 4***

A randomly chosen quorum gets to show up its single viewpoint which is produced by its slot pools to its other quorum members.

***Phase 5***

The other quorums get to verify the viewpoint of a block publishing quorum with their own processed viewpoint if the non publishing quorum’s viewpoint gets matched with the publishing quorum’s viewpoint with a higher majority then the chosen quorum gets to publish its result on to the global state chain with the total majority support from its quorum ordinates achieve support consensus.

***Phase 6***

The other nodes which failed during the consensus process would simply store and support its orbit nodes .If the Quorum fails to get the majority, and then other quorum from the same orbit would be elected to continue the consensus process. Reducing the reputational trust score of a failed quorum.

***Phase 7***

Now as entire orbit has a single viewpoint at a transaction ,it can now pass on to the other quorum ordinate and also to its own up heard orbit Asking them to update their state with a formal verification in converting the fee into tips to achieve delegation consensus.

***Phase 8***

If the other three orbits agree about the state then in return a global consensus with 3 on 3 confirmations are achieved through Ethem tips.

**Phase 9(Post Published)**

Those, Failure Nodes (Byzantine + Pre Published (inactive nodes)) are under serious observation by the community.

**6.3 Consensus pattern:**

Global Consensus = Support Consensus + Delegation Consensus

Support Consensus ->validation of TX (Evoca), Computation of contracts (beta), Resource Allocation (RA) i.e., in terms of Storage, Bandwidth etc.

And cast of message for consensus

1. Inward Consensus through Support

2. Outward Consensus through Delegation

Delegation Consensus -> Audit for TX for Ethem Payments and Delegation of stake

For New Node’s to join the network they need to look for a settled block with a global Consensus on ledger by ignoring the current block under (Support Consensus or Delegation Consensus)

**6.4 Slot Peers inside a Quorum during a Consensus**

For a transaction to get valid entire Quorum needs to have a single view-point as it is majority, by considering the internal slot voting percentage pattern.

SLOT1 -> 1 2 3 4 5 6 7 8

SLOT2-> 1 2 3 4 5 6 7 \* (Ghostnodes)

Probable Cases for a slot series pattern of 15 peer nodes, by considering Quroum31 as example:

1. 5 peer nodes in SLOT1 presenting their viewpoint stating Yes to a transaction & Ghostnodes always yes as it is maintained by the foundation itself.

This Results in confirming the transaction as valid in SLOT1 with 6(5+1) nodes positively responding.

1. 4 peer nodes in SLOT2 presenting their viewpoint stating Yes to a transaction & Ghostnodes always yes as it is maintained by the foundation itself.

This Results in confirming the transaction as valid in SLOT1 with 5(4+1) nodes positively responding.

1. 3 peer nodes in SLOT1 presenting their viewpoint stating Yes to a transaction & Ghostnodes always yes as it is maintained by the foundation itself.

This Results in confirming the transaction as invalid in SLOT1 as there was no majority 4 in the consensus.

1. If peer nodes less than 4 in any SLOT present their viewpoint as Yes to a transaction, the transaction would become invalid even though, Ghostnodes vote as yes this Results in confirming the transaction as invalid by the Quoum31 as there is no majority of consensus between the nodes.
2. **Role of Ghost Nodes**
   1. **Liquidated Voting through consensus democracy**

Evoca choose to have a Decentralized Treasury Model which would provide fixed liquidation to its network peers with a fixed inflation rate of n (n<=5) and n decreases up to 1%.

Every active node on a network needs to cast its vote for any considerable or inconsiderable situations during which the decision has to be made, well the choice of vote on various attributes are presented to the nodes in the form of a Menu like Ballot layout.

Ex: Option 1, 3, 5, 2, 4, 6

Well every node on the network gets to choose their priorities among the option by ranking the entire list sorting them with a priority of top to bottom which is presented by the ghost node the option with majority voting win, out of which the higher prioritized option would be chosen as its prime option of a single node. If the, 3rd option gets the higher majority among the other nodes and an entire Quorum in later stages.

* 1. **Local Governance**

**7.2.1 Monitoring**

Every quorum has 2 slots with N and N-1 peer nodes along with the ghost node participate in the consensus process.

**EX**: **Quorum 32**

1 2 3 4 5 6 7 8 **SLOT1**

1 2 3 4 5 6 7 \* **SLOT2**

Ghost Nodes, has many vital roles to play in the consensus process, helping in Recruiting new peer nodes into the quorum slots and also for an easy updates which need to be made from the foundation end.

After the formation of Quorum all the nodes are under the surveillance of the Ghost Node for their behavioral of **SLOT nodes** during the Block generation

**7.2.2Trust Chain Structure**

**TCS is a communication protocol which primary function is to establish a trust pattern between the different quorums and also to reduce the number of internal messaging between the Quorum members using schnorr signature and digital signature aggregation.**

A single node can trust 2 nodes in its quorum i.e., 1 node from its slot & other 1 from other slot i.e., is by forming 50-50% trust chain with non-repudiation and those 2 nodes which trust each other are enable to collaborate each other to obtain the desired output rather than to compete. With this kind of trust pattern when applied on the node the protocol itself make sure there is more off a reliable way in which the peer to peer communication can be built with a limited number of message flow per single across the network

With this kind of loosely bonded 50% trust architecture for a single node would be very efficient because even if 1 node failover to keep up the consensus still it does not matters as there was only 50% loss of trust making the communication to continue with no breakdowns as mentioned in the above statement.

Example:

Even if 9th node Ditches, the lower order nodes don’t get affected as it follows (previous trust chain). But the 8th node loose out 50% of trust, as It is a chain of trust cycle & also the sub inheritance problem of 8th nod it is very important to pass on the trust series from the higher nodes as i.e., trust increases as time line increases.

* If those two slots peer in the quorum starts to communication with each other then there would be a huge bulk of p2p messages passing across the quorums & the network itself.
* Well in order to eliminate the process of bulk messaging & also creating a pure notion of trust between the two slot peers i.e., without the help of a centralized Ghost Node.
* Through a communication bridging protocols called as “Trails/ TCS”.
* Well the slot peers of a quorum which needs to communicate with each other in building up a common viewpoint of agreement about the validity of the transaction made on the network.
* Well the communication between the slot peers would be in a prefixed pattern communicating to well trusted peers of their choice.
* When a peer needs to present its viewpoint it needs to communicates with the other peers.
* But in case of Evoca the viewpoint convincing peer needs to communicate with only two peers.
* The quorum members use schnorr signature to present their viewpoint about a transaction in the form of a initial transaction within a Quorum as they are compact and small in size.
* Take all the signatures of the quorum members and aggregate them to form a single signature.

1. **Fee Model**

Fee Structure = constant ø+ payable ß. “Both the ø, ß are paid out in Ethems”

constant ø 🡪Payable is minimal for simpler Transaction which involves no complex calculations except a simple transfer functions.

payable ß🡪But for a transaction which involves a complex patterns of calculations in the form of contracts the fee will be based on the instructional opcodes of the Ethem shell which are included in it to execute.

1. **VisionDAO**

The decentralized governance structure through which the entire network securely functions starts from incentivizing, consensus building to resolve major issues and primarily to self-funding the project in order to meet the present days requirements.

Well the DAO is primarily controlled by Evoca token holders, who involve in building up the consensus across the network through a secure liquid democratic model of voting in which the lower level peer’s viewpoints are also considered for any major action to be taken on the DAO.

1. **Ethem Shell**

Ethem shell is actually a virtual machine where the Smart contracts are automated in Evoca platform. They are self-executing with specific instructions written on its code which get executed when certain conditions are made.

So, what are the desirable properties that we want in our smart contract?

Anything that runs on a Blockchain needs to be immutable and must have the ability to run through multiple nodes without compromising on its integrity. As a result of which, smart contract functionality needs to be three things:

* Deterministic
* Terminable.
* Isolated.

**Feature #1: Deterministic**

A program is deterministic if it gives the same output to a given input every single time. E.g. If 3+1 = 4 then 3+1 will ALWAYS be 4 (assuming the same base). So when a program gives the same output to the same set of inputs in different computers, the program is called deterministic.

There are various moments when a program can act in an un-deterministic manner:

* **Calling un-deterministic system functions:**  When a programmer calls an un-deterministic function in their program.
* **Un-deterministic data resources:**  If a program acquires data during runtime and that data source is un-deterministic then the program becomes un-deterministic. E.g. Suppose a program that acquires the top 10 Google searches of a particular query. The list may keep changing.
* **Dynamic Calls:**  When a program calls a second program it is called dynamic calling. Since the call target is determined only during execution, it is un-deterministic in nature.

**Feature #2: Terminable**

In mathematical logic, we have an error called “halting problem”. Basically, it states that there is an inability to know whether or not a given program can execute its function in a time limit. In 1936, Alan Turing deduced, using Cantor’s Diagonal Problem, that there is no way to know whether a given program can finish in a time limit or not.

This is obviously a problem with smart contracts because, contracts by definition, must be capable of termination in a given time limit. There are some measures taken to ensure that there is a way to externally “kill” the contract and to not enter into an endless loop which will drain resources:

* **Turing Incompleteness:** A Turing Incomplete Blockchain will have limited functionality and not be capable of making jumps and/or loops. Hence they can’t enter an endless loop.
* **Step and Fee Meter:** A program can simply keep track of the number “steps” it has taken, i.e. the number of instructions it has executed, and then terminate once a particular step count has been executed. Another method is the Fee meter. Here the contracts are executed with a pre-paid fee. Every instruction execution requires a particular amount of fee. If the fee spent exceeds the pre-paid fee then the contract is terminated.
* **Timer**: Here a pre-determined timer is kept. If the contract execution exceeds the time-limit then it is externally aborted.

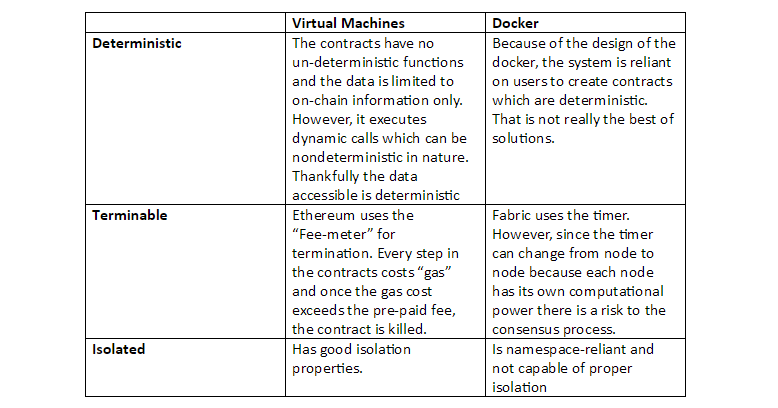
**Feature #3: Isolated**

In a Blockchain, anyone and everyone can upload a smart contract. However, because of this the contracts may, knowingly and unknowingly contain virus and bugs. If the contract is not isolated, this may hamper the whole system. Hence, it is critical for a contract to be kept isolated in a sandbox to save the entire ecosystem from any negative effects.

Now that we have seen these features, it is important to know how they are executed. Usually the smart contracts are run using one of the two systems:

* **Virtual Machines:** Ethereum and Neo use this.
* **Dockers:** Fabric uses this.

Let’s compare these two and determine which makes for a better ecosystem. For simplicity’s sake, we are going to compare Ethereum (Virtual Machine) to Fabric (Dockers).



So, as can be seen, Virtual Machines provide better Deterministic, terminable and isolated environment for the Smart contracts. However, Dockers have one distinct advantage. They provide coding language flexibility.

In a Virtual Machine (VM) like Ethereum, one needs to learn a whole new language (solidity) to create smart contracts.

1. **String Swap through VisionDAO** **& Hot Delegation**

The popular tool for micro financing in the Middle East Asia is through a secure protocol called as chit fund in which lending and borrowing money is made between peer to peer people who are interested in it to participate to meet there financial needs through a well trusted 3rd party called as foreman who manages the fund as a collective pool.

Well the string swap protocol main purpose is to achieve a peer to peer money swap through a chit mechanism by eliminating 3rd party institute or a foreman through a VisionDAO

String Swap is a modified chit strategies which is designed to holds up the same core functionalities of the pure chit protocol as it is tough to achieve traditional chit as per the current limitations of technical advancement in the space itself.

Mechanism:

The chit mechanism would need few prerequisites to meet so that the entire protocol works as per it is intended to work that is general consensus about the,

1. Number of people involved in the chit protocol,
2. Individual contributions per single turns,
3. Duration of the chit protocol,
4. Regular updates.

Summary:

User with two accounts

1. Main Account

The primary account of the user through which he pays up his contribution each time.

1. Collateral Account

The secondary account of the user through which he shows up his loyalty towards a secure chit cycle.

VisionDAO: A substitute for the 3rd party institute or a foreman in a decentralized Evoca platform.

Notice:

1. ”M = total no of peers involved in a chit protocol.”
2. “n =no of participated peers in a specific chit cycle ,were always n>0 ”
3. Duration of the chit cycle ~ no of people.

Auction Model:

1. English Model:

Price Moves with an uptrend, under a competitive n/M peer model.

1. Dutch Model:

Price Moves with a downtrend, under a conservative 1/M peer model.

Differences between Chit and Collateral contracts.

|  |  |
| --- | --- |
| Chit Contract | Collateral Contract |
| Main account for the active protocol. | Acts as collateral in case of a needy withdraw. |
| If the peer wins up a slot in his current turn then his pot is [**toTo minus DAO’s fixed % cut**]. | Gas is produced based on the toTo in a collateral account. |
| Now, peer has his choice to withdraw the funds or not too. | Locked vault gets triggered only, if the peer fails to keep up his consistency. |
| If the peer chooses to withdraw the funds. | Collateral contract gets triggered. |
| After withdrawal the main account gets dividends regularly from the other peer’s turns in the form Evoca. | And regularly pays up its remaining share, till the end of the protocol. |
|  | Additional Evoca which are staked in as collateral to an active chit protocol in a Collateralised contract can be referred in a form of Hot Delegation. |

The dividends received during this chit cycle are of two types:

1. Ethems by hot delegation in collateralized contract.
2. Evoca by chit protocol as hot dividends in Chit Contract
3. **Incentive Structures in Evoca Platform**

The prime success of permission less Blockchains in the cryptospace is due to the incentivisation, which motivates the general public to part of it. But the level of innovation in the incentive structures is also highly required. The incentivizes varies from different platform to platform.

The main clear vision of Evoca Platform is to be First Blockchain which can give out higher incentives to the platform users. As incentives is the prime factor of motivating the users.

In Evoca platform the user can more off a earn crypto rather than to buy crypto,

**Hot and Cold Delegation, Cashback, Ethem Dividends, Block Rewards**

1. **Ethem Payout structure for a block generation**

**The generation of a block with a global consensus would create new resource tokens, Ethem which would be fairly divided and distributed as 70% of cashback to the initiators of the transactions present in a current block & 30% is paid out as dividends for the existing staked Evoca holders from a 100% share of Ethem.**

That is Block Rewards for a Successful quorum gets a fixed block reward as its payout in terms of 25 Evoca and 50 Ethem tokens i.e., in terms of creating or Birth of new tokens causing an INFLUATION.

**13.1 Cashback:**

Ethems are given out as cashback to a transaction’s which were included in current valid block well the cashback are not given out in terms of standard percentages like 15, 10% etc because the cash back’s in terms of percentages lead to variable block rewards. The distribution pattern of 30 Ethems as cashback is split between the Transactions which are present in that block based on the payees accounts Trust Scores.

CuCy Expander has a constant effect on Cyfu staking. CuCy & CyCf are interlinked that if Cyfu increases then staking can be increased.

In simple,

When an account with a higher Trust Score does a Transaction gets a bit of higher cashback in Ethems, than an account with a lesser Trust Score doing a Transaction.

“Proportional-Cake- Cutting Problem, Divide Consensus”

Notice: CuCy 🡪 Cuisine Cylinder Expander

CyCf 🡪 Cuisine Cylinder Function.

**13.2 Ethem Dividends**

**Every time a block is generated with a successful global consensus it would create new Ethem out of which 30% is paid out as dividends for the existing Evoca holders who staked their Evoca tokens. “**Envy-Cake- Cutting Problem”

The biggest differentiating feature is the two-tiered system of EVOCA and ETHEM. Although ETHEM can be bought and sold on a handful of exchanges, users typically buy EVOCA tokens, which represent their stake in the future of the platform. The benefit of the two-tier system comes into play the moment you transfer EVOCA to your EVOCA-compatible wallet.

While holding EVOCA, you start generating ETHEM automatically as more blocks are generated by the construction of the Blockchain. With every new block generated, 25 ETHEM are distributed for all 100,000,000 EVOCA in existence.

This is similar to Ethereum, but very different from mining in Bitcoin in that the value of ETHEM is decoupled from the value of EVOCA. This is in contrast to Bitcoin, where the value of a Bitcoin mined is the same as the value of a Bitcoin purchased.

ETHEM is used to pay for transaction fees on the EVOCA network.

**Gas Decay:**

Gas Decay, being a Deflationary Model, For 1 Token to reach 1 gas is @ the rate of (\*) to reach ~100%

\*-15 days @ 6.6

-30 days @ 3.3

-45 days @ 2.2

-60 days @ 1.65

-75days @1.33

1. **Conclusion**

Able to scale up to millions of Users on a longer run through various measures such as Higher motivation for the Lower Peers on the network to behave honestly through Gift Economy and a right Monetary Policy such as Circular in building a better Decentralized Governance Model by achieving block scalability through Liquid Democracy.

**References**

**[1] https://reddcoin.com/papers/PoSV.pdf**

**[2] https://credits.com/Content/Docs/TechnicalWhitePaperCREDITSEng.pdf**

**[3]** Nakamoto S : Bitcoin: A peer-to-peer electronic cash system. **https://bitcoin.org/bitcoin.pdf**

**[4] https://www.stellar.org/papers/stellar-consensus-protocol.pdf**

**[5] https://eprint.iacr.org/2016/889.pdf**

**[6]https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Byzantine- Generals-Problem.pdf**

**[7]http://docs.Evoca.org/en-us/basic/consensus/consensus.html**

1. **Glossary**

**Paradox of Thrift** Economic concept that if everyone tries to save an increasingly larger portion of his or her income, they would become poorer instead of richer. This is because the economy will slow down from reduction in demand and the very same people would lose their tokens value. This theory, however, applies mainly to Keynesian economics where increased savings represent a diminishing circular flow of income.

**Paradox of Value** Also known as the Diamond-Water paradox it explains how the price of a commodity is based not only on its value-in-use but also on its value-in-exchange.

**Paradox of Choice** The assumption is that if choice is good more choice is better that’s not necessarily true.

**Account**

A combination of two different addresses i.e., Ethem and Ecova

**Total Kitty**

**Chit cycle**

**Foreman**

**Group Trust score**

**Individual Trust score**

**Turns**

**Cold Delegation**

A peer account which has enough of tokens can still provide a supportive notion in the consensus process by delegating their tokens to a quorum of their trusted choice in a special Lockup contract representing a delegated voting right to that quorum, and receiving a long term Cold Dividends on a successful Block Production