MI_CARE EHEALTH SERVICE PROTOCOL TECHNICAL SPECIFICATIONS.

DESIGNED BY

Mulongo Duncan | Steven Kamau | Duncan Santiago | Patrick Oluoch

MI_CARE EHEALTH SERVICE
www.mi_care.org

Abstract: MI_CARE is a completely peer-to-peer decentralized privacy preserving e-health service and crypto which is built on block-chain technology. Its implementation follows from several cryptographic protocols which are used to achieve anonymity of actors over the block-chain and establishing consensus among participants on the platform while securing the MI_CARE network. Unlike the energy-intensive Proof-of-Work [PoW] protocol as used by Bitcoin cryptocurrency, MI_CARE employs an energy-efficient Proof-of-Stake [PoS] protocol and a lightweight Zero-Knowledge-Proof [ZKP] protocol. The protocols work to secure the MI_CARE network and to preserve the privacy of participants on the block chain. In this way, the MI_CARE is built to serve both as an efficient, accurate and honest e-health service and a cryptocurrency network employing tokenization of health services and using them as a value carrying asset in form of tokens [Hert-Bits]. MI_CARE serves to eliminate the need for health intermediaries by linking clients directly to health services, maintaining medical accuracy through diagnosis and/or prescription validation and allowing participants to transact seamlessly without restriction or borders.

Abbreviations: ZKP, PoS, PoW, PoV, HTB NHS, POPV, PRPV.
Keywords: Agreements, Consensus, Bitcoin, Health service providers, Tokenization.

Introduction: While healthcare stands as a basic need to guarantee human survival, many a time it proofs very difficult for health clients to access quality health services in an efficient manner. And with the surge in the demand of healthcare services in our current world, health service providers have struggled to meet the needs of their clients due to a poorly connected health sector. Many health providers depend on current client's health status and additional fragmented information of the client's medical past in order to provide health services. In world that is riding on an ever evolving cutting edge technology, there is great need to organize tools that come with modern technology and optimize them for human survival. Rarely have health sectors taken advantage of block chain technology in implementing systems that ensure secure medical data exchange, collective decision among various specialists in the health sector and guarantee pure medical diagnosis, one that is free of human errors and data corruption.

Trust based model as used in current health service arena offers an incomplete implementation of an efficient, affordable, transparent and mostly accurate health service. Although it is very difficult to design a system that can achieve a completely accurate health service, it possible to reduce medical inaccuracies to as low as 5% by use of block chain technology and artificial intelligence. In existing models, the client must bet on their belief and money by trusting a specific health service provider who may at a times fail to understand the client full and accurate medical past. So far, there exist no solid mechanism that can validate medical diagnosis and/or prescriptions without relying on trusted parties and limited basic principles.

It plausible that there be a way to proof the veracity in the applicability of a given health service which could be some prescription, medication, therapy, rehabilitation etc. Such a service should take into account many factors surrounding the client and not just universal principles of health provision. Cryptographic proofs as applied to block chain could be a game changer in attaining transparency in providing health services. The need for trust is completely eliminated as trusted parties are dislodged from the model. This new method protects the clients against fraud, misdiagnosis and medical inaccuracies by ensuring that health service decision making process and service dissemination is completely decentralized and distributed among various health specialist and/or health service providers.

Consensus: It refers to a general agreement reached among a group of participants.
In a block chain network, such a process could be formalized by specifying the number of nodes required to agree on the global state of the network for a consensus to be reached.

Consensus Mechanism: It refers to the entire stack of protocols, incentives and ideas that allow a network of nodes to agree on the state of a block chain.

Proof-of-Stake & Proof-of-Veracity: MI_CARE bases its consensus mechanism on Proof-of-Stake protocol whose crypto-economic security involves a set of rewards and penalties applied to capital locked by Stakers. The incentive structure encourages individual Stakers to operate as honest validators, punishes those who don't, and creates an extremely high cost to attack the network.

Proof-of-Stake: Is a way to prove that validators have put something of value into the network that can be destroyed if they act dishonestly. In MI_CARE's Proof-of-Stake, validators explicitly stake capital in form of (HBT) into a smart contract on MI_CARE. The validator is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves. If they try to defraud the network (for example by proposing multiple blocks when they ought to send one or sending conflicting attestations), some or all of their HBT can be destroyed.

Validators: To participate as a validator, a health service provider must deposit some HBT not less than a predetermined amount into the deposit contract and should be running a software capable of executing a client, consensus and a validator. On depositing their HBT, the health service provider joins an activation queue that limits the rate of new validators joining the network. Once activated, validators receive new blocks from peers on the MI-CARE network. The transaction delivered in the block are re-executed to check that the proposed changes to MI_CARE's state are valid, and the block signature is checked. The validator then sends a vote (called an attestation) in favor of that block across the network.

Proof-of-Veracity: How can a client verify that a given diagnosis/ or prescription is applicable? Or how can a patient verify and confirm the most efficient medication and/or health routine based on the confirmed diagnosis and/or symptoms?

While Proof-of-Correctness works via loop invariant, which are statements which are true throughout every iteration of the loop, the Proof-of-Veracity achieves the same objective by use of consensus mechanism. Instead of many iteration of loops in a query-response mode, the Protocol sends the query [proposed data block] to as many specialist and/or health service providers as possible. The veracity of a given block of data is achieved only after a consensus is reached. Unlike the traditional consensus mode which relies on one validator one vote in a discrete sense, Proof-of-Veracity employs a continuous view of attestation from validators. The validator does not limit his validation by issuing a thumbs up or down but goes ahead to explain the reasons behind the vote. In this view, the weight of a given block of data being validated is not only decided by the number of votes issued but also by the similarity in the backing [logical explanations] of such votes. Such attestations are therefore measured in terms of probabilities which indicate how similar a piece of explanations compares to attestations by other validators.

To safeguard the transparency in the attestations, the voting is done in such a way that no validator knows about who the other validators are and what their attestations are. By so doing, the Protocol is fashioned against colluding and cheating thus eliminating any possibility of bias in the attestations.

Proof-of-Veracity is based on the fact that for any diagnosis and/or prescription given by specialists and/or health service providers on the MI_CARE network operating under similar governing principles and/or agreements should replicate same results. Any contradiction is considered as dishonesty. For a specialist and/or health service provider (A) using mode A(m) with tools A(t) under conditions A(c) should match with the results of specialist (B) using mode B(m) with tool B(t) under conditions B(c).

Hence the equation; *[A,* $A(m)$*,* $A(t)$*,* $A(c) == B$*,* $B(m)$*,* $B(t)$*,* $B(c)$*].* With arbitrary choice of specialist, Procedures, conditions and tools, the above equation should always hold true for diagnosis and/or prescription to guarantee veracity and validate a block of data on the MI_CARE block chain.

On MI_CARE network, any diagnostic results is treated as a claim until a validation is done by use of the PoV protocol. Hence blocks of data are placed on the unverified queue until they are validated and appended at head of the block chain.

It is possible to make client's symptoms and/or diagnosis public while keeping the client anonymous using the Naked-Hare-Scheme [NHS]. The naked hare decides to cover his face instead of his genitals while his in-laws passes by the river where he is accidently encountered on his bath errands. If he were to cover his genitals and exposed his face, it could be embarrassing for it would be easy for him to be identified and probably shamed, in this mode, the genitals which are considered private are exposed but the identity of the owner is anonymized, the genitals represent client's sensitive medical and/or health records while the face represent the identity of the client. We propose an interactive approach PoV where queries in form of diagnosis and/or prescriptions which form the data block to be validated are gossiped on the network.

In the case of diagnosis and/or prescription via 'Trusted Initiator' and/or "block proposer" who is chosen at random based on the client's preference among validators, we propose a verification step through validators and/or health service providers. The initiator is tasked with creating a new data block which could a prescription and/or a diagnosis. The validator sends out the data block to the block chain where the smart contract assigns it to authenticated validators who may be chosen at random from those who qualify to perform validation. Different data blocks will need different validators chosen based on the type of health services they can offer.

There could be a witness in form of an AI which could be implemented in the smart contract. The witness acts through a smart contract and serves as a moderator which compares attestations from validators and assign them variability ratios. The more close the response are, the stronger the consensus. The POV protocol is designed to test for consensus while the Witness serves to confirm such tests of consensus. An AI system may have access to a particular client's medical data and other records of interest. Such an access is authorized and secured through Public-Private key encryption scheme such that no one, even the validators can snoop on the data being authorized to an AI. The AI preserves a copy of the entire block chain state just like other nodes does. In the case where the client proposes and/or initiates a new block of data which could be symptoms which seeks diagnosis and prescriptions, insurance requests, payments etc. Such a request is gossiped directly on the network without the need of a random initiator. By saying so, we imply that a client as so long he/she is certified on the network can work as a block proposer. He or She may not necessarily be a validator in the literal sense but there exist contribution from his node in such a way that he can authorize a witness, the AI, to access his health records to be used while validating data blocks.

Several steps could be involved during the POV test and consensus confirmation.

1. A comparison among attestations of validators is performed and variability ratios and/or probabilities $[S_0/S_x]$ calculated based on how attestations vary from each other. This is done by use of an AI [Witness] implemented in a smart contract based on given agreements and conditions. This will be discussed further.
2. A comparison of each validator's attestation is compared to the ledgers' verified attestations. $[A_s/A_l]$.
3. The Average attestations' value by validators is compared to the ledgers' verified attestations. $[A_v/A_l]$.
4. Each validators' attestations is compared to the average of validator's committee attestations. $[A_s/A_v]$.
5. Accuracy levels are calculated from the above factors by a witness that leverages and balances facts on the ledger, client's records and validators' attestations.
6. Block validation completion. The proposed block may be validated and appended to the block chain head. It fails to be validated, an entirely new block could be generated during the validation process basing its argument from the client's requests. This is done by coupling many factors surrounding validators and the client's health record and agreements by the smart contract. Once this is completed, the recommendation is send to the client to pursue further actions which could be treatment.

Validators on the block chain are completely anonymous and their attestations are kept private to avoid collusion and eliminate bias. The smart contract in tasked with performing the above steps.

Zero-Knowledge-Proof: A zero knowledge proof is a way of proving the validity of a statement without revealing the statement itself. The "prover" is the party trying to prove a claim, while the "verifier" is responsible for validating the claim.

In the case where some validators may want verification on how the validation has been performed and how the consensus have been reached, the AI will employ the ZKP to convince the validators that a particular verified block is valid by confirming queries given via an interactive approach where the veracity of a given data block is given without revealing the client's personal data or other validators attestations. Equipped with data on the Block Chain and client's health records, the AI can determine the probability of a person having disease X. This has to be verified and voted for. As much as an AI can serve as a witness comparing the attestations and establishing consensus among validators, it can also serve as a block proposer based on the symptoms given and other diagnostics.

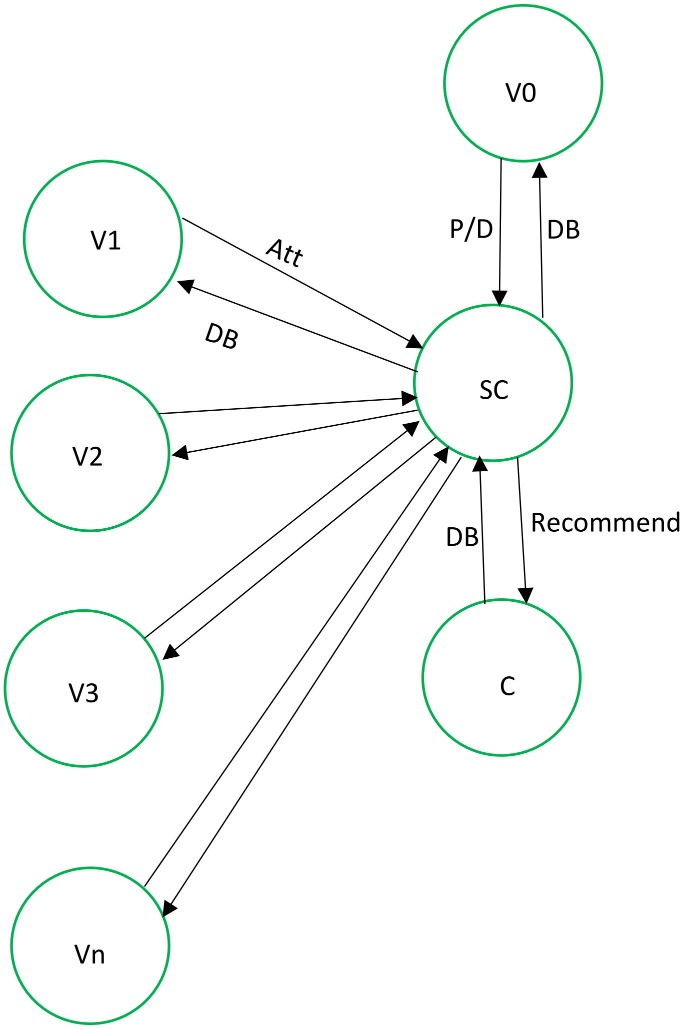
Contradictory attestations attracts penalties while consistence attestations leads to a reward in form of HBTs. This among others will be discussed later while detailing Tokenization protocol as it will be used on MI_CARE network.

Efficiency: We propose a delayed validation approach where results of a given diagnosis and/or prescription are not guaranteed to be instant. A track record of both validated and yet-to-be-validated data blocks is kept. By default, gossiped data blocks will be added to the yet-to-be-validated block and after they are verified, they are appended to the block chain head.

In the case of an emergency, one could be attended to and prescribed in whichever mode by an authenticated validator but the diagnosis and/or prescription given may be gossiped on the MI_CARE network as a new data block which requires validation, this is Post Prescription Validation, [POPV]. This seeks to reinstate a particular prescription or falsify it.

In the case of a risky medication, the most efficient prescription should be determined before such a medication is authorized, this is Pre-prescription Validation, [PRPV]. This seeks to confirm the safety of a given prescription and applicability of a given prescription.

Tokenization: Based on Proof-of-Stake and the PoV, we propose a tokenization protocol in which service providers and clients can transact by use of a token, HBT, (a value holding asset native to MI_CARE). Such a token could be mostly stable due to unchanging nature of health services. Before any client, health service provider is certified to become a block proposer and/or validator on the MI-CARE network, he/she must deposit a predetermined amount in HBTs on MI_CARE. Any successful validation of a data block is rewarded in form of HBTs and any dishonesty acts are penalized by destroying some or even all staked HBTs of a given validator and/or block proposer.



KEY

The relationship between validator V0, Smart contract SC and Client C is in this case indirect data block proposition.

Eliminating V0, becomes a direct data block proposition which involves the client and the block chain without going through a Trusted Initiator, V0.

V: Validator

SC: Smart contract with AI

C: Client

Att: Attestation (Vote), DB: Data block,

Note: How payment is done has not be shown on the diagram.

We have only considered a single service involving a client and a medical service provider. This can be generalized to cover other services like gym, insurance, nutrition Etc.

This doc may contain unintentional errors