Article

Resolving the Blockchain Paradox with Dynamic Immutable Smart Contract (DISC)

Fazal Raheman[1], Tejas Bhagat[1], Akash Dyama[2], Ali Raheman[2], Sajid Anwar,[3] Pieter Becue,[4] Vincent Sercu[4]
[1]Blockchain 5.0 OÜ, Kesklinna linnaosa, Ahtri tn 12, 10151, Tallinn, Estonia
[2]Autonio Foundation Ltd., 5 High Street, 2nd Floor, Bristol BS9 3BY, UK
[3]Department of Mathematics, Anjuman Engineering College, Nagpur 440001, India
[4]W-ILAB.T, IDLab-imec-UGent 9052 Gent, Belgium
drfazal@bc5.eu (FR) tejas@bc5.eu (TB), Akash Dyama (ard.ngp@gmail.com (AD) ali@autonio.foundation (AR), sajidanwar0616@gmail.com (SA), pieter.becue@ugent.be (PB), Vincent.Sercu@ugent.be (PB).
Correspondence: drfazal@bc5.eu Tel.: +441216600153

Abstract: While immutability is Blockchain's* much celebrated covenant, change is the rule of life. The paradox has seriously limited real-world deployability of Smart Contracts (SC), faltering its mainstream adoption and sustainability. Once implemented, SC remains unstoppable even if its execution makes losses, as evident in the recently exploded $50+B DeFi industry. How do we reconcile the two and make DeFI/Blockchain profitable and sustainable? A DISC (Dynamic Immutable Smart Contract) hypothesis was proposed to resolve the paradox. Using an existing decentralized IoT device framework we test the DISC hypothesis, by designing/implementing a DISC protocol that delivers an algorithmically controlled dynamic off-chain data feed into a self-executing SC. The experiment successfully introduced limited dynamism into SC without compromising its immutability or undermining user control over their SC terms. If consistently reproduced in diverse settings, the DISC protocol could earn an important milestone in the evolution of Blockchain's decentralized economy of the future.

Keywords: *Blockchain Paradox; DISC Hypothesis; Smart Contract; DeFi; Oracle; AI, Sustainable.*

**All references to Blockchain (BC) and its immutability throughout this paper, imply public/permissionless blockchain. Private or permissioned BC are mostly controlled by vested interests, and hence may inherently be predisposed to mutability.*

1. Introduction

Blockchain (BC) technology, introduced in 2008 by Satoshi Nakamoto, is the underlying mechanism for cryptocurrencies such as Bitcoin [1]. Cryptocurrencies are currently witnessing a second bull run surpassing a Trillion-dollar market cap. Bitcoin first peaked a record high valuation in the December of 2017 [2] and created a hype around digital currency, eventually crossing an all-time high of 60,000 on 13th March, 2021 [3]. Since Bitcoin's debut, there has been numerous cryptocurrencies based on different blockchains, holding billions of dollars in market cap each. BC is essentially a "distributed ledger or database" where all the transactions are documented regarding all the participating parties. it is a chronological chain of blocks, where each block can be considered as a page in a traditional ledger. The chain grows continuously as miners discover new blocks and append to the existing blocks. Each transaction is broadcasted in the network via cryptographic communication while miners would try to collect as many transactions as they can and verify them using a consensus protocol such as "proof-of-work" or "proof-of-stake" and create a new block. Miners compete with each other to create such blocks. Once a winning block is appended to the existing chain, a new copy of the block is broadcasted to the entire network, thus, creating a decentralized public ledger. While miners or block producers are responsible to verify transactions and update the BC, they are incentivized with rewards. While the traditional ledger technologies need a trusted third-party such as bank, BC is trustless.

In 2013 Vitalik Buterin published a white paper disclosing Ethereum as a new BC that supported a next generation self-executing smart contract, "a piece of code implementing arbitrary rules or even blockchain-based decentralized autonomous organization (DAO)" [4]. However, the term "smart contract" was first introduced by computer scientist and cryptographer Nick Szabo in 1996 as a graduate student at University of Washington. [5] According to Szabo:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

> *"New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart," because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A Smart Contract (SC) is a set of promises, specified in digital form, including protocols within which the parties perform on these promises."*

Szabo explicitly clarified that by "smart" he meant smarter than paper contracts because they can automatically execute certain pre-programmed steps, but not to be seen as deploying artificial intelligence tools that can parse a contract's more subjective requirements. One of the defining properties of smart contracts is that their code is immutable, meaning the parties agree to the terms or "code" of the contract, and that code can't be changed by any party unilaterally, but objectively verified by each party to the contract. As such the result of the execution of the smart contract is unchangeable.

Perhaps, it's time we revisit Szabo's original vision and make SC really intelligent using the modern machine learning techniques and, in the process, resolve the BC paradox, making the self-executing SCs more flexible and compatible with the fundamental rule of life:

"Change is the only constant in life" [6].

Life encompasses intelligence, and intelligence entails dynamism, but SC mandates immutability. If data reflects the reality of life, it has to adapt to the dynamics of life, and change accordingly. But in SC, the data stays frozen in time. Is it the lack of dynamism in BC that's holding it from becoming the promised Trillion Dollar industry [7], despite virtually enabling the $1 trillion market cap in the crypto markets? [8].

Professor Lehdonvirta of Oxford asserts, the blockchain paradox is essentially born out of the conflict between the immutability of SC and the change that real world governance entails:

> *"Blockchain technology may provide for completely impartial rule-enforcement, but that is of little comfort if the rules themselves are changed. This rule-making is what we refer to as governance."*
>
> - Professor Vili Lehdonvirta in **The Blockchain Paradox [9].**

Since the rules governing contracts are subject to change creating a regulatory paradox, developing a sustainable BC-based solution for anything beyond cryptocurrency is turning out to be a huge challenge [10]. Rather, it is posing as a show-stopper for real world applications beyond "*the digital bearer instruments"* [11]. While the global BC adoption pace faulters, critics, a plenty, are calling it "an amazing solution for almost nothing," [12] or "meaningless" [13]. In the meantime, the BC paradox lives challenging us with the big question:

> "*How do you change or introduce dynamism into something that is 'immutable'?"*

SC Immutability: The Show Stopper?

Lauded as a world changer, countless use-cases have been proposed [14] by numerous BC experts [15], but BC hasn't yet seen a single blockbuster real world use-case in over a dozen years of its existence. Of course, two cryptocurrency bull runs kept the excitement alive. Perhaps cryptocurrency is the only BC use case that works fine with pure immutability devoid of real-world dynamism. In fact, the crypto boom has taken the world by storm, and facilitated the worldwide adoption of Ethereum SC, first with the 2017 ICO boom, and now with the DeFi revolution 3 years later. Decentralised finance (DeFi) has exponentially grown from a couple billions to $50+ billion ERC20 tokens locked in liquidity pools as automated market making (AMM) SCs in previous 9 months [16].

The recent rise of DeFi not only brought opportunities to generate staggering returns but a wave to innovate, and an urgent need to resolve the BC paradox. DeFi has billions locked in SCs that secure citizen assets & put them in control of their investments. But unfortunately, SC immutability does not allow any dynamic altering of SC terms if the market changes [16]. That means no room for stop-loss, fee-break, arbitrage, etc to minimize losses. They seem to be delivering in current bullish market, but are likely to falter once bulls exit. Hence current DeFi tools are not sustainable.

Although scalability of BC, for long considered as the original enemy of its mainstream adaption remains unresolved, its immutability is increasingly receiving much attention as a major hurdle. This is essentially because

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

the BC stakeholders have been busier dealing with the scalability problems. Our focus on resolving the paradox in no way implies that BC's scalability trilemma, or for that matter any other bottlenecks are resolved. Vitalik Buterin, founder of the Ethereum project, explained that regarding scalability, security and decentralization, any improvement in one of these aspects will negatively impact on at least one of the other two [17]. For instance, the most scalable and active BC today with 63 times more daily operations than bitcoin – EOS, still suffers from some serious scalability problems [18]. This is evident from the fact that just over two years into operations, running the EOS full node has become economically unsustainable because of its unprecedented growth (4 terabytes in first 8 months of it going live) [19]. At that rate it's already estimated to be north of 12 terabytes, and economically unsustainable for all the 21 EOS block producers to run. Notwithstanding the fact that EOS is still far from mainstream adoption. Another glaring evidence comes from the latest Hurun Report on Global Unicorn companies, which includes 12 blockchain companies in its list of 586 unicorns, but none of those 12 rely on SC as enabler of their core BC business [20]. Out of 5473 BC companies launched between December 2016 & February 2021 as reported by Angel List (https://angel.co/blockchains) [21], we didn't find a single company in production grade implementation of SC technology for a real-world use case.

SC in essence is a computer code executed in a sandboxed environment, a milieu that restricts them [22]. That restriction provides special functions and properties: the famous blockchain immutability is one of them [23]. It seems, the most revered characteristic of SC is becoming its own nemesis as far as real-world use cases are concerned.

Introducing a bit of flexibility to accommodate the real-world changes might help the cause of BC. But how can you make IMMUTABILITY dynamic? We closely examined the paradox that real-life implementation of SC is encountering, and framed a hypothesis to reconcile SC's immutability with life's reality of "CHANGE".

Dynamic & Immutable SC (DISC): The Hypothesis

Traditional transactions pertaining to human activity involve human intervention, and hence the change or dynamism will always be subjective lacking immutability. However, that may not be the case if the change is objective, algorithmically controlled and beyond human intervention.

In an SC, a cryptographic hash function freezes an objective parameter and renders it immutable algorithmically. In the same way, a dynamic parameter can be hard coded and rendered objective using mathematical algorithm to inject such -algorithm-determined dynamic parameter in the SC code. The algorithm may either be plain mathematical or AI-modelled and machine-learned. In either case introduction of a dynamic parameter into the SC ensuring its independence from human tampering and guaranteeing immutability. Based on this logic we framed the following hypothesis to build dynamic immutable smart contract (**DISC**) for resolving the BC Paradox [24].

It is the mathematical algorithm that renders smart contract immutable, it has to be mathematical algorithm that can inject dynamism in smart contract without compromising its immutability.

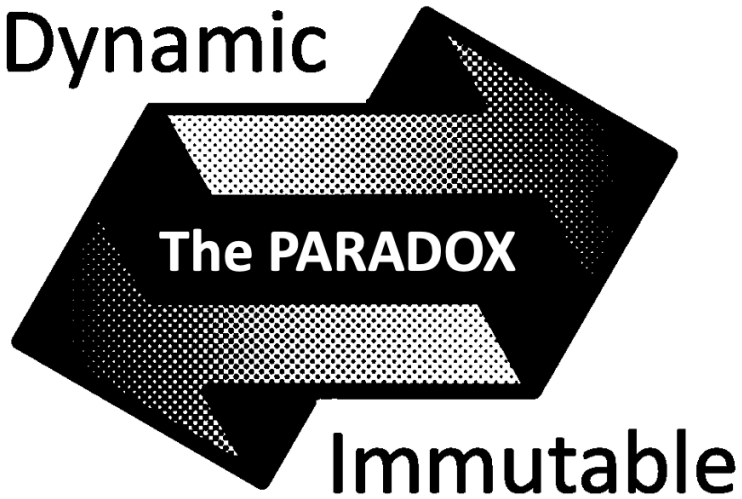

Fig. 1. Blockchain's DISC Paradox (Image Credit: Medium) [24].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

Methodology:
(a) Supporting the Hypothesis with Literature Review

The DISC hypothesis that we framed finds some support in the peer-reviewed literature. In a review article Wöhrer and Zdun suggest that a dynamic parameter can be introduced in the blockchain architecture by coding two smart contracts and linking them together to operate in unison as a base SC and a satellite SC [25]. The base SC can outsource its *"functional units that are likely to change, into separate [] satellite smart contracts and use a reference to these contracts in order to utilize needed functionality."* Essentially dynamism can be introduced in BC by creating an additional satellite SC that encodes the dynamic parameter, and calling the satellite SC from the original base SC to execute the dynamic parameter. Thus, this protocol has three main transactions: the first one is used to update the address referring to the satellite deployed, the second transaction serves to process and calculate the value of the variable relaying to intermediate call of a satellite, and the third one serves to use the calculated result stored in a variable in order to adapt the contract behaviour based on that variable.

While Wöhrer and Zdun's review provides a theoretical support to the DISC hypothesis, a tangible evidential support comes from an experiment by Adnan, et al [26] describing *a model of a dynamic smart contract for permissioned blockchain* in which the dynamic parameter is stored as an off-chain asset instead of being hard-coded in the smart contract logic, as any classical constant/parameter. Since a permissioned blockchain isn't optimally decentralised, and may not meet the strict immutability standards, any proof of injecting dynamism in its smart contract may be at best debatable.

Oracles have also been proposed to mitigate the unstoppable limitation of BC. "**Oracle**", in ancient Greek tradition, were thought to be portals through which the Greek gods spoke directly spoke to people. In classical literature, it essentially implies a person through whom a deity speaks, or a person known for giving wise or authoritative decisions or opinions. In the world of BC oracles are code connecting a BC with real world. They provide the data that smart contracts need in order to execute successfully. Essentially, Oracle is a way for BC to interact with the off-chain world, transferring data between the outside world and the BC [27]. However, the implementation of oracles poses considerable conceptual challenges as they can be regarded as a centralized point of failure or may introduce security and trust concerns [28]. Consequently, much of the research regarding oracles focuses on how to address these security and trust concerns. Xu et al proposed using multiple independent oracle instances to form a decentralised oracle [29]. A considerable attempt to limit the oracle problem was made by Chainlink [30], who proposed a system of decentralised oracles, based on reputation, to reproduce the consensus mechanism of a blockchain. When deciding which data to upload on the blockchain, it takes into account the majority of oracles with the same data and the reputational level of each oracle. The data confirmed by the majority of the oracles are then uploaded on the chain. This system indeed reduces the chance of oracle malfunction; however, collusion or deliberate data tampering could still be performed by the companies controlling the service. Failing to address the oracle problem poses a severe threat to investigating and developing real-world BC applications [31].

More recently Mühlberger, et al [32] addressed the problem by studying foundational BC oracle patterns in two foundational dimensions characterizing the oracles:
(i) the data flow direction, i.e., inbound and outbound data flow, from the viewpoint of the BC; and,
(ii) the initiator of the data flow, i.e., whether it is push or pull-based communication.

They provided a structured description of the four patterns in detail, and explained implementation of these patterns based on use cases.

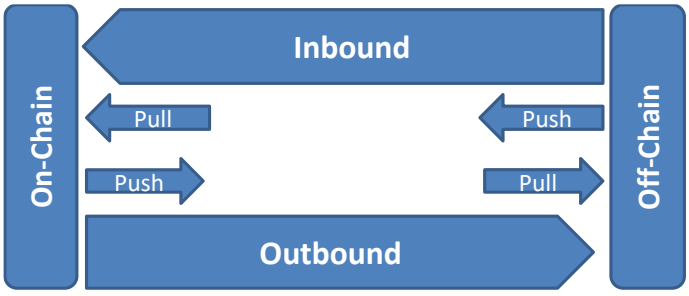

Fig. 2. Oracle data flow patterns adapted from Mühlberger, et al [32]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

The peer reviewed evidence is indeed instructive enough to support the DISC hypothesis, and justifies the need for designing our own research to test the hypothesis in a real-world use case setting. The study we designed is presented herein.

(a) Testing the DISC Hypothesis

While we were formulating and finding support in literature for our hypothesis, we had an ongoing EU funded project (Horizon 2020 Program) – XENO [33], which required BC deployment for securing, anonymizing and fiscally rewarding crowdsourced first responder (FR) peers who rescue a person / woman in distress, by means of an alert triggered via a wearable IoT device worn by the victim as a fashion accessory. Such crowdsourced Good Samaritans would be recruited from the crowd-worker (gig-worker) community that include mobile gig workers who engage in ride hailing, food delivery, or some such services, and are always available in real time in the vicinity of the victim in need of help. Accumulated evidence indicates that ride hailing service, Uber, reached victim faster than an ambulance in metro cities such as New York [34] & San Francisco [35] clocking 2.42 and 3.2 minutes respectively for Uber, and 6.2 and 7.49 minutes respectively for ambulance. With the rapid proliferation of these gig worker-based services the mobility and accessibility of the gig workers is getting even better.

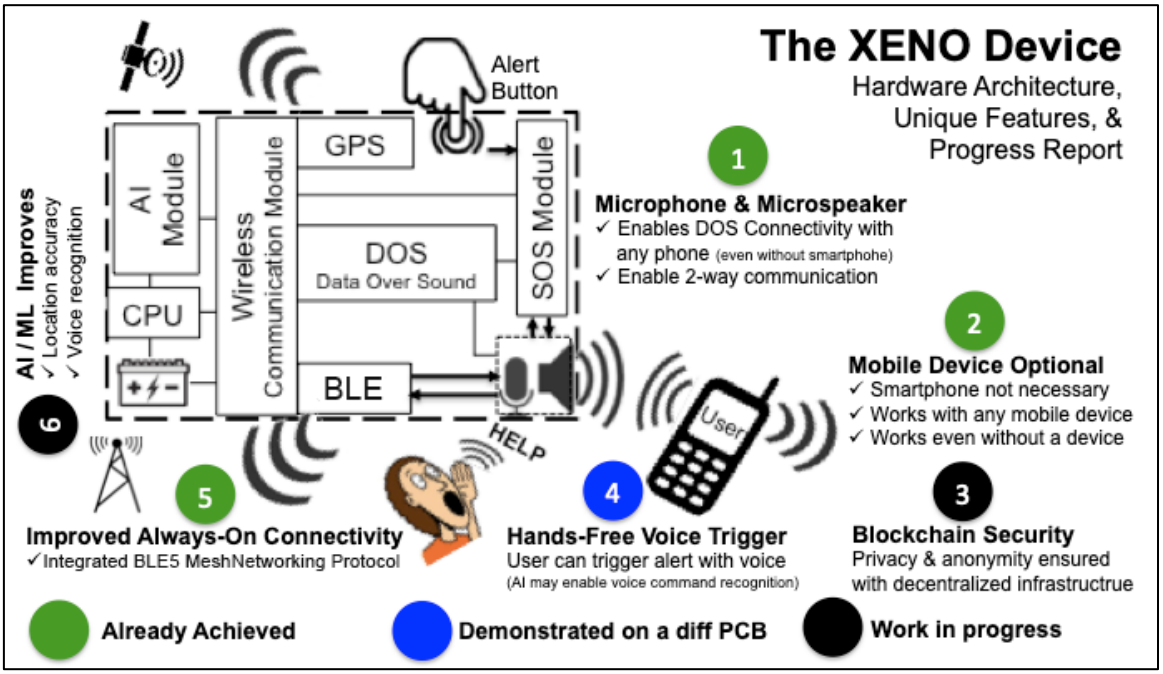

Fig. 3. The original XENO Network Architecture.

The XENO project was implemented at the W-ILAB.T testbed[1](IDLab-imec-UGent, Ghent, Belgium) in two stages funded by Fed4Fire+ project (EC grants). During the first stage the last mile communication problem was solved by implementing and testing the BLE5 mesh networking protocol. The second stage built and tested privacy & anonymity of a victim in distress via a novel decentralized P2P network that ensured an appropriate financial reward to a closest rescuer crowdsourced from the gig worker community (such as ride hailing drivers & food deliverers). Since, this paper explicitly pertains to blockchain's immutable smart contract and testing the DISC hypothesis to make them dynamic, experimental details are limited to blockchain deployment part of the project.

The XENO project basically anonymously crowdsources these gig workers as FRs to speed up help to a victim of sexual abuse or assault (although women's safety is the primary indication XENO device was originally invented for, it can be used in any distress setting). XENO is a wearable device camouflaged as a women's fashion accessory that can potentially save a woman in distress in the shortest possible time, and do it anonymously. Privacy and anonymity are a paramount consideration in designing XENO. Women in some cultures consider it a taboo to disclose their sexual abuse experiences to a third person, or even share it with their own family members. Therefore, many such cases remain unreported.

[1] W-ILAB.T testbed - https://idlab.technology/infrastructure/

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

The term Xeno has its origin in Greek, meaning stranger. Xeno is all about building a community of good strangers that can be instantly mobilized to help a distressed stranger (victim woman) from a bad stranger (perpetrator). XENO decentralised IoT technology is novel in three distinct ways. **Firstly**, it secures privacy and anonymity of the victim as well as victim's rescuer. **Secondly**, crowdsourcing the rescuers from gig workers makes the first responders more omnipresent within the immediate vicinity of the victim thereby speeding up the rescue process. **Thirdly**, it incentivizes the participation of the peers with rewards. We deployed BC technology to enable such a decentralized network of peers (strangers), not only boosting the speed of the rescue, but making the solution highly secure, private and even anonymous at the preference of the participants. Thus, the device justifies its name – **XENO**, the stranger, and its tagline – The Personal Crowdsourced Bodyguard [36].

XENO device consists of a hands-free voice trigger and voice recognition AI/ML module that can be prompted to work with just a voice command. XENO uses a network of anonymised peers (gig workers) to be the First Responders (FR) responding to such mishaps. The device is blockchained to ensure privacy & anonymity of the victim as well as the FRs using a novel decentralised P2P network of stakeholders. The main objective of our Horizon 2020-funded XENO project was to build the backend architecture of the XENO platform based on BC technology. Our experiment goal was to develop and test a decentralised P2P network and a SC working in tandem with the XENO hardware, and provide API that connected the XENO network to a third-party gig-working app. The decentralised XENO network ensured the user's privacy and anonymity while incorporating a financial incentive system to automatically reward FR gig workers for their rescue activity. The financial reward to the crowdsourced FR was secured via a self-executing SC. The identities of both the FR/rescuer as well as the victim were kept confidential and secure on the BC. Yet the FR/rescuer was rewarded handsomely for his/her efforts without involving any third-party mediator. For the privacy, security and anonymity of the entire incident handling process, including the gig worker FR/rescuer's financial reward, a SC was designed for deployment. In the production grade XENO framework, the reward would be generated by BC's cryptocurrency mining protocol, but since we neither had a custom BC specially designed for XENO, nor an active alliance with any gig-worker app at the time of developing and testing the XENO ecosystem, we had to simulate a setting wherein the rewards to the rescuer was sponsored by patrons. But the problem was these rewards would vary depending on geographical location, incident circumstances and the quantum of funds sponsored by the patrons. This created a situation where immutability of smart contract would not permit to accommodate the real-life circumstances in each unique incident with variable quantum of rewards. And, moreover the FR/rescuer had to know upfront the quantum of incentive at stake that the XENO SC will guarantee for undertaking the rescue. It had to be guaranteed, and had to be significantly more than the fare or delivery commission that his/her gig work provides for the same amount of time. For example, a reward of €1,000 for responding to a destress alert would be more than a week of gig worker's earnings, and an attractive incentive to take up a humanitarian cause. This real-world situation offered us an opportunity to design a dynamic SC framework and test our DISC hypothesis.

For the purpose of illustrating the decentralised XENO ecosystem following stakeholders are relevant:

1. XENO Device User / Victim: The one who initiates the SOS alert and validates the successful addressal of the event. The reward will only be transferred to the rescuer after the final approval from the victim (by conveying a 4-digit unique incident OTP to the rescuer, set by the user at the time of registration)**.**

2. First Responder (FR) / Rescuer: The gig worker who is registered on any third party crowdwork application (linked to XENO application via API).

3. Patron: The one who contributes to the XENO ecosystem by sponsoring financial rewards for incentivizing the rescuers (in production grade XENO the rewards will be automatically generated via BC's mining rewards).

The XENO Process Flow

XENO wearable device works in conjunction with a companion mobile application that receives the SOS signal and broadcasts it to the nearby gig workers, registered on the any third party crowdwork application like Uber, connected to the XENO network via API. Every XENO user, while registering on the XENO mobile application is assigned a unique SSI (Self-Sovereign Identity) registered on our XENO decentralised network to ensure the privacy and anonymity, and is required to set up a unique PIN which is recorded in an encrypted form. The PIN is mandatory to complete the transaction once the event is claimed to be addressed by the rescuing peer. The gig worker, FR/rescuer registered on any third-party application (connected to XENO application via APIs) is asked to create a personal wallet on XENO network on signup. The BC deployed to create the SSI and the wallet is Matic

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

Network Network – a BC scaling sidechain solution provider [37]. The XENO reward tokens are delivered to this wallet after successful completion of the rescue and authentication by the victim. The XENO rewards wallet holds the funds assigned for the next rescue and are contributed by the patrons via the rewards pool. The high-level architecture and process flow for implementing DISC in XENO ecosystem is illustrated in Fig. 4.

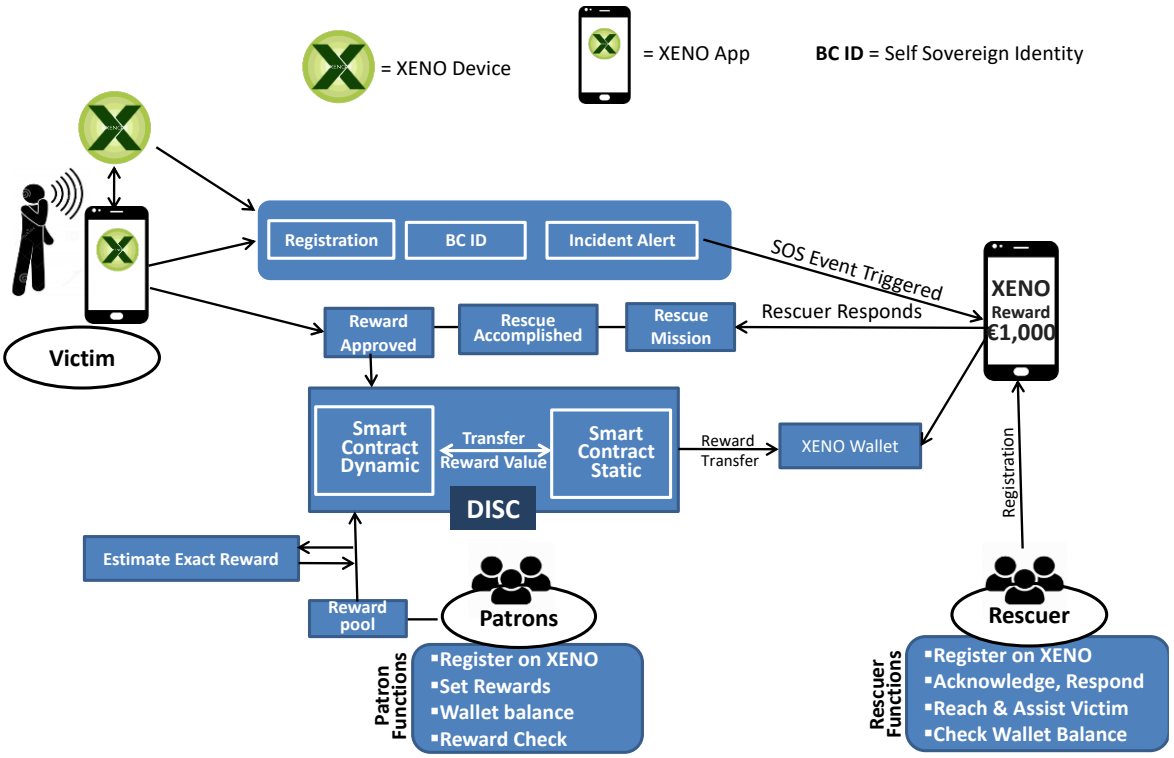

Fig. 4. XENO Device Decentralization Architecture & DISC Implementation

For introducing dynamism of estimation and delivery of the reward in real time as financial incentive for rescuing a victim in distress, we created a DISC strategy that relied on a pair of SCs on the Matic Network [37]. One of the two SCs was the base or the parent SC, and the other was the satellite or child SC, which we address in this experiment as Static SC (SSC) and Dynamic SC (DSC) respectively. The SSC was coded as a conventional SC, which calls the DSC for execution. The DSC was coded to take a dynamic feed from a designated XENO reward pool wallet funded by funds sponsored by patrons. The XENO reward wallet funds vary according to the circumstances of the incident. When victim triggers the distress alert, the quantum of reward offered for the rescue is displayed on the FR/ rescuer's device along with the incident alert. The logic we apply basically ensures that the FR/rescuer knows his / her variable reward value upfront before initiating the rescue. On triggering the alert, the SSC calls the DSC to execute and consummate the contract and deliver the funds to the FR wallet once the victim approves the reward. Thus, the FR receives the guaranteed reward automatically as soon as the rescue operation is completed and authenticated by the victim, without any third-party intervention. Thus, the DISC protocol injects real world flexibility to the XENO smart contract while retaining its immutability.

Since the FR/rescuer is informed of the exact amount of reward before he/she undertakes the rescue operation there is no need for external oracles in this case. Thus, XENO is a very simplistic implementation of the DISC concept wherein the smart contract retains immutability, and yet flexible to accommodate rewards that vary according to the demand of the circumstances. Although devoid of dynamic complexities that most real-world transactions would entail, and far removed from the urgent needs of the primary driver of this research -DeFi, the results are instructive and sufficient to test the DISC hypothesis.

DISC & GDPR Compliance

A section of legal experts believes that the SCs are in conflict with GDPR, which mandates data subject's right to forget [38]. However, their concerns are partly misplaced, because with any BC implementation the personal data is

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 May 2021 doi:10.20944/preprints202105.0028.v1

no more controlled by any third-party data controller. In fact, blockchain basically transcends the concept of *"data subject,"* to *"data owner,"* making the data controller redundant as the personal data at all times remains in full control of the data owner. In any BC implementation, the third party never controls the citizen data, but uses it only for the time and for the purpose that data owner authorizes. Hence, there's never a question of third party forgetting the data. Nevertheless, the data owners may not want to keep their personal data on the BC forever, and would want to exercise their right to erase the data. Hypothetically, the DISC protocol can make that possible if at all there remains any perceived conflict between GDPR and BC/SC.

Future Plans: Making Smart Contracts Smarter with AI

We're excited about the results of our research to date, but we're not done yet. The approach we used in the XENO experiment is very simplistic implementation of the DISC concept, and may not apply in many more complex scenarios. Although sufficient to test the hypothesis, we need more robust approach to prove the hypothesis so that it wins mainstream applicability. The dynamic parameters feeding the SC have to be more trusted than the third-party Oracles. Oracles will always be prone to comprising the immutability of SCs. If the DISC concept has to work in all and sundry transactional environments, the dynamic feed to the DISC has to be algorithmically secured. This will entail integrating sophisticated AI agents to feed the algorithmically controlled dynamic parameters to DISC via machine learning models. And, perhaps eternally securing these algorithms by wrapping them with homomorphic encryption techniques [39]. Streamlining these processes will go a long way in enhancing the practicality of this approach for widespread use.

Several experiments are on our drawing board to prove the DISC hypothesis in several complex real-world scenarios. One of them addresses an urgent need of the biggest potential beneficiary of DISC by volume of assets staked - DeFi industry. The rise of Decentralised Finance (DeFi) has not only brought a newfound wave of innovation to the broader BC ecosystem, but also the opportunity for savvy investors to generate staggering returns. The exponentially growing DeFi industry has exploded to a $50+ billion behemoth from just over a billion in previous 9 months [16]. Much of this growth is attributed to liquidity mining using automated market makers (AMM). AMMs have several shortcomings, most lethal of them being SC-triggered unstoppable trading of assets even if the trades are making losses. Current AMMs are therefore bound to crash if the current bull market slows down. A specifically designed DISC implementation for intelligent market making (IMM) customized for individual trader's risk-taking appetite is currently in works in our labs as liquidity providing SC. Our initial research suggests, that our DISC strategy will be intelligent enough to minimize trading losses that current generation AMMs are prone to in less than bullish markets. Such DISC powered IMM will make DeFi more profitable in the short term, and more sustainable in the long term.

Conclusion

SCs have too many external dependencies that limit their utility in almost all use cases beyond digital bearer instruments on decentralised platforms like bitcoin [11] and countless other cryptocurrencies. Surprisingly, such a serious show-stopping limitation of BC's real world deployability is not even on the radar screen of BC community who are exclusively focused on solving BC's scalability trilemma [40]. Scalability can be solved sooner or later, but the mainstreaming of BC cannot move forward unless the BC paradox is resolved. The DISC hypothesis strives to change that by providing ample evidence to support and test the DISC hypothesis. Proving the hypothesis in diverse real-world scenarios will be crucial in making SCs more real world friendly and sustainable. Until DISC becomes a robust technological reality, we chose to interpret the results with caution, merely as our baby steps towards resolving the BC's most stubborn paradox, and eventually making BC suitable for real world use cases. Finally, the technological challenges around BC immutability — and the opportunities it presents — are too big for any one entity to take on. We solicit support and cooperation of BC stakeholders across all domains, and look forward to positively impacting the global BC landscape.

Competing Interests:
None declared.

Author's contribution:

FR designed and coordinated this research and prepared the manuscript in entirety.

Funding:

This work was partly supported by a sub-grant under the Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020), Call: H2020-ICT-2016-2017, Topic: ICT-13-2016 for the implementation of the project entitled "*Federation for FIRE Plus*" pursuant to grant agreement ID: 732638. The stage 1 grant experiment was successfully completed, and stage 2 experiments are ongoing. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies. We also acknowledge the support and cooperation of Matic Network for making available their online resources for designing and implementing our smart contract experiments.

Conflict of Interest:
None declared

References:

[1] Nakamoto, S. "Bitcoin: A peer-to-peer electronic cash system," *Bitcoin.org*, 2008. Available online: https://bitcoin.org/bitcoin.pdf. (accessed on 19-Feb-2021).

[2] Taskinsoy, J. Bitcoin Nation: The World's New 17th Largest Economy (February 28, 2021). Available online SSRN: https://ssrn.com/abstract=3794634 or http://dx.doi.org/10.2139/ssrn.3794634

[3] Emma Newburger. Bitcoin surpasses $60,000 in record high as rally accelerates. *CNBC.com Markets, 2021*. Available online: https://www.cnbc.com/2021/03/13/bitcoin-surpasses-60000-in-record-high-as-rally-accelerates-.html (accessed on 19 March 2021).

[4] Buterin, V. "ethereum/wiki." *GitHub*. 2013. [Online] Available at: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 19 February 2021).

[5] Alexander Savelyev. Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, Information & Communications Technology Law, 26:2, 116-134, 2017
DOI: 10.1080/13600834.2017.1301036

[6] McCombs, I. Change Is The Only Constant - VMware Careers. 2020. [Online] *VMware Careers*. Available online: https://blogs.vmware.com/careers/2020/07/change-is-the-only-constant.html (accessed on 19 February 2021).

[7] PwC, 2020. "Time for trust: The trillion dollar reasons to rethink blockchain." [online] *PwC*. Available online: https://www.pwc.com/hu/en/kiadvanyok/assets/pdf/Time_for_Trust_The trillion-dollar_reasons_to_rethink_blockchain.pdf (accessed on 19 February 2021).

[8] Subramanian, S. "Crypto is now the world's fifth-most circulated currency by value," *Quartz*, 2021. Available online: https://qz.com/1954555/all-the-worlds-crypto-is-now-worth-more-than-1-trillion/. (accessed on 20-Feb-2021).

[9] Lehdonvirta, V. "The blockchain paradox: Why distributed ledger technologies may do little to transform the economy," *Oxford Internet Institute*, 2016. Available online: http://www.oii.ox.ac.uk/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/. (Accessed on 19 March 2021).

[10] Guarín Duque, G. and Zuluaga Torres J.D. "Enhancing E-Commerce through Blockchain (DLTs): The Regulatory Paradox for Digital Governance," *Global Jurist*, vol. 20, no. 2, 2020.

[11] Song, J. "The Truth about Smart Contracts," *Medium*, 15-Jun-2018. Available online: https://jimmysong.medium.com/the-truth-about-smart-contracts-ae825271811f. (accessed: 02 March 2021).

[12] Frederik, J. "Blockchain, the amazing solution for almost nothing," *The Correspondent*, 21-Aug-2020. Available online: https://thecorrespondent.com/655/blockchain-the-amazing-solution-for-almost-nothing/86649455475-f933fe63. (accessed on 20 February 2021).

[13] Jeffries, A. "'Blockchain' is meaningless," *The Verge*, 07-Mar-2018. Available: https://www.theverge.com/2018/3/7/17091766/blockchain-bitoin-ethereum-cryptocurrency-meaning. (accessed: 20 February 2021).

[14] Zile, K and Strazdiņa, R. "Blockchain Use Cases and Their Feasibility," *Applied Computer Systems*, vol. 23, no. 1, pp. 12–20, 2018.

[15] Mohanta, B.K.; Panda, S.S. and Jena, D. "An Overview of Smart Contract and Use Cases in Blockchain Technology," *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2018.

[16] DeFi, "DeFi Pulse: The DeFi Leaderboard: Stats, Charts and Guides," *DeFi*, 2021. Available online: https://defipulse.com/. (accessed on 19 February 2021).

[17] Monte, G.D.; Pennino, D. and Pizzonia, M. "Scaling blockchains without giving up decentralization and security," *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2020.

[18] Blocktivity, *blocktivity*, 2021. Available online: https://blocktivity.info/. (accessed on 20 February 2021).

[19] Benshahar A. "Why EOS DApps Are Dangerously Dependent on Just Five Nodes?." CryptoPotato.com. 2019. Available online: https://cryptopotato.com/why-eos-dapps-are-dangerously-dependent-on-just-five-nodes/?amp (accessed 19 February 2021).

[20] Hurun.net. 2021. "*The Hurun Global Unicorn List*." [online] Available online: https://www.hurun.net/en-US/Rank/HsRankDetails?num=WE53FEER (accessed 19 February 2021).

[21] AngelList, "Blockchains Startups | AngelList," *AngelList*, 2021. [Online]. Available online: https://angel.co/blockchains. [accessed on 01 March 2021).

[22] Kosba, A.; Miller, A.; Shi, E.; Wen, Z. and Papamanthou, C. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

[23] Hofmann, F.; Wurster, S.; Ron, E. and Bohmecke-Schwafert, M. "The immutability concept of blockchains and benefits of early standardization," *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, 2017.

[24] DrFazal, "Resolving the Blockchain Paradox: The DISC Hypothesis," *Medium*, 21-Jan-2021. Available online: https://drfazal.medium.com/resolving-the-blockchain-paradox-the-disc-hypothesis-de4f44148f09. (accessed on 20 February 2021).

[25] Wohrer, M. and Zdun, U. "Design Patterns for Smart Contracts in the Ethereum Ecosystem," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018.

[26] Imeri, A.; Lamont, J.; Agoulmine, N. and Khadraoui, D. Model of Dynamic Smart Contract for permissioned Blockchains. In *Proceedings of the Practice of Enterprise Modelling 2019 Conference Forum, Luxembourg*, 2019.

[27] Xu, X.; Weber, I.M. and Staples, M. "Blockchain Patterns," in *Architecture for block chain applications*, Cham, Switzerland: Springer, 2019.

[28] Mendling, J.; Weber, I.; van der Aalst, W.M.P. et al.: "Blockchains for business process management -

challenges and opportunities.*" ACM Trans. Management Inf. Syst.* 9(1), 4:1–4:16, 2018

[29] Xu, X.; Pautasso, C.; Zhu, L.; Lu, Q. and Weber, I. "A pattern collection for blockchain-based applications." in *EuroPLoP*. pp. 3:1–3:20. ACM, 2018.

[30] Harper, C. "What is ChainLink? A Beginner's Guide to Decentralised Oracles," *CoinCentral*, 04-Apr-2018. Available online: https://coincentral.com/what-is-chainlink-a-beginners-guide-to-decentralised-oracles/. (accessed on 20 February 2021).

[31] Caldarelli, G. "Understanding the Blockchain Oracle Problem: A Call for Action," *Information*, vol. 11, no. 11, p. 509, 2020.

[32] Mühlberger, R.; Bachhofner, S. Castelló Ferrer, E.; Di Ciccio, C.; Weber, I.; Wöhrer, M. and Zdun, U. "Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World," *Lecture Notes in Business Information Processing*, pp. 35–51, 2020.

[33] Alarcon, M. "XENO," *FED4FIRE+*, 06-Nov-2020. Available online: https://www.fed4fire.eu/demo-stories/cc/xeno/. (accessed on 20 February 2021).

[34] Pham, S. "Is Uber Really Faster than an Ambulance?," *NBC Bay Area*, 14-Apr-2015. Available online: https://www.nbcbayarea.com/news/local/is-uber-really-faster-than-an-ambulance/119386/. (accessed on 20 February 2021).

[35] Howard, K. "Ambulance Working Group Conclusion," Office of the Mayor, Memorandum to Mayor Lee, 23-Feb-2015. Available online https://sf-fire.org/sites/default/files/FileCenter/Documents/3896-EMS%20Progress%20Memo%202.23.15.pdf. (accessed on 20 February 2021).

[36] "World's First Crowdsourced Bodyguard," *MyXeno*. Available online: https://www.myxeno.org/. (accessed on 24 February 2021).

[37] "Scalable and instant blockchain transactions," *Matic Network*. Available online: https://matic.network/. (accessed on 20 February 2021).

[38] Riva G.M. "What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights," *Frontiers in Blockchain*, vol. 3, 2020.

[39] Bowditch, W.; Abramson, W.; Buchanan, W.; Pitropakis, N. and Hall A. "Privacy-preserving Surveillance Methods using Homomorphic Encryption," *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, 2020.

[40] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.