Building an Inclusive Distributed Ledger System

Cynthia Dookie
Banking Technology Contractor
Princes Town, 851130, Trinidad and Tobago
cynthiadookie@gmail.com

***Abstract*—In 2008, bitcoin disrupted the transactional ecosystem with its value propositions. However, sustaining autonomous, deregulated systems in markets filled with laws and regulations has had its challenges. There are also open questions of scalability, resilience, availability, speed and finality of transactions. Sound technical components have emerged but we need to take this one step further and integrate the units to provide an accepted packaged solution. Using a game application as an entry point, we propose a simple, inclusive asset transfer system which will stimulate adoption and create traction in the distributed ledger universe.**

***Index Terms*—blockchain, biodata, scaling, ancestral node**

I. Introduction

Moving the distributed ledger system, (DLS), into mainstream requires a catalyst. We therefore need to widen the consensus pool away from techies and increase usability with a compelling, front end application coupled with a proven consensus protocol. We further believe that creation of new assets in the mining process further inhibits inclusiveness across various sectors and crypto assets should not be used as rewards or fees. Randomly generated cryptic keys give anonymity and secure transactions or outputs. However the need to store these keys on accessible devices and pieces of paper pose a security risk which also hinders inclusivity. In order to maintain a network's resilience, we need to maintain a sustainable size that matches the available storage space both at the core and at the personal space of its participants. Simple size maintenance algorithms must be part of the DLS's core processes. In addition, reduction of fees required in executing contracts compels a more attractive and inclusive peer to peer transfer system.

II. Components of Our Proposed DLS

Reengineering existing DLS components can be the solution for enabling an inclusive DLS. Our approach is to modify and integrate existing processes from diverse sources to create a scalable DLS solution with an improved delivery system, increased token security, and one that allows parameterization.

A. GPS Enabled Game Application as an Access Node

Participation builds an inclusive community. A TechCrunch report [1], states that games are played by almost every demographic stratum of society and gamers are a third of the world's population. A gaming application is therefore the perfect vehicle to be used as a building block to our inclusive DLS. We therefore propose the development of a high-entropy GPS or augmented reality game like Pokémon Go, which will be bootstrapped to the node of the DLS. The consensus mechanism will form part of the game's objectives and the DLS node setup and core services' algorithms will be reengineered and integrated into the game's backbone so that it appears seamless to the gamer. As rewards, gamers will form the pool from which validators and committee members are chosen to participate in the consensus mechanism and add blocks.

B. An Ancestral Node to Seed Credentials

We propose a structure with an ancestral node which spawns child nodes, (bootstrapped to the game), linked to permissionless DLS. Registration on the ancestral node is via the game application after which a spawned child node is back linked to the DLS. Transfer of assets can only be made by ancestral node registrants. Gamers who are non asset owners can choose not to register and retain connection only to the DLS thus creating an expanded inclusive peer community.

C. Keys Generated from Biodata

Jagadeesan and Duraiswamy in their paper, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris [2]," claims that they have an efficient approach for the secure key generation on the basis of multiple modalities like, Iris and fingerprint. Minutiae points and iris texture are then fused by processes of concatenation, shuffling and merging to build the multimodal biometric template. This template is then used to generate the required secure 256 bit cryptographic key. We can use this cryptographic key to generate a public key used to sign outputs. For accounts where there are multiple signatories to the token, one public key can be associated to multiple private keys as suggested by Nayak, Ashok and Awasthi in their paper, "Multiple Private Keys with NTRU Cryptosystem [3]," thus creating a more inclusive DLS.

D. Tailored References of Outputs

Movement of assets is represented by outputs or change of state which are defined by its attributes. By tailoring the reference of these attributes, we can offer generality of code that is parameter driven allowing extensibility towards a more autonomous and inclusive structure instead of smart contracts with superfluous strings and fees for execution. For each asset type, we can parameterize its unit, type and restrictions.

E. Grouping of Blocks for Pruning and Size Maintenance

Creating a system to completely remove and archive the oldest blocks without disrupting the immutability of the chain

978-1-7281-5143-4/20/$31.00 © 2020 IEEE

SANER 2020, London, ON, Canada
LBI Track

can solve the scalability issue. We propose a system structured into groups where each new group starts with blocks containing unspent outputs transferred from the oldest blocks. These transactions are broadcasted and verified as other outputs. Total number of blocks in a DLS is predetermined and should reflect a manageable size, thus creating an inclusive structure suited for both small and large entities. Equation (1) determines the optimal number of blocks, (x), where (t) is the anticipated outputs per day using an estimation of five hundred outputs per block and the maintenance of a ninety day output history.

$$x= ((t/500)*90) \quad (1)$$

Equation (2) determines the number of blocks (y) to be grouped together for an optimal number of blocks (x). We give a hundred groups as a manageable structure.

$$y= ((ceiling(x, 1000)/100) \quad (2)$$

Equation (3) determines the number of blocks (c) to be read and consolidated at each instance for a given group size (y).

$$c= (y/2) \quad (3)$$

Pruning does not coincide with grouping and should be delayed for at least two cycles. Automated scripts will create new groups not interrupting the continuous processes. Archived ledgers set to read only and encrypted with the signatures of the owners of the brought forward outputs should be available on demand. Nodes can decide whether to store these ledgers on or off the network. Please note that this process will only work if the DLS is for peer to peer movement of assets not hoarding.

F. The Byzantine Agreement as the Consensus Protocol

Taking advantage of Algorand [4] strong byzantine agreement, we integrate this consensus protocol into our game software. The gamers will provide a pool for Algorand's cryptographic sortition [5] from which committee members, leaders and validators are chosen. These roles must appear as roles in the game. Jing Chen and Silvio Micali in their paper, "Algorand [5]," explain that their nonce is a certificate made up of both a long term and an ephemeral key of the consensus team. As the long term key, we use the built in encryption of the game bootstrapping process and the ephemeral key is produced by a random generator seeded with two sources of entropy collected during the game as paths and images change. Halpin and Naor [6], suggests that the competitive nature of a game makes humans act more randomly which can be a source for randomness for cryptographic purpose.

G. Participation Rewards

With Algorand's [4] message passing byzantine agreement, there is no need for miners. However it is necessary to provide incentives and rewards so that gamers will strive to participate in the consensus. Reward points to assist in enhancing the gaming experience or coupons, discounts and products from financial sponsors can be offered. In addition, with our GPS enabled game, we can offer geolocation advertising to generate income.

III. Beyond The "Green Screen"

Although there are many APIs available to assist in creating a client node on your personal device, setup instructions are more suitable to programmers than to the everyday tablet user. Even adding smart contracts to your blockchain requires some programming. We propose to take this system beyond the "green screen" and move it to mainstream with our game design approach. This ambitious approach offers innovation with its client services deployment as well as the removal of the dependency to dwindling cryptocurrency reserves as is being experienced by other DLSs.

IV. A Practical Application

Our proposed DLS is better suited for fostering a cashless society with its potential for mass adoption and inclusion than other DLSs which are encumbered by mining of crypto assets, fees and mining pool cartels. This application is suitable for Central Banks who through the ancestral node can act as a bureau de change to convert tokens to and from fiat currencies and run compliance and identity checks to thwart money laundering and terrorist financing. Once tokens are recorded in the permissionless DLS, they are as good as cash and can be transferred within the network without monitoring, transfer fees and settlement delays.

V. Conclusion

We have introduced game-playing as an incentive to stimulate participation and expand the consensus pool. By integrating Algorand [4] consensus protocol, we can provide secure, instantaneous outputs. We have proposed keys generated from biodata and a system of maintaining optimal size without compromising the immutability of the links. We have suggested parameterizing our outputs scripts in an attempt to make peer to peer transfer in a trustless environment feeless. With these components, we believe we can build a new, inclusive distributed ledger system suited for either small or large public or private enterprises.

References

[1] Omer Kaplan, "Mobile gaming is a $68.5 billion global business and investors are buying in", August 22, 2019, pp 2 [Online]: https://techcrunch.com/2019/08/22/mobile-gaming-mints-money/

[2] A. Jagadeesan, Dr. K. Duraiswamy, "Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris", International Journal of Computer Science and Information Security, vol 7, No 2, February 2010

[3] Rakesh Nayak, Ashok Kumar Nanda and Lalit Kumar Awasthi, "Multiple Private Keys with NTRU Cryptosystem", International Journal of Research in Computer and Communication Technology, Vol 4, Issue 3, March -2015

[4] Jing Chen, Sergey Gorbunov, Silvio Micali and Georgios Vlachos, "Algorand Agreement Superfast and partition resilient byzantine agreement", April 25, 2018, [Online]: https://eprint.iacr.org/2018/377.pdf

[5] Jing Chen, Silvio Micali, "Algorand Theoretical Paper" May 2017, pp 4-13, [Online]: https://arxiv.org/abs/1607.01341

[6] Ran Halprin , Moni Naor, "Games for extracting randomness", Proceedings of the 5th Symposium on Usable Privacy and Security, July 15-17, 2009, pp 10, Mountain View, California, USA, [Online]: http//doi.acm.org/10.1145/1572532.1572548