PART 1 - Vera - the Solution

1. Introduction

a. Overview

For the UNWID 2022 Hackathon, our team decided to approach the second challenge – Blockchain for Good. We have aligned our solution to address sustainable development goal #9 as we propose to use blockchain technology to build resilient public service infrastructures and foster innovation. As we will explore later, we believe our solution can eventually cover a majority, if not all, of the UN's goals. This document serves to provide an overview of Vera from both a technical and business perspective.

Our solution is Vera Protocol, a secure digital fabric for smart city living and modern digital needs. It is a blockchain protocol that will allow ubiquitous access to real life functionality and data by bringing public service infrastructures together into one platform tailored to each city's unique needs. As part of our submission, we have created a prototype website and dApp to showcase our solution. We have developed three features for the dApp, including sending requests for information, receiving requests and deciding on them, and checking metadata associated with a user's account. We have used IPFS to host our frontend, deployed the smart-contract to the Polygon Testnet blockchain, and include a list of other tools and resources used in the development of our MVP at the end of this document. Our use of both IPFS and Polygon is evidenced in the FAQ section of our website.

b. MVP and proposed solution

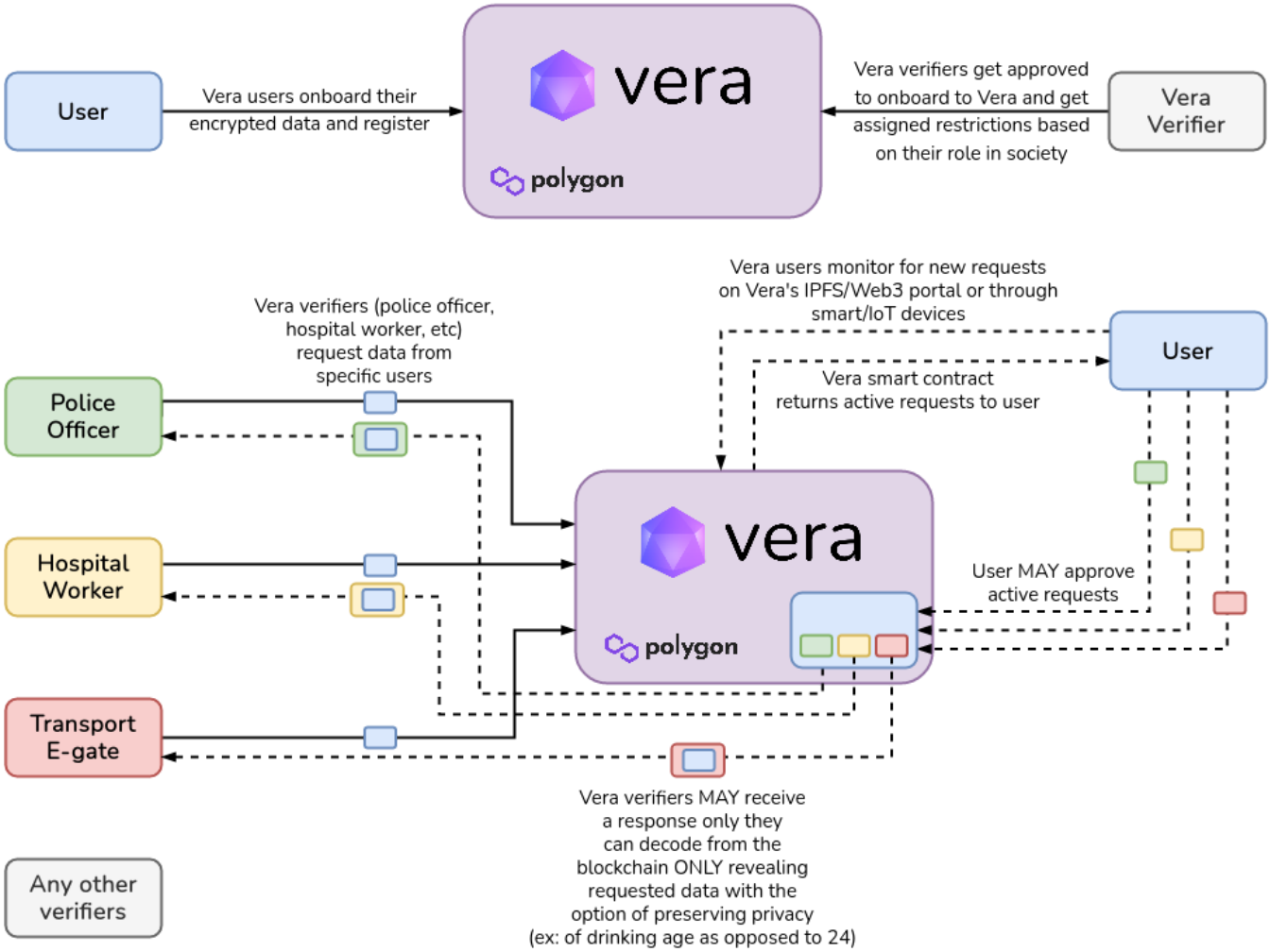
The Vera contract serves to be a rather simplified illustration of how sensitive data of day-to-day citizens in modern cities can be stored on the blockchain with no privacy leaks. By hosting it on an efficient L2 Ethereum-Virtual-Machine such as the Polygon Network, it is also important to highlight that such a solution is exceptionally fast, cheap, and easy to use, especially with the advent of 5G and modern devices making the internet a practically ubiquitous utility. As such, a smart contract akin to Vera will be all but universally accessible in the future at lightning speeds from nearly all devices.

Registered government officials, police and federal officers, paramedics, cashiers, bankers, insurance agents, pharmacists, security guards, utility company agents, transport officers, taxation officers, amongst countless of myriad other occupations will leverage a contract such as Vera to its full power by being able to query whether users' data on-chain matches their expectations. For example, this can be a taxation officer ensuring that all outstanding taxes of a citizen are paid, or a pharmacist ensuring that the script for medicine is legitimate, or even toll gates querying a smart device for a

user balance in terms of metro credits, amongst a sea of other potential applications. At each step of the way, data will always be encrypted, with only the results of the required checks, should the requestor have the permissions to access such data, returned to the requestor in encrypted form they can verify if the user chooses to submit the verification to the blockchain.

We are aware of a small number of simplifications that result in privacy leaks in our prototype, however we would like to highlight that ZKP solutions such as those available on the Polygon Network, albeit immensely complex, can render such a vision into reality - those were avoided due to their immense sophistication and time constraints. We would also like to highlight that by hosting the Vera front-end portal through IPFS, Vera's uptime and attacks such as DNS cache poisoning, amongst countless others such as DDoS attacks become more or less futile. Lastly, we would like to note that we have explicitly referenced a good amount of data by the users' addresses in plaintext, but this could have easily been obfuscated to be in encrypted form, which we have avoided doing for simplicity of understanding and for simplicity of use.

Please refer to the diagram of Vera's functionality below.



2. UN Sustainable Development Goals

Vera was conceptualized to implement distributed ledger technology (DLT) into existing government infrastructures by tailoring a blockchain specific to each city and its unique public services. Applied in this way, DLT can effectively address every sustainable development goal (SDG) that the UN has set out to accomplish. This has already been evidenced in the UNJIU's analysis of "DLT solutions for use cases for key challenges in the 17 SDGs" [1]. For the purposes of this submission, we will limit the discussion to Vera's ability to progress a specific handful of the UN's SDGs that are most achievable in its current conceptualized iteration.

In the context of reforming government infrastructure, SDG #9 (industry, innovation and infrastructure), and more specifically target 9.1, is progressed by a city's implementation of Vera. Cities today operate within an environment where its residents have low trust in the government, and yet maintain high expectations [2]. By transforming government infrastructures through the intergration of DLT, Vera can help governments revolutionize public service delivery and operations by making them more secure, efficient, flexible, and transparent. This is the overarching goal that Vera addresses, especially so as all utilities and services that stem from this protocol will innovate upon existing government infrastructure.

In pursuit of SDG #9, Vera will likely achieve progress in many other SDGs. All SDGs are linked to government policy and infrastructure in some way, and as such, Vera can effectively address every challenge to varying extents. Specifically, we will address SDGs that are covered by the use cases we discuss below. SDG #11 (sustainable cities and communities) will be progressed as DLT will enable a more sustainable public transport system to be implemented. By leveraging DLT, Vera will facilitate robust maintenance data management and more accessible universal payment and ticketing systems. Additionally, SDG #16 (peace, justice and strong institutions) will be addressed with Vera's DLT implementation of secure government issued identification which will facilitate safe, secure, and fast identity checks, and in doing so, mitigate instances of corruption and fraud.

3. Use cases

Vera has the potential to implement a plethora of personalized utilities and services for host cities. We cannot meaningfully cover all potential use cases in this discussion. We will focus on public service sectors that we believe would see major benefits from integrating DLT, and those that are showcased in the Vera MVP. As such, below we will discuss a non-exhaustive list of use cases Vera will cover. It is important to emphasize that Vera can be implemented as an extensible system in the real world, to which any number of additional services can be attached.

a. Health system

Healthcare systems internationally deal with a similar issue – interoperability. By leveraging DLT, data stored on the blockchain could be universally accessible to specific individuals or organizations

that have the required authority. This would allow better, distributed, ubiquitous, and decentralized management of health records, offer health-care providers more informed decision-making, and increased accountability.

Gupta et al. has proposed an explanation as to how blockchain can be leveraged to enable a secure electronic health records exchange which places health consumers as the rightful owners of their data [3]. The proposed scenario would begin small-scale and involve only storing metadata of health and medical events on the blockchain so as to avoid initial scaling issues associated with supporting complete health records.

Vera's implementation would begin in a similar way as a step in that direction. The onboarding process for the healthcare component of Vera would involve both user and authorized institutions. The working solution would involve storing key metadata such as allergies, pharmacy scripts, insurance, blood type, and other relevant key information. After which, healthcare consumers and all of their future healthcare events would be stored on the blockchain. Because of Vera's zero-proof knowledge implementation, any and all requests for a Vera user's healthcare information would have to be authorized by the user, unless declared otherwise or the registered healthcare provider has the relevant authority. For instance, a user may approach a pharmacist with their IoT device linked to Vera and when prompted for their pharmacy script, the pharmacist could use their IoT device to query the user's authority to receive the medication.

This provides users with total ownership over their own data. Vera could eventually upgrade this component by leveraging smart-contracts to facilitate agreements between healthcare providers and patients.

b. Public transport

Mass transit and its operational success in each city is vital to the progress of sustainable cities and communities as an SDG. There are many applications of DLT in the context of public transport, but for Vera's current iteration, it would enhance the privacy of users and the maintenance data management of public transport systems. Clear issues with these two aspects have arisen internationally over the last few years. For instance, in 2017-2018, Rome's residents dealt with over 22 bus explosions because of electrical short-circuits [4], which could have been avoided if they had a more robust system for storing maintenance and usage records. In the context of privacy, Australia's public transport system in the state of Victoria leaked a dataset of 1.8bn historical records of users which exposed peoples touch on and off areas [5]. Bad actors were able to abuse this information so long as they knew at what time someone touched on and off.

Both instances could have been avoided by utilizing DLT. Vera's public transport component proposes to hold metadata relating to mass transit including, metro balance, service used, and where the service was used. Users would be able to access their city's metro ticketing system on all NFC, RFID, and IoT smart devices that support Vera. Vera utilizes a zero-proof knowledge system which makes it so that only public transport institutions would be capable of interacting with user data, this

type of access can never be changed once established because the blockchain is immutable. In addition to this, there is no single point of failure to shut down or penetrate the network.

The public transport component will also consist of a maintenance data management system for the operations of a city's public transport system. This would be a component only accessible to a certified government institution and as such will not be included in the Vera MVP. It would involve tracking maintenance and usage records, and automated alerts to all stake-holders of potential issues. As such, our implementation would offer legacy systems the opportunity to change into a more smooth and safe system by leveraging DLT.

c. Taxation

Taxation systems around the world may benefit with Vera as government tax systems move towards digitizing and assessing tax in real-time. A 2016 PwC study on the impact of implementing blockchain into government tax systems concluded that its application could reduce the administrative burden on the tax system and collect tax at a lower cost [6]. For the purposes of this discussion, we will limit it to Vera's implementation of Value-Added Tax (VAT) because, according to KPMG, there are over 140 countries in the world that implement this tax [7], and it would likely be a commonly utilized component in a government's integration of Vera. Despite this, it should be noted that Vera will have the functionality to allow users to view and pay their taxes, as well as access tax records and other taxation related documents.

Current VAT systems are reliant on businesses themselves calculating the amount of VAT they are due and submitting it to the taxation authorities. Taxation is heavily reliant on transaction dates because it is calculated over a fixed period as opposed to the actual transactions. Blockchain would be perfect in this context as each goods and services transaction could be linked to a user's wallet which would, just by the nature of DLT, automatically record the transaction, its type, and its timestamp. Having such a system whereby businesses and consumers alike effectively report on every VAT-eligible transaction automatically would help prevent taxation fraud. In the international context, it would allow non-governmental organizations and their constituent members to reliably disclose accurate VAT data as countries that implement Vera's solution would have similar transparent and secure records.

Vera's implementation would involve a fluid system between consumers, businesses and tax-entities. Metadata relating to all business and consumer transactions would be accessible to certified government institutions, and to those that are part of the transaction unless declared otherwise. Additionally, added functionality would enable users to link their commonly used payment methods to generate their tax reports based on the transactions they've made with them.

d. Law enforcement

Law enforcement stands to benefit from the use of DLT by developing effective, accountable, and transparent systems at all levels. There are a variety of adaptations that can be made to the many

issues current law enforcement entities face, from evidence mismanagement to renewing trust in police. For the purposes of this discussion, Vera will focus on its government issued identification proposal (which occurs during registration to Vera as a service) and its potential impact.

Vera and its law enforcement component will allow governments to issue identification documents as a set of integrated data stored within each user's Vera account in an NFT-like fashion which will be minted directly into a user's blockchain wallet. The account would contain metadata such as expiry dates, type of identification, renewal reminders, etc., all of which will be accessible to the user, and the institution that issued the identification. Anyone approaching the user for their identification would effectively have to query the blockchain and have the user authorize the request, otherwise they would not be able to access the user's identification. By utilizing zero-proof knowledge procedures in this way, the entire process is entirely encrypted, secure, private, and even quick because it would be as simple as an officer's IoT device interacting with the user's device. In doing so, we preserve the security and privacy of both people involved in the transaction. On a wider scale, this may prevent fraudulent attempts to steal users' private information and police misconduct.

PART 2 - Vera - the Business

4. Business

During our research we were unable to discover any protocols that propose a personalized blockchain protocol to each unique city and their public service infrastructure in the same way Vera does. We have found projects from the past, such as CityChain, that proposed similar ambitions but, for reasons we were unable to uncover, have ceased development. With this in mind, we believe if Vera was to be realized to its full potential, it would benefit from a first-mover advantage in the market.

Vera solves the issue of preserving privacy when it comes to personal information data for real life scenarios being stored in a digital form. The protocol maintains a minimum amount of exposure in this process by implementing a zero-knowledge proof procedure for accessing and revealing personal information, be it to users themselves or to authorized verifying parties. Around the world, governments and their public services infrastructure have the capability to meet modern standards of security, accessibility, transparency and privacy by leveraging DLT, and Vera would be a part of their progression to those standards.

The solution itself is a blockchain protocol making use of ZKP that is tailored to each individual city and its public services infrastructure. We envision an open-source proof-of-stake blockchain layer 2 solution akin to the Polygon Blockchain which allows Vera and other protocols to be built on top of it, as an ideal candidate for such a system. Vera will make use of the B2B model which will involve the Vera development team creating separate and individualized blockchain protocols for cities and

their public services infrastructure. This is where our company's primary revenue stream is derived as we would require governments to pay for the development of their blockchain protocol, and a licensing fee for continued use and support from our team for future integrations.

We define our primary customer segments below.

1) Developers and entrepreneurs

Developers and entrepreneurs are capable of building on top of the Vera blockchain protocol given our open-source nature. We would support protocols developing DLT solutions that align with our core product offering, values, and goals by creating an accelerator or incubator program in which these protocols would participate.

2) Governments & Privatized public services infrastructure

Governments will be able to engage Vera for a personalized blockchain protocol catering to their unique needs. Similarly, privatized public service infrastructures such as utilities and healthcare providers will be able to engage with Vera to implement DLT.

Given the large undertaking Vera would be to get up and running, scaling is an obvious issue, but not impossible to tackle. The organization will directly support protocols that are building alternative solutions to common public service infrastructures and systems, such as those we have outlined in the use cases section above. By partnering within Vera's development team, these projects can legitimize themselves over time, and their solutions may eventually be integrated with a B2B customer's individualized blockchain.

Our go-to-market strategy will broadly consist of both organic and paid distribution channels. In regards to organic channels, we will provide extensive support for our development community to promote building DLT solutions in line with our protocol. This will be accomplished by providing detailed, both technical and non-technical, documentation which will be iterated upon with user feedback, writing articles, consistent roadmap updates, high-level overviews of key concepts, actively seeking partnerships with protocols aligned with our unique value proposition, and step-by-step user guides. Our paid channels will be catered to the B2B model primarily as we will focus on spreading brand awareness to attract our main customer segment for this model. We may decide to engage people of influence, both established and up-and-coming, invest in experienced community managers, host community events with meaningful rewards, and potentially engage a blockchain marketing service to advertise our services internationally.

References:

[1] P. Dumitriu, S. Helck, E. Bricks, D. Dincic, R. Yu and S. Mueller, *Blockchain applications in the United Nations system: towards a state of readiness* Geneva: United Nations, 2020, pp. 62-64.

[2] C. Moore, B. Rainwater and E. Stahl, *Blockchain in Cities*, 1st ed. Washington, D.C.: National League of Cities, 2018, pp. 6-23.

[3] N. Gupta, A. Jha and P. Roy, *Adopting Blockchain Technology for Electronic Health Record Interoperability*. Cognizant Technology Solutions, 2016, pp. 1-10.

[4] A. Giuffrida, "Tenth bus explodes in Rome this year after 'short circuit'", *The Guardian*, 2018. [Online]. Available: https://www.theguardian.com/world/2018/may/09/bus-explodes-rome-historic-centre-italy-investigation. [Accessed: 01- May- 2022].

[5] G. Clark, "Myki data leak put privacy at risk: report - Government News", *Government News*, 2019. [Online].Available: https://www.governmentnews.com.au/myki-data-leak-put-privacy-at-risk-report/. [Accessed:01-May- 2022].

[6] M. Schofield et al., *How blockchain technology could improve the tax system*, 1st ed. London: PwC, 2016, pp. 1-4.

[7] K. International, "Indirect Tax Rates Table", *KPMG*, 2021. [Online]. Available: https://home.kpmg/xx/en/home/services/tax/tax-tools-and-resources/tax-rates-online/indirect-tax-rates-table.html. [Accessed: 01- May- 2022].

Tools:

IPFS-hosted frontend built with React.js, web3.js, and Metamask connectivity.

Solidity-based smart contract deployed on the Polygon testnet.

Blender for our logo prototype.

web3.storage & fleek.co for IPFS facilitation.