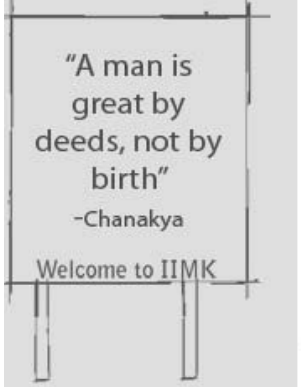

INDIAN INSTITUTE OF MANAGEMENT KOZHIKODE

Working Paper

IIMK/WPS/466/ITS/2021/07

June 2021

MPVIDS-SVB: Mobile Phone Virtual ID system based on smartphone volunteers' Blockchain

Lija Chandran T V[1]
Mohammed Shahid Abdulla[2]

[1]Independent Researcher, Information Technology and Systems, Email: lijachandran@gmail.com

[2]Associate Professor, Information Technology and Systems, Indian Institute of Management, Kozhikode, IIMK Campus PO, Kunnamangalam, Kozhikode, Kerala 673570, India; Email: shahid@iimk.ac.in, Phone Number (+91) 495 – 2809254

MPVIDS-SVB: Mobile Phone Virtual ID system based on smartphone volunteers' Blockchain

Abstract

Digital security threats to computers or smartphones exist in the form of viruses, spywares, or phishing/hacking activities. Smartphone devices, with knowledge of our mobile numbers, have thus become targets of cyber attacks and identity theft. Despite this risk, our personal mobile numbers are collected by many online and offline entities to grant us access to their services and amenities. We propose here a blockchain based solution which provides a virtual ID in lieu of a privacy-aware user's mobile number. This virtual-ID could then be used for typical services. The solution further consists of a decentralized Android app, blockchain nodes hosted on volunteers' smartphones which run Ethereum-style smart contracts for typical tasks on the system. Users begin by registering in the app to generate such a virtual ID for a period of their convenience. This proposal contributes to greater privacy awareness towards their IDs that consumers regularly trade-off in favour of behavioural analytics, marketing messages or worse.

1. Introduction

Consumers' personal mobile number is being collected by various online and offline merchants for a variety of reasons. For example, while signing up for a new website, while purchasing items from a retail shop, to receive OTP etc. we give away our personal mobile number. This is often done due to the lack of knowledge about fraudulent activities that can be carried out if a malicious actor gets hold of our phone number. As mentioned in an article[1], "Your cell phone number is a single point of failure" and "if someone steals your phone number, they become you - for all intents and purposes". Such an outcome requires to be mitigated to the best extent possible, using technology.

In an incident widely reported in the media[2], a correspondent's SIM was swapped by a hacker and, within minutes, passwords of his relevant online accounts were reset. The

hacker also tried to borrow Bitcoins from his friends' wallets. While the mechanics of what the malicious actor did are serious yet irrelevant here, it is useful to avoid handing off either mobile number or SIM card for a host of other reasons too.

For example, Whatsapp is a mobile messaging app for which the users have their own mobile numbers as unique ID. Whenever a mobile app is released, it need not be 100% safe and may contain 'zero-day vulnerabilities'. These are security glitches that have not been uncovered during formal security testing, or bug-bounty programs and hackathons during the app's beta testing. A 'zero-day vulnerability' could well be found by a hacker without need to materialize on it, since he/she could sell a description of this vulnerability on the Dark Web to obtain a higher reward - than the app-developer company's bug bounty - in the form of cryptocurrency. Whatsapp's buffer overflow vulnerability[3] was discovered by hackers in a similar fashion, resulting in a situation where hackers could take control of the target user's device by merely initiating a Whatsapp voice call. Thus, communication infrastructure should both be robustly designed-developed, yet free of any unique identifier that could provide a privacy-violating 360-degree view of the user.

In countries like India, most commercial complexes have security posts where mobile numbers of any casual visitors are jotted down, complete with name and address. While the explanation for this is that contacting in an emergency should be possible, it is likely that en masse sales of mobile numbers and details such as addresses are occurring to sales companies, robo-callers, SMS marketing companies or many other types of malicious actors. Patterns of a vulnerable individual's movement can also be discovered using such information, as registers from many locations and over many days can be scanned at scale, often with automated character recognition and pattern recognition software.

Thus, mobile numbers are as important as our credit/debit card numbers. We would thus like to not reveal our personal mobile number, yet be able to subscribe to the services which need our mobile number. This paper proposes a solution that provides a virtual mobile number ID for a specified period of time for each mobile number that is given as input. As an analogy, imagine that any person trying to contact this virtual-ID will initially reach an interactive voice response (IVR) system, where this virtual-ID has to be keyed-in. The call will now be redirected to the real mobile number after translation of the virtual-ID to the real mobile number. It is relevant to note here that the (key, value) pair, i.e. (virtual-ID, real-ID) mapping, where real-ID is the actual mobile number, is stored in a blockchain distributed ledger which avoids a single point-of-failure wherein a malicious actor could steal the entire mapping table. While avoiding this single point-of-failure problem doesn't

make a blockchain infrastructure necessary, there are also other tasks required by the participating nodes of this blockchain, which render smart contracts of certain activities necessary. For such outcomes, blockchain is considered ideal.

Our map for this paper is as follows: Section 2 covers relevant technological solutions that allow privacy for mobile number Real-IDs, and the drawbacks of each. Section 3 briefly profiles blockchain, covers the features of the Ethereum blockchain that makes it (or a parallel installation) amenable to our proposal, and introduces a feature in Android that helps phones guard against 'jailbroken' nodes. Section 4 describes our proposal in detail, with Section 5 providing 2 illustrative use-cases for communication between the app's users. We conclude and provide future directions in Section 6.

2. Existing solutions for bypassing real mobile number

There are mobile apps and websites who currently provide alternate mobile numbers to the users who do not want to reveal their personal mobile number, here are some examples:

2.1. Doosra

Doosra is a mobile app available on Android and iOS platforms, which provides a virtual phone number to the users who sign-up to the doosra service with their real phone number. These virtual phone numbers can be used to contact the users either via call or SMS.

Drawback: According to their privacy policy[4], all the data is transferred to their servers. Further, the database backup is encrypted, and in addition the data collected from the users is stored in a centralized database in India. Any centralized database, even if encrypted, raises the possibility of 'single point of failure'. This also suggests a design pattern that will not be easily accepted by privacy-aware customers, who might also suspect a start-up firm with engaging in underhand exchange of data or transaction-trails in lieu of commercial consideration from brands, investors, political parties or criminal syndicates.

2.2. Websites providing disposable mobile numbers

There are many websites[5] which provide temporary phone numbers for the users who want to bypass OTP verification. Users can choose the mobile numbers according to their region/country first, and then enter this number in the merchant website where they want to bypass the OTP. The recent SMS with the OTP received on the temporary number will be shown on the website. Users simply enter this OTP on the merchant website.

Drawback: A pool of temporary SIMs offered by a service provider however prevents a sequence of SMS messages from reaching the same number, since such a sequence may be important to accomplish a set of actions (e.g. income tax return filing, or setting up bank transfer beneficiaries). In our solution, a virtual-ID can be attached to a real-ID either throughout or, flexibly, for a fixed amount of time. Further, this disposable mobile number method can be used only to bypass OTP via SMS and is not useful to route voice calls if required to be made by the party with whom your mobile number is deposited.

2.3. Virtual Phone Number Apps (currently not supported in India)

There are apps like Google Voice, Burner, Line2, Skype Number, Hushed and many more which provide the users with a virtual phone number. These apps do not, however, work with Indian mobile phone numbers.

3. Blockchain Technology

Blockchain is a distributed ledger technology[6] where the data of multiple transactions - right from the beginning of a system - is stored in data 'blocks'. Each block has within it an encrypted reference to the previous block and this creates a chain of blocks, as illustrated in Figure 1. The entire data of transactions is thus divided into blocks, the trail of blocks viz 'blockchain' being maintained in copies across multiple participating devices called 'nodes'. Some of these nodes add a new block from time-to-time by combining transactions, and such addition needs to be verified by all the participating nodes using consensus algorithms. Thus, tampering with a commonly agreed-upon blockchain is not possible short of large-scale collusion (there are theoretical results to this effect). Blockchain is known for its high reliability and security, with the cryptocurrency Bitcoin being a notable example of such an implementation.

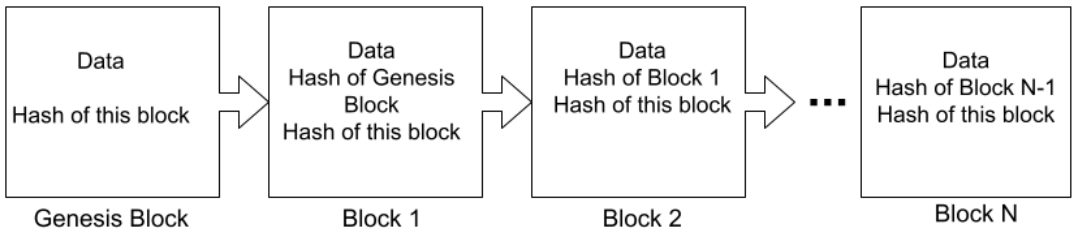

Figure:1

3.1. Permissionless and permissioned blockchain

Anyone can join a permissionless blockchain network as a node since no permissions or approvals are required, and thus can see and participate in verifying all the transactions that occur in the network. The computational work for validating a block of transactions by a node is indicated by a certificate known as 'proof of work', which entitles the validating nodes (also called 'miner') to a payout. In the case of Bitcoin happens to be a few units of the cryptocurrency, thus making mining attractive to scalable and low-cost cloud-services providers. These permissionless networks are not controlled or owned by any organization and government nor do they carry any key person risk like a brand. Examples of these are the many coins, e.g. Bitcoin, Ethereum, but increasingly country's central banks are also issuing such cryptocurrencies that have the advantage of being backed - and equivalent - to 1 unit of the local currency. Such examples are China and Cambodia.

In contrast, permissioned blockchain comes with certain restrictions and roles, most notably the restriction that only approved members can join the network, or view/process the relevant transactions - e.g. only registered exporters, banks, insurers and logistics firms inside a trade finance application using blockchain. These are access control authorizations which improve the security of the blockchain, yet maintain relative privacy and immutability (guaranteed lack of document tampering) among the participants. Further, such a blockchain is also able to deploy smart contracts, i.e. scripts or applications hosted over the blockchain which result in specific outcomes linked to actions or events. Such examples could be a transfer of underlying cryptocurrency if a loan application hosted on blockchain has been approved. Examples of such blockchain are applications implemented with infrastructure SW named Hyperledger (open source) and Corda (open source).

A useful example of a permissioned blockchain is that of rooftop energy title transfer in Germany and Austria [7]. In this application, multiple apartments in an apartment complex possess a common title to the rooftop solar plant, the energy from which is fed into the grid and can be used to offset the monthly electricity bill - issued by the electricity company - of every single apartment. However, the share of energy is also made tradeable, i.e. an apartment owner who will be away from their house for an entire month may grant entire credit from the rooftop plant's electricity generation to a neighbour (thus becoming a useful subsidy for the neighbour's monthly bill). Intervals as short as 15m can be traded in such a system, yet the system needs to be privacy aware to the extent of no users knowing any other users activities, no users

laying claim to any bogus records of credit being transferred to them, and to a large extent the requirement that no centralized database of such credits is kept by the electricity utility company. We shall refer to elements of this implementation when describing our own solution below.

3.2. Ethereum

An example closer to our specific requirement is that of a blockchain-based DNS which piggybacks on a popular currency blockchain named Ethereum[8]. We choose to describe Ethereum since it is:

- a programmable blockchain, i.e. a blockchain whose nodes can have programmable scripts which execute upon successful verification of certain events or actions,
- has a blockchain-based DNS (domain naming service) similar to the one required for (Virtual-ID, Real-ID) translation, and
- has its infrastructure available as open-source, with amenability to modification for a smartphone-only node network that we propose.

Ethereum is a platform which allows developers to build and operate decentralized applications (Dapps)[9]. Dapps are a combination of a user interface written in a manner suitable to a particular client or group of clients and smart contracts[10]. The latter serve the purpose of being the logic written into the dapp, an example being transfer of tokens to a service provider if that service provider maintains sufficient liquidity for all trade in the security that you sponsor. Many smart-contract applications in Ethereum belong to the rubric of Decentralized Finance, or De-Fi. Ethereum has also been associated with lesser energy use, among cryptocurrencies, as opposed to Bitcoin[11] whose energy use is alleged to be equivalent to a middle-sized country.

3.3. Ethereum Node Types

Ethereum also has a flexible family of types of nodes that run the core Ethereum infrastructure. Following are the different types of nodes[12], each having different responsibilities towards the underlying distributed data:

a) Full Node
   - Stores full blockchain data and provides the data on request
   - Needs devices with storage capacity to store the full blocks

b) Light Node
   - Stores only the headers and requests the rest of the data
   - Suitable for low capacity devices like mobile phones

c) Archive Node
   - Stores the archive of historical states of data in the full node
   - This also needs very high storage capacity devices

d) Mining Node[13]
   - Aggregates the transaction requests broadcasted by users into a potential block.
   - Verifies the validity of each such transaction request
   - Produces the *Proof-of-Work* certificate for the potential block.
   - Broadcasts the completed blocks to other nodes
   - Requires devices to have high processing capability

Of these, b. and d. represent the correct fit for the proposed blockchain based on volunteers' smartphone nodes. Note that d. might per se hint at a computational platform far more intensive than a regular platform, however there are instances of smartphone manufacturers producing models which qualify to be a mining node on even computation-intensive blockchains such as bitcoin (refer Section 4.2 below).

3.4. Ethereum Name Service (ENS)

Ethereum Name Service[14] has an objective similar to the Internet's familiar Domain Name Service. DNS performs lookup in a distributed, hierarchical table for IP address values corresponding to a human readable domain name. The only superficial difference in ENS is that the domain name in question would have an extension exclusive to ethereum viz. .eth. These human readable names can be registered via Ethereum supported platforms and these can be mapped to a website address (called 'dWebsites' for decentralized websites) or a wallet address. A problem of squatters, viz. entities who have booked a popular domain-name.eth using ENS, has also come to the fore[15].

Figure 2, shows the steps along how a domain-name, say "almonit.eth", which is already registered on ENS and the corresponding decentralized website "*https://almonit.eth.link/*" accessed via a plugin on Chrome browser. Due to the cryptocurrency and blockchain boom, many browsers now support ENS - though ENS domains are not recognized by the Internet's naming co-ordinator ICANN.

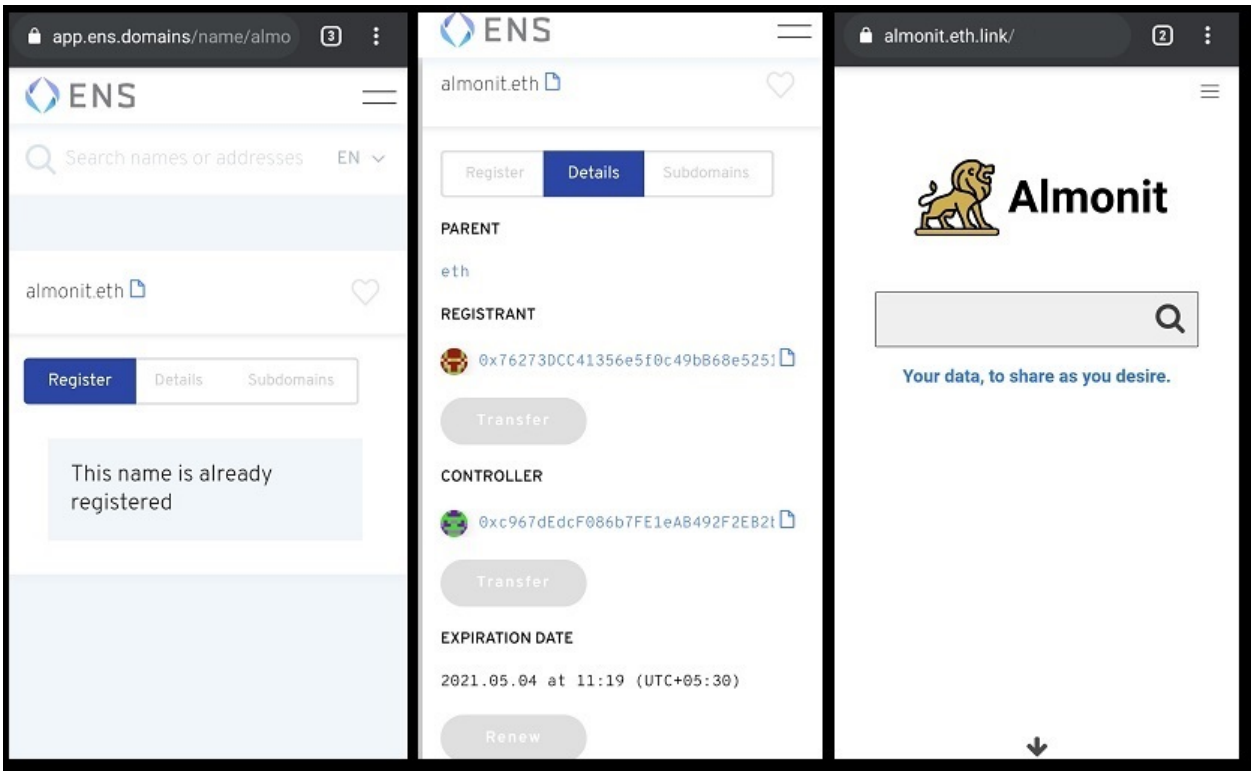

Figure:2

The main components of ENS services are Registrar, Registry and Resolvers. Registry is where the information about the domains and subdomains is stored - i.e. owner of the domain, resolver of the domain and time-to-live for all records under the domain. Registrars are *smart contracts* responsible to create and allocate new names to users. Resolvers are similar contracts that can translate the domain name into address. Figure 3 illustrates steps along the name resolution process when using ENS.

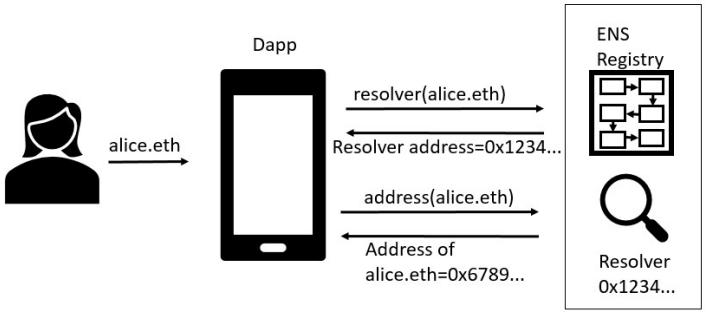

Figure:3

3.5 SafetyNet in Android

A first-level measure to station a blockchain's nodes on a smartphone - and to run smart contracts therein - would be to ensure the node is not on a 'jailbroken' smartphone. Scripts that can be included in a node's app are available to do this. In particular, SafetyNet in Android[16] is a set of APIs and services to protect the apps in the Android platform against security threats; it can detect whether the device is monitored, infected with malicious apps and also detect whether the device is rooted or jailbroken. Android as a platform, recommends[17] using these APIs to protect all critical actions in an app like login, purchase events etc. The app proposed in our solution will be using SafetyNet while invoking all the functions which need critical information to be passed on to other nodes in the network. Based on an article by an android developer[18], apps like IRCTC, Android pay, Samsung pay and PokemonGo have implemented the SafetyNet API.

4. Proposed Solution MPVIDS-SVB using blockchain

This paper is proposing a solution which works in a similar fashion as ENS; i.e. providing a virtual ID to the users who register to the solution with a real phone number. The virtual ID will be translated to the real phone number when SMS needs to be sent and the virtual ID will be translated to the corresponding app ID whenever a call has to be established.

This solution would comprise of the following devices and application on Android platform, of which a. needs a high level of GPRS connectivity and resource reservations:

a) N number of nodes on the public network, which are volunteer mobile devices to run the smart contracts and have sufficient storage space to store the blockchain of (Virtual-ID, Real-ID, App-ID) pairs or relevant transactions of the blockchain.
b) A decentralised app for users of the system. These users could be both I. consumers who wish to use a virtual-ID instead of their Real-ID, and II. initiators of communication to consumers in I. due to their insistence on virtual-ID.

4.1. Virtual Number App

The users who do not want to share their personal mobile number can register themselves in the decentralised application with their real mobile number. Each app installation would also be assigned with a unique app ID. This app will be communicating with the '*registrar*' smart contract residing in the nodes to register the

user details and create virtual ID. Generating virtual ID can follow the same process as the ethereum address generation[19].

Consumers can provide this virtual ID to security guards, merchants, websites or in any other places where they don't want to reveal their mobile number. The businesses/merchants who want to contact these users will also have to use this app, where they will be provided with another interface to enter the Virtual ID of the customer with the options to call or text. This app will then contact the nodes to execute the *resolver* smart contract wherein there is a query of the blockchain database to find the real mobile number mapped to the virtual ID. The same resolver node then either acts as a post-office to host a video/voice call or forwards the senders' SMS onwards to the real number using 3G-4G GPRS, SMS pack respectively. To protect the privacy of both receiver and sender, the content of the SMS will not be stored in the node and will be auto-deleted based on the permission granted to the blockchain's infrastructure app which would be installed in all nodes.

4.2. Nodes

Every blockchain network has a different purpose and hence the roles of the participating nodes are defined by such requirements. In our proposed solution, smartphones which are connected to this solution's blockchain network will be running the full node. They will execute the smart contracts and store the blockchain data. The assumption here is that devices would have dedicated storage space, a decent computing power and network bandwidth. Devices like smartphones can be used as nodes in a blockchain. According to the energy-trading blockchain article[7] (described by us in Section 3.1) an open-source blockchain named ResselChain was built from scratch, wherein the nodes were run on *Raspberry Pi 2 Model B*[20] devices which have very limited resources - all to support 1000s of users at a lowest-possible 15m gap between transactions. Our personal communication with the authors of the same article (16 Jun 2021), dozens of MB were needed to store thousands of blocks, RAM usage was in the range of 100MB and CPU usage was dependent on the intensity of the mining criteria. Another article[21] lists some of the smartphones available in India which can be used to mine cryptocurrencies. A Taiwan-based consumer electronics company has started manufacturing blockchain enabled smartphones from 2018[22]. A more recent example[23] claims to run Bitcoin's full node.

A comparative study on blockchain based DNS design[26] concludes that running full nodes in the participating devices will be required to safely resolve domain names in an early DNS-competitor called Namecoin. The node which performs the translation of phone number could claim 'proof of work' points - like miners do in the bitcoin arrangement: the currency being distributed to volunteer nodes could be Ad revenue from generic display or App Install Ads in the consumer app of MPVIDS-SVB.

Redefining Ethereum's Registrar, Registry and Resolver for phone number lookup:

- Registrar will be the contract which will generate and allocate the virtual ID for the user who registers with the real phone number.
- Registry will save the encrypted (Real-ID, Virtual-ID, App-ID) triplet, the corresponding resolver's address and an appropriate Time-To-Live.
- Resolver will translate the hashed virtual ID to a real phone number

In addition, custom smart contracts are needed for the following functionality:

- To forward an SMS or chat message
- To conduct a video/voice call between initiator and recipient.

5. Use cases on MPVIDS-SVB

Let us assume Alice works for an organization and has to deal with multiple client organizations. When she goes to meet a client in a particular office, the security guard Bob asks Alice for her contact details to be written in a book at the guard post. Alice has a virtual ID from the App already drawn in the morning at work, and she gives the same to Bob to note down in his book. Note that 'registry' in Figure-4 is the blockchain which stores timestamped (Virtual-ID, Real-ID, App-ID) triplets in rough order of when they are created. A 'time to live' field enables such conversions to be retained for as long as law enforcement might seek information on past communications, in view of the intermediary rules that Govt of India has now notified for such systems.

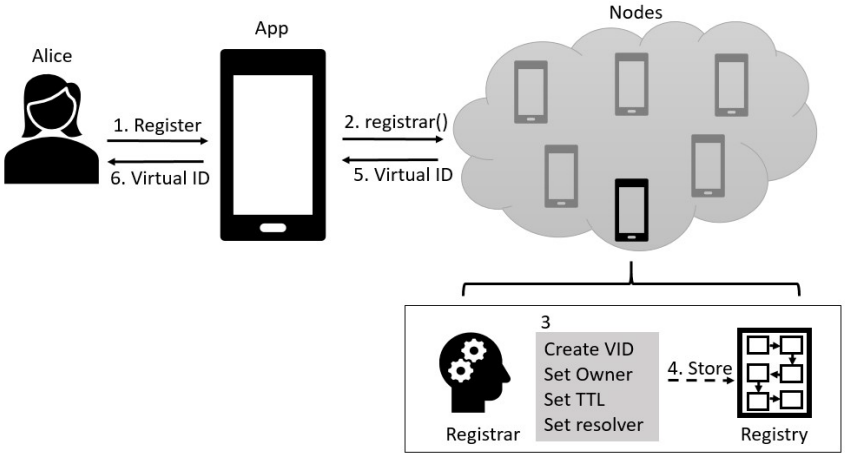

Figure: 4

5.1. Send SMS

Bob will have to enter the Virtual-ID of Alice in the App1 installation on his phone and type an SMS e.g. 'Please call me back at 9037437361, I'm the security guard and need to speak to you urgently, there's a fire drill in the next 15 minutes'. This message from Bob is required to be received as a regular SMS in Alice's phone.

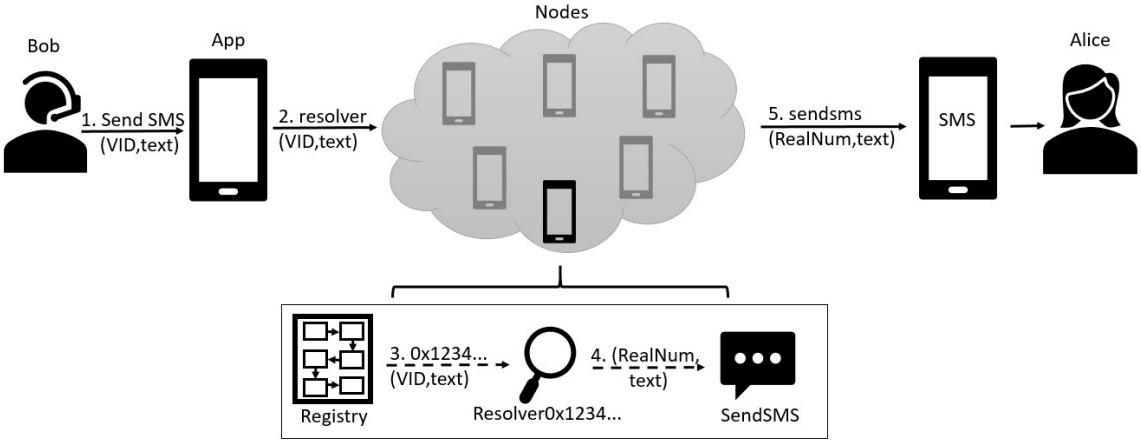

Figure: 5

Since it will have to be sent as an SMS from the particular blockchain's node that is translating - there will be a cost for SMS incurred by the owner of that node. At the same time, the contents of the SMS or the mobile number of the receiver of this SMS should not be known to the node which has performed this translation - hence the smart-contract will also contain instructions for auto-deletion of the sent SMS with OS permission. An important note here is that Alice will receive an SMS from a mobile number which she could misuse. Note, however, that presence of such a number doesn't give a 360^ view - i.e. no other details of the node's owner are revealed - unlike in a security guard register.

Further, if the blockchain's nodes could also be incentivised to obtain a SMS sender ID in the form of a letter-code (as brands in India do), then a sent SMS from the node's smartphone will have such a letter code. The identity problem is thus mitigated entirely. A schematic in Figure 5 above explains this.

OTP Verification on websites: The same workflow as described above will be carried out when Alice tries to perform an OTP verification on a website. But in this case, the front-end is the merchant's website which will be connecting to the smart contracts running on the nodes. So, when Alice enters the virtual ID for OTP verification, the website can check whether it is a virtual ID or real phone number. Alternatively, the website can even provide a checkbox near to the phone number input field, which indicates that it is a virtual ID. Appropriate APIs are then used by the merchant website to connect to the smart contracts of our solution. The SMS containing this OTP will then be delivered to Alice's real number by our solution.

5.2. Place a voice/video call

Bob has to use his App and thus types in the Virtual-ID of Alice. The Virtual-ID to Real-ID translation is done by one of the nodes in the blockchain and this node's GPRS bandwidth is now used to connect a call between 2 ends: Bob and Alice, without either knowing the Real-ID of the other. Let us call this translating node as Cathy. Thus, the voice call is in essence established as (Bob to Cathy) followed by (Cathy to Alice). It is relevant here to note that Cathy is incurring GPRS charges for placing a call to Alice (as well as receiving the call from Bob) - and so is Alice on account of GPRS calls requiring the recipient also to spend bandwidth. Note also that Cathy, who is one of the N infrastructure nodes on the blockchain, is merely forwarding a stream of encrypted Voice-over-IP packets and cannot snoop on this call. Notice this in Figure 6 below.

However, an important question here is whether Cathy is aware of Alice's Real-ID or App-ID, a problem here since a call may last for longer than an SMS' forwarding operation ? Thus we have a situation where Cathy is playing a temporary role as the Centralised call-routing server - essentially a web server based on a smartphone platform. Note how WhatsApp's server plays a similar role, albeit a permanent one, in routing calls between 2 IDs on its network (these calls are end-to-end encrypted). In our proposal, the IDs that Cathy is capable of discovering are 'App IDs' and are seen at a low frequency by Cathy due to the nature of the distributed system - these are not 'Real IDs' that can be used for actual communication. Use of 'App IDs' judiciously by the node's source-code - which is

downloaded as if it is an App from a store - can also ensure that Cathy cannot eventually write a malicious script to communicate to Alice using ‘App ID’ alone**.**

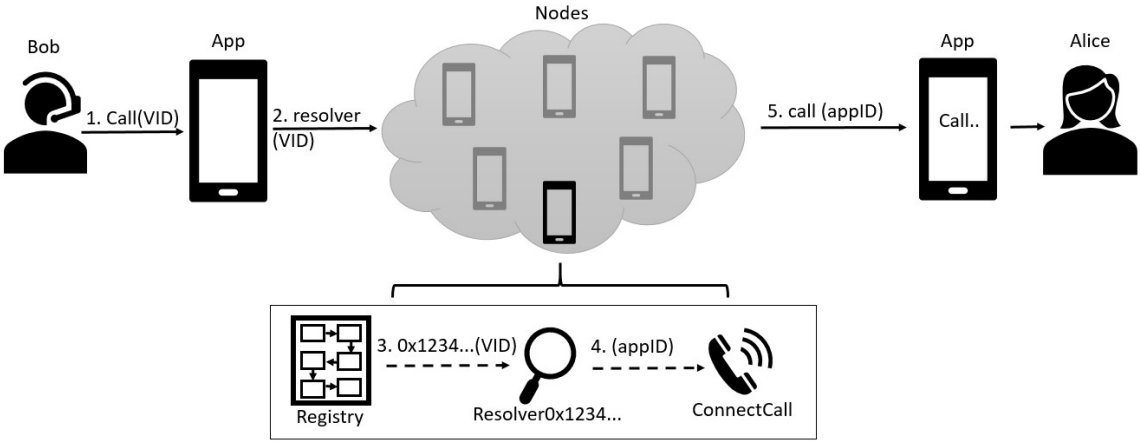

Figure: 6

6. Conclusion and Future Directions

The proposed solution using volunteer-hosted blockchain helps privacy-aware consumers to keep their personal mobile numbers private and yet be able to access all services and amenities - both of online (Call) and offline variety (SMS) - using the virtual ID. Though there are similar solutions available, they are all proprietary and use centralized storage, thus becoming a single-point-of-failure. Adapting the system to match social media intermediary rules, which in India require immediate identification of a call or message’s initiator, would be a necessary field of investigation. Combining such a privacy-aware blockchain with incentive schemes to profitably compromise on some privacy, in the pattern of web browser Brave’s ‘Attention Token’ (BAT) can also be pursued using smart contracts.

Acknowledgement

We thank Professor Asharaf S. (Digital University of Kerala) and Ms Mazeeda A M (formerly an MTech student, Information Security, Govt. Engg College Trivandrum) for their valuable inputs towards this paper.

Bibliography

[1] Whittaker, Z. (2018, December 26). Cybersecurity 101: How to protect your cell phone number and why you should care. *TechCrunch*. https://techcrunch.com/2018/12/25/cybersecurity-101-guide-protect-phone-number/
[2] Biggs, J. (2017, August 24). I was hacked. *TechCrunch*. https://techcrunch.com/2017/08/23/i-was-hacked/
[3] WhatsApp. (2019). *WhatsApp Security Advisories*. https://www.whatsapp.com/security/advisories/archive/
[4] Doosra. (accessed in June 2021). *Privacy Policy*. https://www.doosra.com/privacy-policy
[5] Yashu-Blog. (2019, December 26). *Top 15 Websites - Fake Phone Number for Verification | OTP Bypass Online*. https://www.yashublog.com/2017/11/top-15-websites-fake-phone-number-for.html
[6] Wikipedia. (accessed in June 2021). *Blockchain*. https://en.wikipedia.org/wiki/Blockchain
[7] F. Knirsch et. al. (2019, March 11). Implementing a blockchain from scratch: why, how, and what we learned. *EURASIP Journal on Information Security, 2019*(1). https://doi.org/10.1186/s13635-019-0085-3
[8] Buterin, V. (2015). A Next-Generation Smart Contract and Decentralized Application Platform. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
[9] Ethereum. (accessed in June 2021). *Introduction To Dapps*. https://ethereum.org/en/developers/docs/dapps/
[10] Ethereum. (accessed in June 2021). *Introduction To Smart Contracts*. https://ethereum.org/en/developers/docs/smart-contracts/
[11] Digiconomist. (accessed in June 2021). *Ethereum Energy Consumption Index*. https://digiconomist.net/ethereum-energy-consumption/
[12] Ethereum. (accessed in June 2021). *Nodes And Clients*. https://ethereum.org/en/developers/docs/nodes-and-clients/#node-types
[13] Ethereum. (accessed in June 2021). *Mining*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/mining/
[14] Ethereum. (accessed in June 2021). *Introduction*. https://docs.ens.domains/
[15] P. Xia et. al. (2021, April). Ethereum Name Service: the Good, the Bad, and the Ugly. https://arxiv.org/pdf/2104.05185.pdf

[16] Android. (accessed in June 2021). *Protect against security threats with SafetyNet*. https://developer.android.com/training/safetynet
[17] Android. (accessed in June 2021). *SafetyNet Attestation API*. https://developer.android.com/training/safetynet/attestation#request-attestation-process
[18] Goyal, H. (2017, May 31). *Secure Android app with SafetyNet*. https://medium.com/@hargoyal/secure-android-app-with-safetynet-8e367a1c8ad0
[19] Ethereum. (accessed in June 2021). *Ethereum Accounts*. https://ethereum.org/en/developers/docs/accounts/#account-creation
[20] Raspberry. (accessed in June 2021). *Raspberry Pi 2 Model B*. https://www.raspberrypi.org/products/raspberry-pi-2-model-b/
[21] Cashify. (accessed in June 2021). *Top 5 Smartphones To Mine Cryptocurrency In India*. https://www.cashify.in/top-5-smartphones-to-mine-cryptocurrency-in-india
[22] Mearian, L. (2018, July 13). *Here come the first blockchain smartphones: What you need to know*. https://www.computerworld.com/article/3289687/here-come-the-first-blockchain-smartphones-what-you-need-to-know.html
[23] HTC. (2019, October 19). *HTC Launches The Exodus 1s — The First Smartphone To Put A Full Bitcoin Node In Your Pocket*. https://www.htcexodus.com/us/newsroom/2019-10-19/
[24] Y. Liu et. al. (2019). A Comparative Study of Blockchain-Based DNS Design. *Association for Computing Machinery*, 86-92. https://doi.org/10.1145/3376044.3376057

Research Office
Indian Institute of Management Kozhikode
IIMK Campus P. O.,
Kozhikode, Kerala, India,
PIN - 673 570
Phone: +91-495-2809237/ 238
Email: research@iimk.ac.in
Web: https://iimk.ac.in/faculty/publicationmenu.php