One: Community & Entropy Based Access For Networks

by Nagaraju Gangaraju (April 2023)

Abstract:

Introducing computational discontinuity through the human mind, social structures and nature could be key to addressing ill-effects of centralization.

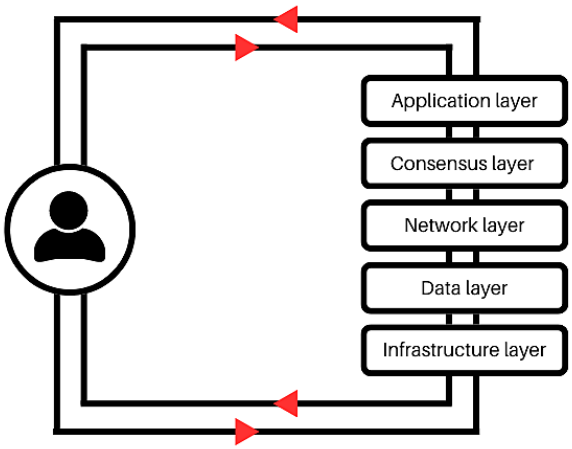
Introduction:

Internet is one of the largest centralized information systems by humans with two basic uses of information it contains: (i) active use - used to derive value (eg. instant messaging, internet search, placing an order, any computation of stored data, etc.) and (ii) passive storage - used to derive value later (eg. chat backups that can be looked up for reference later, indexed values of website that'll be useful when someone searches the internet again, inventory of products/goods that'll be useful when someone needs it, data storage, etc.) i.e. storage doesn't have value other than that it can be used to derive value later. The ability to identify is key to preserving advantages of centralized information (ability to send a message to a friend, find exact information on a topic, place an order for an exact product needed, etc.), but it also exposes the information for exploitation in centralized ways (chat backups are vulnerable to hacks or surveillance, search history used for surveillance, order histories used for selling more than you need, etc.). It makes sense to use orderly (i.e. logical) ways of computation for active use of information, but why do we use the same orderly (i.e. logical) ways of computation for encryption of information for storage? *Almost like hiding the keys and relying on the increased complexity of the map to them, to protect their whereabouts.*

Everything on networks/blockchains today depend on passwords/keys that are computationally generated/stored someplace. Depending on how important they are to someone else, there will always exist an orderly way to compromise them - if the device is connected to a network, it could be hacked; and if it isn't connected to a network, it could physically be hacked by methods including social engineering (most popular way security is compromised); and if nothing else works, with enough time they can be guessed by brute force trial and error. If only they are not generated and stored in orderly way i.e. are non-computational, we could ensure there exists a computational discontinuity in ways of passive storage of information and security is not tied to orderly ways of computation. Which implies it doesn't matter if the device is hacked over a network or physically, security of the information is linked to all possible information in the universe over all time. *Like hiding the keys and not making a map to them at all to protect their whereabouts.* The only reliable source of computational discontinuity which doesn't require trust is one's own mind - which could be central to a community and entropy based access platform for networks like the internet. This is the non-original thesis this research expands upon

Vulnerability of Networks/Blockchains:

Cryptography of networks/blockchains is not quantum-proof today; even if it is tomorrow, it'll not be *string*-proof tomorrow and so on. Science is based on orderly ways and there'll always be new science, as long as cryptography is based on orderly ways, it'll always be breakable.



From the perspective of individual that interacts with the network/blockchain, one wouldn't want the keys to be compromisable. If they are compromisable, it creates the problems of impersonation, privacy invasion and theft for the individual and as for the network, loss of trust necessitates additional energy to be spent to re-establish trust through more complex computation. From the perspective of the network that built it, every node that is compromised enables centralization, especially through artificial intelligence. *The ability to compromise is what enables centralization to exist and as a consequence the compromises are the ill-effects.* This could be addressed by ensuring cryptography is based on increasingly non-orderly ways.

One Solution:

Consider the encryption method developed by Ron Rivest, Adi Shamir and Leonard Adleman (RSA encryption) which relies on orderly ways of mathematics of two large prime numbers which when multiplied together generates a larger number which is computationally difficult to find factors for, is hence used for *secure enough* communication over the network. For example, 829 times 379 is 314191, but larger numbers are used in application.

$$829 * 379 = 314191$$

More generally, $A * B = X$ *where A and B are prime numbers*

Apart from benefiting from quantum computing (QC) itself, Shor's algorithm developed by Peter Shor is able to break the RSA encryption because it relies on the prior knowledge that it was encrypted in an *orderly* way in the first place (i.e. *two prime numbers* 829 and 379 were *multiplied* to generate 314191). Provided QC and Shor's algorithm, factors can be solved for and encryption can be broken as a result.

i.e. $314191 = 829 * 379$

More generally, Given X, it's factors A and B can be solved for;

Also, if through social engineering, one of the factors is known, the encryption can be broken too. Same applies for all encryption based entirely on mathematical/hardware cryptography including those used in blockchains.

If instead 'color of the shoes I wore when we first met' (represented by a number *say* 439931 or 11) times 'time of the night when you observed saturn rings on star gazing trip' (represented by a number *say* 111 or -7) is 314191, was used for encryption *along* with mathematical/hardware cryptography.

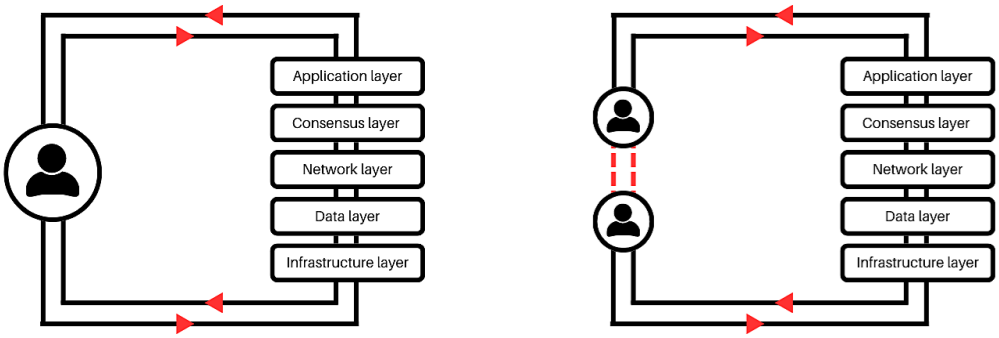
i.e. 'color of the shoes I wore when we first met' * 'time of the night when you observed saturn rings on star gazing trip' = 314191;

or, 439931 * 111 = 314191

or, 11 * (-7) = 314191

More generally, $A * B = X$ *where A and B are ANY number*

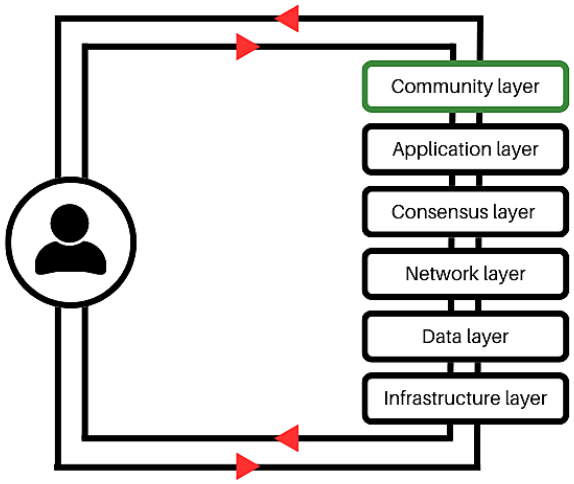
This would infinitely increase the computation required for breaking the encryption since (i) *A* times *B* need not be equal to *X* and (ii) there are an infinite ways of arriving at the two numbers *A* and *B*. *Good luck computing that.*



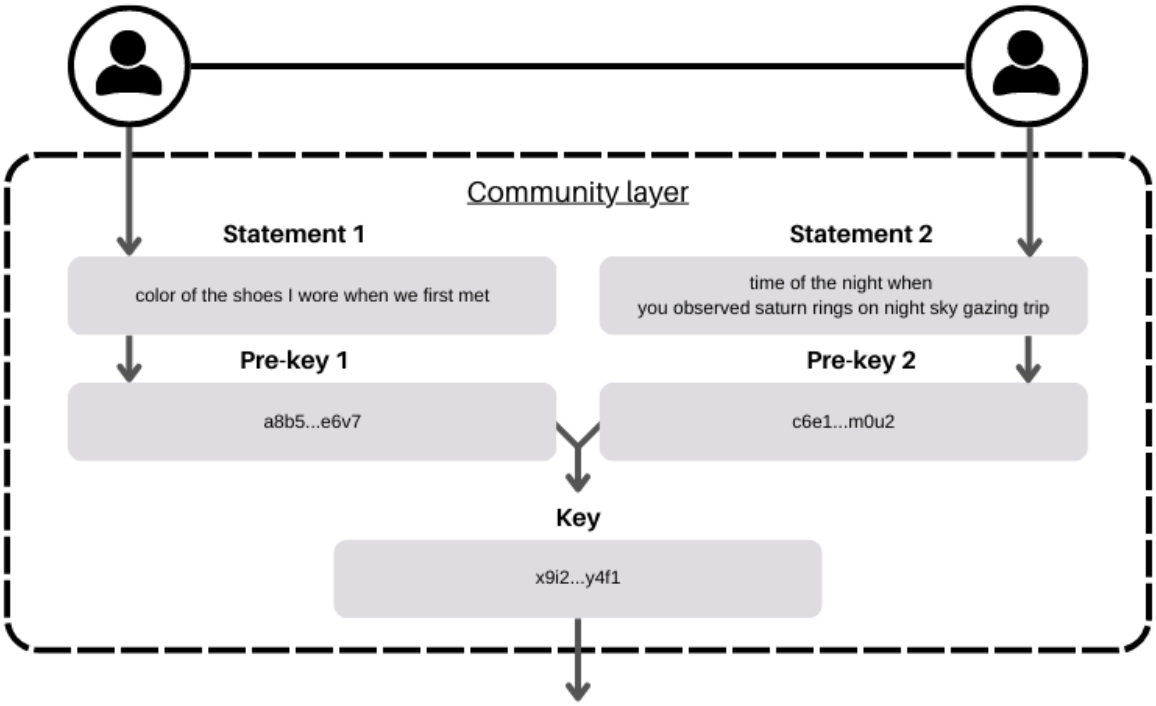
The main difference would be that the keys are not generated in however computationally complex ways and assigned to individuals, but rather are generated through complexity of two minds that can communicate. This ensures computational discontinuity by ensuring the logic flow of generating and storing keys are off the chain/network. This forms a community based access layer that could be the quantum-proof foundation for blockchains and networks like the internet.

Implementation:

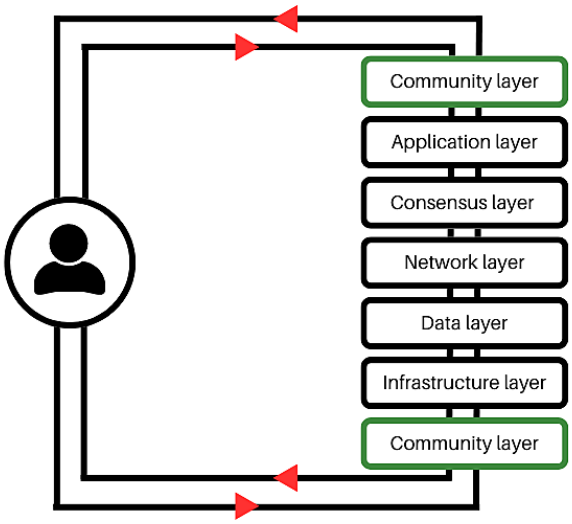
Such a computational discontinuity can be achieved by introducing a *community layer* before members of the network use the application layer to interact with the network.



Community layer is simply an open-sourced, sufficiently random key generator which requires two or more members to create *pre-keys* which when combined generate keys that can be used by members to interact with the network as usual. These pre-keys are generated by members and their infinite minds through two statements whose connection is known to only them. Each combination of pre-keys creates a verified connection.



If the community layer is introduced before builders of the network interact with the infrastructure/hardware layer as well, you would further address security threats including that of artificial intelligence.



Application:

With its implementation, the internet could become quantum-proof. The active use of the internet would remain fully functional, while passive storage (which is where exploitation happens) could be tied to the infinities of the universe which protects everyone connected to it.

Future Research:

Time-based security dimension to keep out bot-activity.

Reference & Further Reading:

Ancient knowledge of India.