Privacy as a core value of Web3

Privacy has been a time memorial virtue that has been coveted by societies and individuals alike, and rightly so. From building walls around living spaces to setting up virtual firewalls to hide activity, privacy has long been the name of the game, for without privacy many aspects of modern life would cease to exist. Development of newer ideas and technologies is highly dependent on it being private before being stable enough to be released to the public. Almost all research and innovation is conducted following a pattern of private development, semi-private refinement, and finally public utility. Without this process, a new idea may be corrupted or abandoned owing to various factors not limited to theft and societal pressures.

Since the advent of the internet, the world has gotten remarkably smaller and more connected. This has only increased the value of privacy in the modern world. In the beginning of the internet, users or network participants were largely private, only identified by the IP address that they used to connect with the network. As time has gone on, this abstraction of the user has been systematically eroded in an effort to provide a user with better personalisation, to the extent of a few organisations now powerful enough to match humans with their activity and behaviour with increasing accuracy. Granted, this invasion of privacy has been self inflicted with users often exchanging their data for a cost effective experience; ie, privacy is not and has never been free.

Indeed, history has shown the lengths to which individuals and organisations have gone to maintain privacy, from Julius Caesar incorporating box ciphers for his messages to the Germans using the Enigma code for their communication in WW2. However, with web3 and blockchain technology in general, sophisticated cryptography has become the norm by incorporating one way functions at its core. This heavy use of asymmetric cryptography goes a long way in ensuring privacy for the average user. Indeed, privacy is also mentioned as a core design principle in Bitcoin, the original blockchain, achieved via *anonymity* through the use of public key encryption and one way functions.

Having said that, some loss of privacy is guaranteed owing to the open nature of blockchains wherein all transaction data is made public, albeit anonymous. As the paper mentions, some linking to a common owner is unavoidable, particularly in the case of multi input transactions. However, by using new key pairs for every transaction, users may further hide their activity on the network in the name of privacy. Additionally, as a blockchain becomes more mainstream and network effects grow, block analysis becomes increasingly expensive, thereby reserving the justification of such analyses only in the case of malicious actors. For the general public, privacy is *practically* achieved.

Another feature of blockchains that ensures privacy for the average user is the cryptocurrency aspect of the chain; ie, by having every interaction on the chain associated with a cost, often in the form of paying network tokens, the cost of privacy is brought down. It is not difficult to imagine a network where user data is encrypted and owned by the user themself, with the decryption of said data by a third party made possible by paying the user some network tokens. Indeed, this is the contrast between web3 and web2.0; ie, where earlier free experiences were paid for by user data, now user data is effectively monetized with the incentives being awarded to the users themselves. The rewards of providing data to a third party can then simply be a straightforward transfer of tokens or in more sophisticated cases, an enhanced experience of an application or service, such as personalisation.

Blockchains, or web3, have ushered in a new form of economy — the creative economy; ie, an economy where novel ideas and creations are valued more than reputation and past performance. This change in focus also ensures greater privacy for the average user since the value of knowing a user on a personal level is significantly lower. Combined with no cost address generation, this allows a user to maintain multiple identities on a network or across networks, to the limit of an identity per creation, further enabling privacy. Indeed obfuscation is often a goto paradigm in secrecy and web3 is highly conducive to the same. So long as users maintain certain practices, such as new key pairs per transaction, abstinence from transacting between owned accounts, etc. they may remain highly private on the network. Indeed, the network does not care who the user is, so long as the user acts in a good faith manner and avoids malicious activities.

In summary, privacy is an essential part of life, but is seldom granted in modern life owing to the cost associated with it. Web3 aims to change that with having it as a core value within its design from incorporating asymmetric cryptography to network effects achieved by growing blockchains. One significant way web3 achieves this dedication to privacy is by pushing the cost of eroding privacy to the entity doing the eroding, be it from paying for data access to expensive block analyses. Indeed, web3 is often thought of as a *step function improvement* to web2.0, and one of these improvements is the switching of user experience for data to tokens (or money) for data. A good experience is often guaranteed by the permissionless and capitalistic nature of the network, ie, users often have a greater choice to switch in the case of bad user experience. Although absolute privacy may not be achieved, due to block analyses, the costs associated with tracking ensures such expensive analyses are reserved for malicious actors and the general user is provided with practical privacy.
