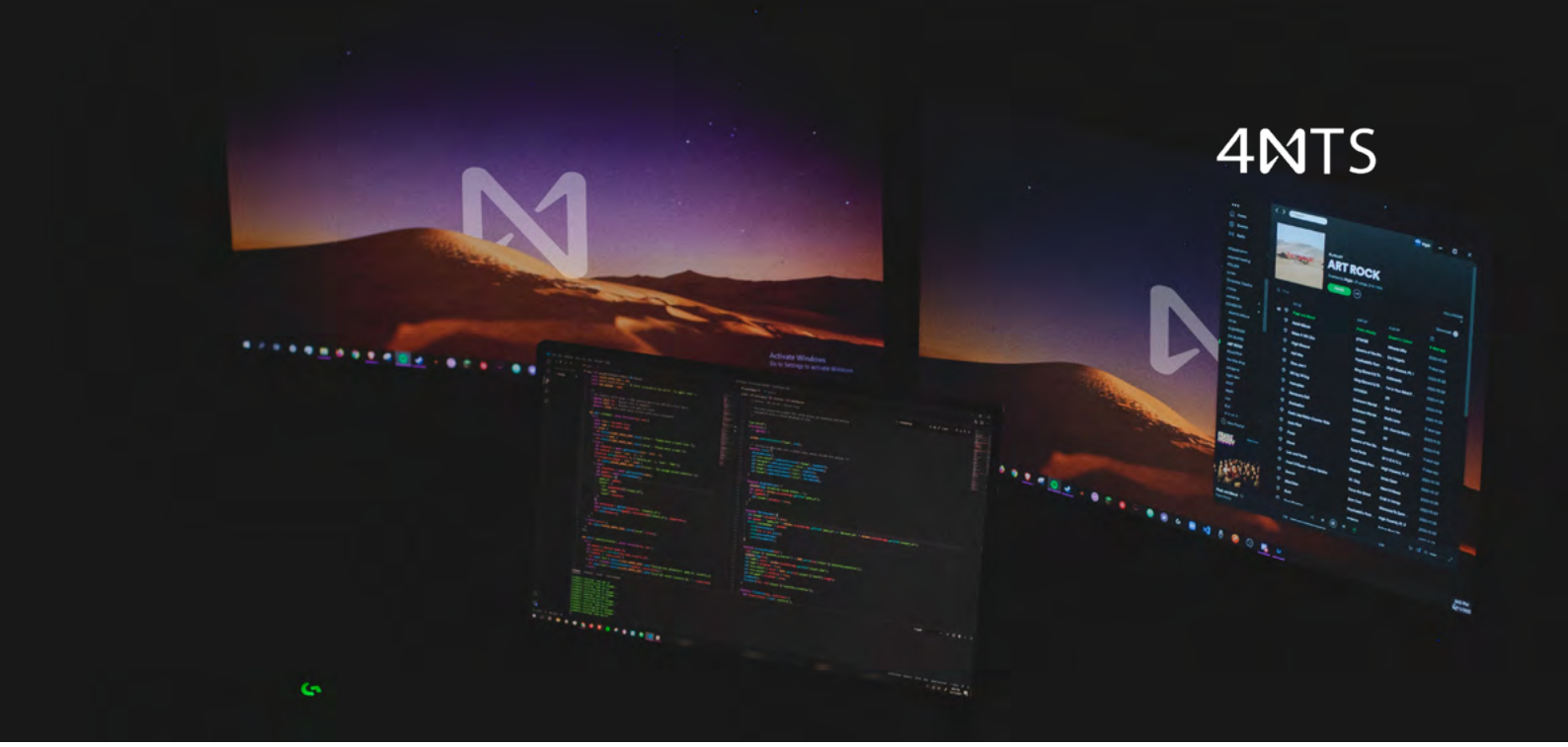


The Open Web and Privacy

A Brief Overview

Numerous data breaches in recent years, such as the Cambridge Analytica scandal, have prompted questions regarding how companies and governments should handle the information entrusted to them by their users. This in turn, has also intensified research into the development of new technologies that are better able to preserve the privacy of companies and users.

As a result, countries and legislators have rushed to establish new compliance requirements for user's privacy and data collection - such as the General Data Protection Regulation in Europe and the Chinese' Personal Information Protection Law. In parallel, a new trend of turning to new technologies such as blockchain to solve privacy issues has emerged. In this regard, contrary to the initial perception of many, blockchain technology could not only be GDPR-compatible, but help increase levels of data privacy and protection while also returning data ownership of that information to individuals. Therefore, blockchain technology can very much be used as a privacy tool.

As a result of this value proposition, many players in the industry have started competing for leadership in numerous privacy related fields.

Monero (XMR) is an open source highly fungible cryptocurrency that gained the reputation of being the most anonymous cryptocurrency on the market. Monero's blockchain is configured to be opaque, that is, to provide anonymity to transaction details by disguising the addresses of participants (Monero. "About Monero." Accessed Jan. 22, 2021). Since it is able to provide intractability of transaction history it offers its user a safer network that impedes its participants to be blacklisted.

ZCash is another cryptocurrency that was created with the aim of improving privacy in the world of cryptocurrency. Similarly to Monero, ZCash guarantees anonymity by blurring the transaction's information (blurring of sender and receiver addresses, and amounts of transactions). However, unlike Monero it provides the possibility to operate fully anonymous transactions or partially anonymous transactions and operates in a different way.

Zero-Knowledge Proof Transactions are able to provide complete transactional privacy by using hash functions, which makes it possible to carry out transactions without disclosure of personal information. The only requirement to engage is that those involved in the transaction demonstrate the veracity of information that they possess, but without revealing other sensitive information.

Data Compliance and Blockchain: The security related attributes that blockchain technology display have a great potential to provide data protection to users. Through peer-to-peer (networking) and cryptography it allows for two major improvements: it creates an immutable database for data assurance purposes, and facilitates the exercise of individual rights (i.e. the right to be informed, right of access etc..)

Private Keys: Blockchain uses asymmetric cryptography to enable the exchange of assets (such as cryptocurrencies) between one person and another. Each person holding an asset (of any kind) on the blockchain has a public key - also known as an 'address' - and a private key. Anyone in possession of the public key used to encrypt a message will not be able to decrypt it, the only way to do this is to use the private key associated with the public key used. The use of private keys then provides an extra layer of security for those engaged in transaction.

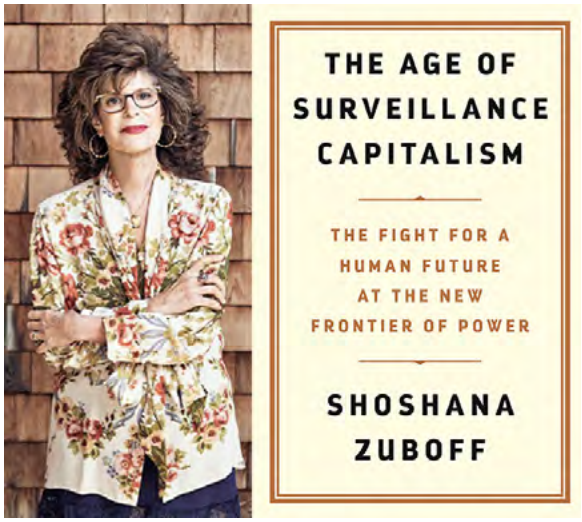
Blockchain Technology as Tool to Protect Privacy and Increase Security and Transparency

As explained in the introduction, a blockchain is a decentralized network in which all the records are carved in a distributed manner and shared among different devices scattered around the world. The records are kept by all members of a blockchain, and network confirmations are executed at regular intervals, linking (chained and encrypted) to the previous existing blocks. This makes the logs immutable and inviolable.

With blockchain technology, instead of providing our information to centralized platforms/shops, we can store it within a decentralized ledger, free of single points of failure. That makes it possible to encode a significant number of interactions and increase reliability, eliminating the political and commercial risks associated with the process being managed by a central entity.

The fact that transactions are recorded on a blockchain in the form of a hash means there is a high degree of transparency while securing the content of the recorded transaction. Transactions recorded on the blockchain take on the format of an “alphanumeric code” (which includes the date and time). Thus, its structure provides transparency while simultaneously protecting the content recorded on the network. This alphanumeric code, or hash, is the equivalent of a “fingerprint” of a piece of data that exists outside of the blockchain network. The chances of two different transactions having the same hash recorded in a blockchain are virtually zero. Thus, transparency and confidentiality can be reconciled on a blockchain.

Blockchain to Safeguard Political Freedoms and Prevent Power Imbalances



As Shoshana Zuboff has pointed out in *The Age of Surveillance Capitalism*, big tech companies have an unprecedented amount of control over people’s personal data. That creates a power imbalance between provider and consumer which jeopardizes people’s freedom in significant ways. Over the past years companies like Amazon, Google, and Facebook have increasingly used their power to not only starve off competition - posing a threat to small size and medium size businesses- but also to interfere in the political life of citizens. The latest example of their power to interfere in political affairs is Facebook and Twitter’s decision to indefinitely suspend Donald Trump’s Twitter and Facebook account following the events at the Capitol, thus arrogating to themselves the right to take a decision on a public matter of the highest political importance.

Another troubling aspect of this state of affairs is that the amount of private data that these companies have access to allows them to get insights into patterns of human behavior, study emotional responses, and foresee future behavior with the help of big data analytics. This allows them to create better and more addictive products but also to develop techniques to trigger emotions and desires, and all without the consumer's knowledge.

The adoption of a technology that prevents tech giants from holding a disproportionate amount of power and information about people becomes crucial in order to safeguard people's political freedoms and dignity – as well as ground a vision of a better more open future. Ultimately, the Open Web, and its core underlying technology blockchain, have the capacity to ground a pathway towards a society where privacy, freedom, and transparency are provided to its citizens. It is then crucial that its development is followed, discussed, and encouraged.

Topics to Discuss

Anonymous Cryptocurrencies and Financial Services (DEX's)

Data Protection and Compliance

Open-Source Applications and User First Data Models (Users Give Permission)

The Open Web As A Response To Surveillance Capitalism

The Danger of Misappropriating a Blockchain for a Surveillance State

NEAR

NEAR Protocol is a 3rd Generation Blockchain Platform built with scalability and usability in mind. The NEAR Ecosystem is home to a number of cutting edge projects in the crypto space that hold the promise of building the Open Web. Geographically diversified, NEAR features headquarters across 3 continents (USA, San Francisco; China, Shanghai; Switzerland, Zug). The NEAR Community, NEAR Guilds, and the NEAR Team are growing the NEAR Ecosystem to be a home for native crypto, enterprise blockchain, and emerging technology solutions around the world. Learn more about NEAR at NEAR.org or join the discussion on Telegram.