STEEL KIWI

“Using Blockchain Technology to Boost Cyber Security”

Yuliia Horbenko
MARKET RESEARCHER

HOME / BLOG / BUSINESS

Navigating the online world safely has become a real concern over the last few years and, looking at how intense and sophisticated some of the recent hacker attacks around the world have been, it seems like things are bound to only get worse.

Even though hackers are getting better at hacking, the ways to combat them are also improving very fast. In fact, we already have a nearly impenetrable technology, known as blockchain, which can be used to protect our data from cyber attacks and improve cybersecurity across industries.

This article provides an overview of how blockchains can improve the online security of any business, ensuring that data cannot be damaged, stolen, or lost.

Blockchain technology 101

Blockchain technology has been around for just under a decade, initially introduced as a way to store and/or send the first cryptocurrenc gradually spread worldwide, people have be industries, including as a means to increase

Steelkiwi Inc. · Typically replies within a day ✕

Hi! How can we help you?

Continue as Vedika

Not you? Log into Messenger

What is a blockchain?

Blockchains are distributed networks that can have millions of users all over the world. Every user can add information to the blockchain and all data in the blockchain is secured gh cryptography. Every other member of the network is responsible for verifying that t being added to the blockchain is real. This is done using a system of three keys (private,

How do blockchains get formed?

A verified piece of data forms a block which then has to be added to the chain. To do this, blockchain users have to use their respective keys and powerful computing systems to run algorithms that solve very complex mathematical problems. When a problem is solved, the block is added to the chain and the data it contains exists on the network forever, meaning that it cannot be altered or removed.

How can data be updated?

In order to make updates to a particular pie
new block on top of the previous block, crea
even something as small as a comma, gets
the entire chain across the network also ch
alteration or change to any piece of data is
because users can always look at previous versions of a block to identify what is different in
the latest version. Using this thorough form of record-keeping makes it easy for the
to detect blocks that have incorrect or false data, preventing loss, damage, and corru

results in two things. First, they can earn money for renting their “extra” storage space and, second, they ensure that the chain will not collapse. If, for instance, someone who is not the owner of a piece of data (say, a hacker) tries to tamper with a block, the whole system analyzes every single block of data to find the one that differs from the rest (or from the majority). If the system finds this type of block, it simply excludes it from the chain, identifying it as false.

Blockchain technology is designed in such a way that there is no central authority or storage location. Every user on the network plays a part in storing some or all of the blockchain. Everyone is responsible for verifying the data that is stored and/or shared to make sure false data cannot be added and existing data cannot be removed.

Preventing fraud and data theft

Blockchain technology provides one of the best tools we currently have to protect data from hackers, preventing potential fraud and decreasing the chance of data being stolen or compromised.

In order to destroy or corrupt a blockchain, a hacker would have to destroy the data stored on every user’s computer in the global network. This could be millions of computers, with each one storing a copy of some or all the data. Unless the hacker could simultaneously bring down an entire network (which is near impossible), undamaged computers, also known as “nodes”, would continue running to verify and keep record of all the data on the network. The impossibility of a task like taking down a whole chain increases along with the amount of users on a network. Bigger blockchain networks with more users have an infinitely lower risk of getting attacked by hackers because of the complexity required to penetrate such a network.

This complex structure provides blockchain
secure form of storing and sharing informa
why innovators have begun applying the te
and increase protection of data.

How Guardtime uses blockchain technology to safeguard data

Guardtime has already become successful in using blockchain technology to keep important data safe.

The company takes away the need to use keys for verification. Instead, they distribute every piece of data to nodes throughout the system. If someone tries to alter the data, the system analyses the whole mass of chains, compares them to the metadata packet and then excludes any that don't match up.

This means that the only way to wipe the entire blockchain out is to destroy every single separate node. If just one node remains rur n be restored, even if all of the other nodes ar

Guardtime's system works in such a way th been made to the data and is constantly ve discrete way to tamper with blocks in the c

Preventing Distributed Denial of Service (DDoS) att s

until the site gets overwhelmed with requests and crashes. DDoS attacks have been happening at an increased frequency recently, affecting bigger companies like Twitter, Spotify, SoundCloud, and more.

The current difficulty in preventing DDoS attacks comes from the existing Domain Name System (DNS). DNS is a partially decentralized one-to-one mapping of IP addresses to domain names and works much like a phone book for the Internet. This system is responsible for resolving human-readable domain names (like steelkiwi.com) into machine-readable IP addresses (made up of numbers).

The fact that it is only partially decentralized means that it is still vulnerable to hackers because they are able to target the centralized part of DNS (the one which stores the main bulk of data) and continue crashing one website after another.

Using blockchains to prevent DDoS attacks

Implementing blockchain technology would fully decentralize DNS, distributing the contents to a large number of nodes and making it nearly impossible for hackers to attack. Domain editing rights would only be granted to those who need them (domain owners) and no other user could make changes, significantly reducing the risk of data being accessed or changed by unauthorized parties. By using blockchains to protect the data, a system can ensure that it’s invulnerable to hackers, unless every single node is simultaneously wiped clean.

Some companies are already implementing blockchain in this area to prevent DDoS attacks from occurring. For instance, Blockstack provides a fully decentralized option for DNS. The concept behind the company is to make the entire worldwide web decentralized by removing all third parties from managing web servers, ID systems, and databases.

If current DNS would operate on blockchair
names, but only authorized owners would
the data would be stored on many different
would have a copy of the entire data on the
hack or destroy it completely.

MaidSafe is a similar company based in the UK. Their goal is also to decentralize the web and create something like an alternative Internet where users are able to run apps, store
and do everything else they normally do online, but in a more secure environment.
signing up for this service, users can choose how much of their personal storage space they

can make the data readable again is its owner, ensuring that the data is not accessible by anyone other than the authorized owner.

Innovative uses for blockchain technology

As more people join the worldwide web and technology continues to develop, more data gets produced and more hackers will attempt to steal or corrupt that data. The technology behind blockchain is versatile and incredibly useful for the future of the Internet, allowing users to better secure their data.

Innovative uses for blockchain technology are already becoming a part of other fields beyond cryptocurrencies and can be especially useful to boost cybersecurity. By implementing rigorous encryption and data distribution protocols on a network, any business can ensure that their information will remain safely intact and out of the reach of hackers.

If we've managed to captivate your interest with the ambitious prospects of the blockchain's future in cyber security, please feel free to contact one of our sales representatives and ask them about the ways to implement this technology into your own business, thus making its benefits a part of your own life.

Useful article? Please share it with your followers:

SHARE SHARE 0 SHARE

Steelkiwi Inc. · Typically replies within a day ×

Hi! How can we help you?

Continue as Vedika

Not you? Log into Messenger

Related articles