AUGUST 9, 2022

DSEC

DEMOCRATIZING CYBERSECURITY

The cybersecurity industry is growing exponentially, and the number of attacks on businesses is also increasing. One of the reasons for this is that cybersecurity experts are in high demand, but there are not enough professionals to meet the demand. This has led to an increase in cyberattacks and data breaches.

The traditional security assessment approach is time-consuming and expensive and does not provide adequate coverage. Red teaming is a term that describes a penetration test that is performed by an independent team of experts (the red team) against the same system or network to which the blue team, which is the company's in-house security group, is defending. A red teaming operation can be used to evaluate the effectiveness of a company's security program and identify potential risks and weaknesses. Red teams can also be used to test how well an organization would respond to cyberattacks and other types of incidents.

The problem with red teams is that they are expensive and hard to manage because they require large amounts of time from skilled personnel who have access to sensitive information about the company's infrastructure or systems.

At DSEC Labs, we are working on a new approach based on blockchain technology that offers a more scalable solution that can be automated. We believe the blockchain provides a revolutionary way to democratize cybersecurity by providing a way for anyone to assess their own security and identify vulnerabilities without relying on an outside party. The blockchain will allow for the creation of new markets and opportunities for those who are interested in cybersecurity. It will have a profound impact through greater automation of security assessments via smart contracts. It will also help to develop new

tools, resources, and services with the potential to improve cybersecurity practices across the board.

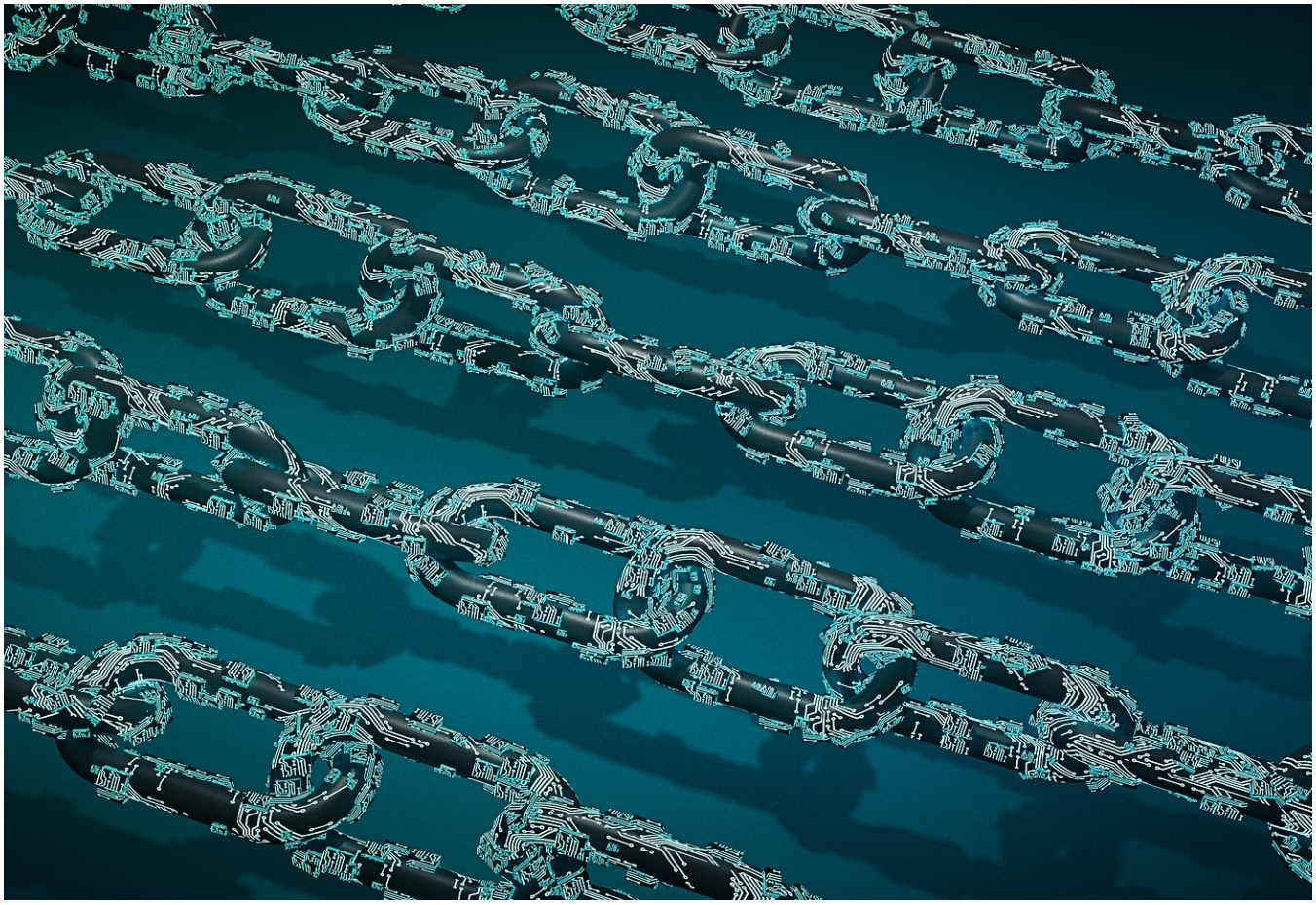
Our technology has many ways in which it can help cybersecurity professionals, including:

- Providing a tool for penetration testing on demand and at scale
- Enabling companies to conduct red team assessments without revealing any sensitive data and without any human intervention
- Allowing companies to use automated data cleaning and analytics to help identify potential cyberspace threats
- Delivering new insights into the detection of malicious code
- Helping companies become more efficient by removing human error and freeing up time for other tasks
- Enabling companies to improve their data utilization rates by turning large, static datasets into interactive graphics for cybersecurity training, decision making, and other purposes.

Through DSEC Labs, we strive to reposition cybersecurity from a central authority to the hands of individuals, making security a shared and manageable responsibility.

MARKET

The cybersecurity market has been growing exponentially, and the spending is expected to be resilient, according to the article *"2022 cybersecurity forecasts predict growth, emphasizing resilience"* in https://venturebeat.com/2022/07/05/2022-cybersecurity-forecasts-predict-growth-emphasizing-resilience/. Estimates for the annual cost of cybercrime are at $10.5 trillion by 2025, up from $3 trillion in 2015. Furthermore, Gartner



Pixabay License

predicts the market for information security products will grow from $172.5 billion in 2022 to $267.3 billion in 2026, achieving a CAGR of 11%. In addition, the article projects that AI within cybersecurity platforms will continue growing steadily over the next five years and is expected to be worth $46.3 billion in 2026.

Finally, Cybersecurity Ventures predicts the cyber insurance market will grow from $8.5 billion in 2021 to $14.8 billion by 2025, reaching $34 billion by 2031 with a 15% annual growth.

Remarkably, $5.9 billion was invested in cybersecurity startups in the first quarter of 2022. Crunchbase says that funding in the first quarter of this year was nearly a 50% increase from the first quarter of 2020.

Source: 2022 cybersecurity forecasts predict growth, emphasizing resilience

VISION AND CORE FEATURES

At DSEC Labs, we are harnessing the power of blockchain technology to create a decentralized cybersecurity ecosystem. This new system democratizes cybersecurity and marks a significant shift from traditional, closed-market approaches to cyber defense.

The landscape of the cybersecurity industry is changing; automated attacks are becoming more prevalent as penetration testing and security assessments transition from human-driven to computer-powered processes. Given this shift and the availability of attackers, it's not cost-effective for companies to hire expensive Red Teams for on-demand security tests. Instead, we advocate for the use of automated Red Teaming tools to enhance the efficiency of penetration assessments and increase companies' proactive stances towards security risks.

Our vision is to leverage blockchain technology to provide personalized cybersecurity testing, transition to a shared economy model where every participant contributes to their own security, and foster an ecosystem where individuals and entities benefit from building security tools, identifying vulnerabilities, and aiding in attack mitigation and system patching. We aim to incentivize the proactive inspection of systems, websites, and infrastructures for better protection against cyber threats.

The rising trend of open-sourcing cybersecurity tools has expanded the pool of available resources for companies seeking the right tools for their security needs. Despite these advancements, the traditional centralized server components of these tools, such as Metasploit and Nessus, still present vulnerabilities that could be exploited. By integrating blockchain technology, we aim to decentralize cybersecurity for a more secure future.

Blockchain has immense potential to revolutionize cybersecurity and penetration testing. By automating manual processes, it allows security testers to work more efficiently, reducing both time and cost. The decentralized nature of blockchain eliminates the need for centralized servers and reduces the risk of exploitation. Each tool in the ecosystem can be made public and open-source, which prevents single-point vulnerabilities that could compromise entire systems in traditional setups.

A standout feature of our protocol is the ability to create smart contracts for automation. Smart contracts digitally define the rules, penalties, and rewards of an agreement, allowing tasks to be performed without reliance on intermediaries such as cloud service providers or penetration testers. Blockchain-based smart contracts verify and enforce obligations between parties on a distributed network, negating the need for a central authority or third-party enforcement mechanism.

The blockchain's ability to facilitate automated and decentralized execution of security assessments, penetration tests, red teams, and a myriad of other tasks reshapes the cybersecurity landscape, enabling operations that were previously challenging or impossible to execute on an open internet.

THE DSEC FRAMEWORK: KEY ACTORS AND FEATURES

The DSEC framework is based on the following actors:

- Requestors
- Defenders
- Governors

DSEC is an innovative, new technology that connects computers in a peer-to-peer network, enabling business owners and single individuals (so-called “Requestors”) to ask for the execution of security tasks to specific software applications. DSEC makes use of the computing power of all the computers in its network. This allows Requestors to delegate tasks such as anti-virus scans or data encryption to multiple computers simultaneously to increase efficiency.

Defenders are the network nodes that act as security task executors. They use their computing power, the best open-source tools, and the most advanced AI algorithms to execute tasks and give results back to Requestors. A single node can act as both a Requestor and a Defender.

Governors are responsible for maintaining the latest version of the software tools and the AI algorithms, reviewing and accepting new security tools proposed by Defenders. Governors are also responsible for delivering Digital Identity services to the Requestors that ask for them.

The DSEC framework merges the client-centric security assessment protocol and information commons of blockchain with red team and open-source to establish a system resilient to bad actors at all organizations, from 1 to N. By employing blockchain technology in a distributed services model, DSEC is an independent source for cyber asset management that avoids a single point of failure in traditional centralized approaches.

The new paradigm provides unmatched levels of access control, resilience to external threats, interconnection with other blockchains, an open template for function linkage supporting DLTs, and a more sophisticated notion of roles than just the requestor/defender/governor schemes.

The table below summarizes benefits and incentives for the 3 actors of the DSEC network.

Actor	Who they are	Role	Incentive to participate
Requestors	Any digital solution owner, from global companies to single individual	Request security services for digital solutions	Get access to high quality security services at a price which is a fraction of the centralized scenario in a very simple way of usage

Defenders	Anyone (minimal requirement to possess at least X DSEC native tokens and X computing power)	Run security services using the tools provided by the network and using their computing power	Get paid using their existing hardware and software capacity
Governors	Anyone (minimal requirement to possess at least Y DSEC native tokens and Y computing power)	Maintain the Security registry and manage the DID provision	Get paid using their existing hardware and software capacity

FOCUS

DSEC is a blockchain-based and AI-powered security infrastructure that can assist with conducting an automated breach assessment. It can help remove the tedium of taking on manual assessment tasks and traditional industries' archaic methods from companies that are forward-thinking enough to adopt a next-generation security ecosystem.

Our focus is to change the landscape of cybersecurity by making red team and penetration testing tools decentralized. The project will use blockchain technology as well as smart contracts in order to make these tools auditable, immutable, and accessible for everyone. Using blockchain technology, DSEC has developed smart contracts that allow both red team exploitation and blue team defense capabilities to be decentralized and shared across a consortium of nodes in the network. By doing this, we can create more transparent and collaborative environments for information security.

The DSEC platform reduces security budget, labor, and management costs while providing a single interface with which any company can conduct its own internal assessments.

The DSEC infrastructure focuses on hacking, penetration testing, and red teaming. DSEC's primary goal is to make these three services open-source and decentralized. Our mission is to build a permissionless security modeling assessment protocol for not just securing confidentiality but also integrity and availability in all business sectors.

THE DSEC TOKEN

The DSEC Token ("DSEC") is a core component of the network and is designed to ensure flexibility and control over the project's future evolution. Tokenizing a service that rewards productive behavior can deter bad outcomes. Therefore, it makes sense that the DSEC token would be used as a reward system to incentivize good behavior.

We want to incentivize defenders to assess the security and enforce rules. We believe this can come from a decentralized cybersecurity solution with tokens. The DSEC token would encourage more organizations to use assessment providers and, in turn, provide them with better defense. Red teamers, consultants, and penetration testers would earn DSEC tokens by identifying vulnerabilities and creating decentralized security assessment tools. The singular goal of our decentralized security ecosystem is incentivizing teamwork by rewarding defenders with DSEC tokens for providing agencies with assessment reports and facilitating hacks on organizations' networks—in essence, giving security teams the tools they need to get ahead of potential threats.

The DSEC features are:

- Payments from Requestors to Defenders will be made in DSECs.
- Applying as Defender or Governors will need a certain number of DSECs.
- Voting and approval of new security tools will be done through DSECs.

DSEC is created during the crowdfunding period (described in this whitepaper), and, following the first significant release of our system, DSEC will be associated with a variety of functions in the network.

The DSEC token enables organizations to use cryptoeconomics on the blockchain in order to incentivize defenders, who are incentivized to help protect all systems. The DSEC token is a utility token and will be used as a means of payment for services provided by network participants. Security assessments, bug bounties, alerts, etc., will all be paid for in DSEC tokens. The cost for these services is set in the Smart Contract so that everyone—including those who are not on the team—can be incentivized to participate.

DSEC will be used by:

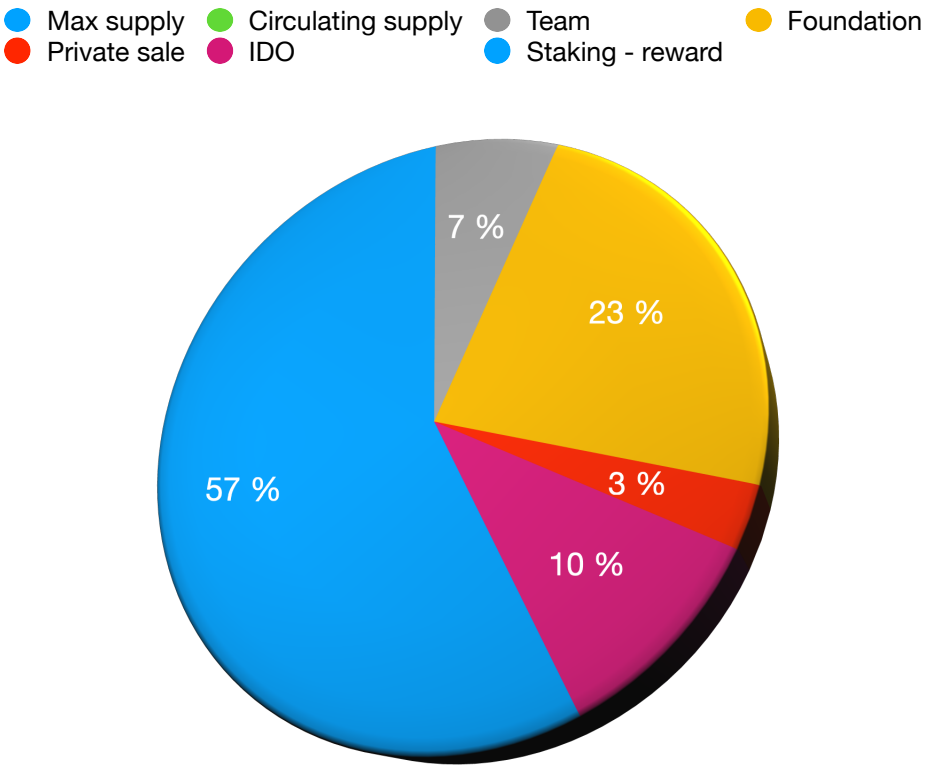
- Defender:
    - Participate in the network: the minimum amount of DSEC to hold is x
    - Get rewards. Rewards = (DSEC hold/total circulating DSEC) + (provided computing power in the last 30 days/total computing power or the network in the last 30 days)
- Governor:
    - Participate in the network: the minimum amount of DSEC to hold is y
    - Get rewards. Rewards = (DSEC hold/total circulating DSEC) + (provided computing power in the last 30 days/total computing power or the network in the last 30 days)
- Requestor:
    - Pay the requested security services. Considering the value of DSEC is supposed to increase over time, the price of the security services is quoted through a stablecoin, although the payment is processed through DSEC only.

TOKEN ECONOMICS

The following table shows the token economics of the pre token:

Tabella 1

			Token price		N. Token
Max supply					2.000.000.000
Circulating supply					860.000.000
Team		7 %			140.000.000
Foundation		23 %			460.000.000
Private sale		3 %	US$	0,10	60.000.000
IDO		10 %	US$	0,15	200.000.000
Staking - reward		57 %			1.140.000.000
MARKET CAP	US$	301.000.000	US$	0,35	



VESTING

- **TEAM:**
    - 20% initial release
    - 80% locked for 1 year
- **FOUNDATION:** 100% initial release, since those tokens will be used for:
    - marketing;
    - CEX/DEX listing;
    - advisors;
    - backup for emergencies.
- **PRIVATE SALE:**
    - 20% initial release
    - 20% every following quarter
- **IDO**:
    - 20% initial release
    - 20% every following quarter

SECURITY SERVICES

The penetration testing market is a hugely significant pillar in the cyber protection industry. Currently, most cyber protection testing comes from vendors that employ red team groups, which security services indirectly provide to client companies. As a result of this indirect relationship, transparency and compensated incentives are not explicit or prominent.

DSEC aims to launch a blockchain-based penetration testing marketplace - an incentivized model that incentivizes red teams to signalize vulnerabilities by rewarding them with DSEC tokens. It will allow penetration testers access to rewards by accessing a list of available requests from qualified organizations and delivering their attack scenarios.

Feeding insights for a more secure ecosystem: DSEC offers unmatched advantages over classical models of security assessments in terms of speed and also cost efficiency. There is no need for any third-party trust to ensure nothing corrupt is happening. That, together with the enhanced accountability and transparency that the blockchain enables, makes this much safer than traditional security assessments where people trust a central metering point.

We expect the DSEC network to promote security and privacy worldwide by delivering top-quality security products and services to everyone at an affordable cost. It will provide several types of security services, such as:

- Identity management services: Nowadays, we have more options for identity management services like DIDs (decentralized identifiers), SSIs (self-sovereign identity), or even things like smart contracts so that you can store your information on a blockchain and control how it is used by yourself.

- Vulnerability assessment: It is a process of identifying and mitigating potential vulnerabilities in an organization's IT infrastructure. It is a critical step in the security process, as it helps to identify weaknesses that hackers can exploit. The vulnerability assessment process typically includes the following steps:
  - Identifying assets and their vulnerabilities

- Identifying threats
- Determining risk
- Developing mitigation strategies
- Implementing mitigation strategies

- Penetration testing: It is a process of evaluating the security of an application by simulating an attack on it. It is a way to identify vulnerabilities in the system and fix them before hackers exploit them. The penetration testing process can be divided into three phases: information gathering, vulnerability analysis, and exploitation. The first phase involves gathering information about the target system, such as its IP address, operating system version, and open ports. The second phase involves analyzing the gathered data to find vulnerabilities in the system that can be exploited. The third phase involves exploiting these vulnerabilities to gain access to sensitive data or perform malicious actions on the target system.

- Password cracking test: As a part of the security assessment, penetration testers will often be asked to find out if it is possible to crack a password. This is usually done by brute-forcing the password. However, this can take a long time and needs to be done manually. AI-enabled applications can help make this process even easier by providing a number of different tools that do this for you.

- Performance tests: They are also a test used to see how the system performs under different workloads. The tests are meant to analyze a system's responsiveness and stability with different loads, stress levels, and soak time. The use of AI can also be applied to measure the performance of a system in other ways. For example, it can give clarity on how scalable and resource-efficient that system is.

- Software quality assurance: A review of the source code can help improve internal code quality and maintainability and find problem areas not picked up by manual tests. It also looks at aspects important to the "outside" world, such as correctness, performance, security vulnerabilities, and other issues affecting customer experience.

- Smart contract assessment: Smart contracts are a way to conduct transactions without having to trust anyone. These transactions are trackable and irreversible. There are many ways to assess smart contract security. One way is to use penetration

testing tools that will scan for vulnerabilities in your smart contract code and find potential exploits. Another way to prevent exploitation is to reward red/blue teams for finding vulnerabilities and fixing them before they get exploited.

- DeFi protocols test: Decentralized finance security assessment measures and assesses the ecosystems of cryptocurrencies and decentralized applications (Dapps) to identify vulnerabilities, market threats, and attacks. Decentralized finance enables innovation in broken financial markets. However, like everything else in this niche, it brings a mixture of risks and opportunities that should be considered before adoption. Decentralized finance security assessments should include pen testing, vulnerability scanning, reverse engineering, competitive analysis, and adversarial thinking applied to Dapps. Competitive analysis may unearth weaknesses that have not been addressed by development teams that could be exploited by cybercriminal groups.

- Wallet password recovery: The Wallet Password Recovery (WPR) protocol is a decentralized application that can be used to recover the password of a crypto wallet. It does this by following the same best practices of password cracking, which means that it uses dictionary attacks and brute-force attacks to recover the wallet's password. WPR has many advantages over centralized services. For example, WPR does not need trust in any service provider or a third party because it relies on blockchain technology.

DSEC penetration testing marketplace will operate on a blockchain. Usually, penetration tests require marketplaces to be centralized for professionals to conduct their services as well as maintain records and billing information. With a decentralized application model, all the tasks above could be sorted out with algorithms and managed by the blockchain.

This method of conducting penetration tests has many advantages in terms of trustless service, where each transaction is open to public scrutiny, and rewards are distributed among Dapp developers and testers.

THE FIRST RELEASE: A TRUST-LESS PASSWORD TESTER

Passwords are critical for any organization's security and must be tested regularly to ensure that they can withstand hacking attempts from malicious actors.

PassGAN is a password generator that uses generative adversarial networks (GANs) to generate complex passwords. The generated passwords can be used in penetration testing or red teaming to bypass security measures. A GAN is a type of neural network with two competing neural networks, the generator and the discriminator. The generator generates new samples based on the data it receives, while the discriminator tries to identify if something is real or fake. The goal of this system is for the generator to fool the discriminator into thinking its generated samples are real.

Our first release of DSEC will provide decentralized password testing functionalities based on the PassGAN technology. With a decentralized password testing tool, hackers are rewarded for their efforts to test the security of a password. In addition, they can also get rewards for providing data to drive the machine learning algorithms and train them.

The idea is to use smart contracts and blockchain technology to incentivize hackers by rewarding them with DSEC tokens. This way, they can be encouraged to test all possible combinations of passwords and brute force attacks, increasing the speed at which they can break passwords.

Our first use case will be a trust-less wallet recovery service. We are building a self-executing contract that combines smart contracts and oracles to help recover lost passwords and allow people to regain control over their cryptocurrency funds again. Cryptocurrency has been around for a while now, and it is no surprise that many people have lost their passwords to their crypto wallets. This is a problem because recovering crypto wallets for users of lost passwords can be difficult if not impossible. That is why it's important to recover passwords to these wallets - they can sometimes be worth millions of dollars. Indeed, cryptocurrencies started becoming popular in 2009, with the first bitcoin wallets popping up. The initial value of these coins was so low that many users underestimated the need to adequately guard the passwords and private keys of these digital wallets. We estimate that 2,000,000 of the 18,500,000 Bitcoins in circulation are

lost or inaccessible. We also estimate that 300 Ethereum GENESIS wallets containing a total of 1,500,000 Ethereum have never been accessed.

Sources: Artificial intelligence just made guessing your password a whole lot easier, PassGAN: Password Cracking Using Machine Learning

ROADMAP