A major issue faced by users in the cybersecurity community is their inability to fully know which security vendors they can or cannot trust. Security vendors can make all the claims they want — regarding the performance, effectiveness, detection capabilities, and other promises about their security solutions — but at the end of the day, customers simply have to take their word for it. But that’s where blockchain can help. With blockchain technology, customers using cybersecurity services can verify that the web attacks being detected and blocked are in fact legitimate.

- > Một vấn đề lớn mà người dùng trong cộng đồng an ninh mạng phải đối mặt là họ không thể biết đầy đủ nhà cung cấp bảo mật nào mà họ có thể hoặc không thể tin tưởng. Các nhà cung cấp bảo mật có thể đưa ra tất cả các tuyên bố mà họ muốn - liên quan đến hiệu suất, hiệu quả, khả năng phát hiện và những lời hứa khác về giải pháp bảo mật của họ - vào cuối ngày, khách hàng chỉ tin vào những lời nói ấy là thật. Nhưng đó lại là điều nơi mà blockchain có thể giúp ích. Với công nghệ blockchain, khách hàng sử dụng các dịch vụ an ninh mạng có thể xác minh rằng các cuộc tấn công web bị phát hiện và bị chặn trên thực tế là hợp pháp.

The type of attacks, attack methods, file signatures, hashes, and any other proof that provides legitimacy of an attack can be made available on the blockchain. As mentioned, records that go on the blockchain are permanent and difficult to alter. Instead of taking the word of the security vendor, customers can refer to the blockchain to verify threat data, including false positives. Additionally, because the blockchain is powered by a user community, other third-party security experts and vendors can come to a consensus to verify that such attacks are indeed attacks.

-> Loại tấn công, phương pháp tấn công, chữ ký tệp, mã băm và bất kỳ bằng chứng nào khác cung cấp tính hợp pháp của cuộc tấn công có thể được cung cấp trên blockchain. Như đã đề cập, các bản ghi trên blockchain là vĩnh viễn và khó thay đổi. Thay vì lấy lời của nhà cung cấp bảo mật, khách hàng có thể tham khảo chuỗi khối để xác minh dữ liệu về mối đe dọa, bao gồm cả xác thực giả. Ngoài ra, bởi vì blockchain được cung cấp bởi cộng đồng người dùng, các chuyên gia bảo mật và nhà cung cấp bên thứ ba khác có thể đi đến đồng thuận để xác minh rằng các cuộc tấn công như vậy thực sự là các cuộc tấn công.

**\* Transparency for security vendors and their users**

- Blockchain makes data open/transparent in a way that has not existed in financial systems, which is why many argue that blockchain could be used as the new standard for transparency. How exactly is data made transparent on the blockchain?

- Network participants have the ability to access holdings and transactions of public addresses using a block explorer, used to search the blocks of a blockchain, their contents, and their relevant details.

-> Blockchain làm cho dữ liệu mở / minh bạch theo cách chưa tồn tại trong các hệ thống tài chính, đó là lý do tại sao nhiều người cho rằng blockchain có thể được sử dụng làm tiêu chuẩn mới cho tính minh bạch. Chính xác thì dữ liệu được thực hiện minh bạch trên blockchain như thế nào?

Những người tham gia mạng có khả năng truy cập các khoản nắm giữ và giao dịch của các địa chỉ công cộng bằng cách sử dụng trình khám phá khối, được sử dụng để tìm kiếm các khối của chuỗi khối, nội dung của chúng và các chi tiết liên quan của chúng.

- In the case of cybersecurity this means decentralized threat data can be made accessible. While some may argue that in-depth analyses and reports provide sufficient confidence that the security solutions are performing as they’re supposed to, bias may come into play since these companies are paying for the analysis reports, certifications, and other acknowledgements in the first place. With blockchain, any bias can be eliminated, thanks to this transparency.

-> Trong trường hợp an ninh mạng, điều này có nghĩa là các dữ liệu mối đe dọa phi tập trung có thể được truy cập. Mặc dù một số người có thể tranh luận rằng các phân tích và báo cáo chuyên sâu cung cấp đủ tin cậy rằng các giải pháp bảo mật đang hoạt động đúng như mong muốn của chúng, nhưng sự thiên vị có thể phát huy tác dụng vì các công ty này đang trả tiền cho các báo cáo phân tích, chứng nhận và các xác nhận khác trong lần đầu địa điểm. Với blockchain, bất kỳ sự thiên vị nào cũng có thể bị loại bỏ nhờ tính minh bạch này.

**\* Transparency in cybersecurity**

- There’s no denying that blockchain is changing the way we look at cybersecurity. Transparency is just one of the many ways in which blockchain can benefit security vendors, regular end users, or even governments in the cybersecurity community. It’s not every day that we are presented with a technology that can guarantee the legitimacy of attacks and be made public at the same time.

- With blockchain, security vendors can have concrete evidence to back up their claims of performance or effectiveness, and individuals will be able to refer to this information when choosing a cybersecurity solution.

-> Không thể phủ nhận rằng blockchain đang thay đổi cách chúng ta nhìn nhận về an ninh mạng. Tính minh bạch chỉ là một trong nhiều cách mà blockchain có thể mang lại lợi ích cho các nhà cung cấp bảo mật, người dùng cuối thường xuyên hoặc thậm chí các chính phủ trong cộng đồng an ninh mạng. Không phải ngày nào chúng ta cũng được sử dụng một công nghệ có thể đảm bảo tính hợp pháp của các cuộc tấn công và đồng thời được công khai.

-> Với blockchain, các nhà cung cấp bảo mật có thể có bằng chứng cụ thể để sao lưu các tuyên bố về hiệu suất hoặc hiệu quả của họ và các cá nhân sẽ có thể tham khảo thông tin này khi lựa chọn giải pháp an ninh mạng.

How safe is blockchain technology? It has proven to be a powerful technology for protecting the integrity of vital information. But that doesn’t mean it’s entirely safe.

The technology has become increasingly prevalent in recent years as the cryptocurrency markets have moved toward center stage. One reason for its rapid adoption is that blockchain is designed to offer unparalleled security to digital information.

In its short life, blockchain—also known as distributed ledger technology—and the cryptocurrencies it powers has seen its share of successes and failures. And as its applications spread, blockchain security has become more important—and not just for cryptocurrency investors.

-> Công nghệ blockchain an toàn như thế nào? Nó đã được chứng minh là một công nghệ mạnh mẽ để bảo vệ tính toàn vẹn của thông tin quan trọng. Nhưng điều đó không có nghĩa là nó hoàn toàn an toàn.

Công nghệ này ngày càng trở nên phổ biến trong những năm gần đây khi thị trường tiền điện tử đã chuyển sang giai đoạn trung tâm. Một lý do giải thích cho việc áp dụng nhanh chóng là blockchain được thiết kế để cung cấp khả năng bảo mật vô song cho thông tin kỹ thuật số.

Trong vòng đời ngắn ngủi của nó, blockchain - còn được gọi là công nghệ sổ cái phân tán - và các loại tiền điện tử mà nó cung cấp đã chứng kiến sự thành công và thất bại của nó. Và khi các ứng dụng của nó lan rộng, bảo mật blockchain trở nên quan trọng hơn - và không chỉ đối với các nhà đầu tư tiền điện tử.

\* Basic blockchain security

Blockchain technology produces a structure of data with inherent security qualities. It's based on principles of cryptography, decentralization and consensus, which ensure trust in transactions. In most blockchains or distributed ledger technologies (DLT), the data is structured into blocks and each block contains a transaction or bundle of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

Blockchain technology enables decentralization through the participation of members across a distributed network. There is no single point of failure and a single user cannot change the record of transactions. However, blockchain technologies differ in some critical security aspects.

->

Công nghệ chuỗi khối tạo ra một cấu trúc dữ liệu với các phẩm chất bảo mật vốn có. Nó dựa trên các nguyên tắc mật mã, phân quyền và đồng thuận, đảm bảo sự tin cậy trong các giao dịch. Trong hầu hết các blockchain hoặc công nghệ sổ cái phân tán (DLT), dữ liệu được cấu trúc thành các khối và mỗi khối chứa một giao dịch hoặc gói giao dịch. Mỗi khối mới kết nối với tất cả các khối trước nó trong một chuỗi mật mã theo cách gần như không thể giả mạo được. Tất cả các giao dịch trong các khối đều được xác nhận và thống nhất theo cơ chế đồng thuận, đảm bảo rằng mỗi giao dịch đều đúng và chính xác.

Công nghệ chuỗi khối cho phép phân quyền thông qua sự tham gia của các thành viên trên một mạng lưới phân tán. Không có điểm lỗi duy nhất và một người dùng không thể thay đổi bản ghi của các giao dịch. Tuy nhiên, các công nghệ blockchain khác nhau ở một số khía cạnh bảo mật quan trọng.

## \* How security differs by blockchain types

Public and private blockchains

Public blockchain networks typically allow anyone to join and for participants to remain anonymous. A public blockchain uses internet-connected computers to validate transactions and achieve consensus. Bitcoin is probably the most well-known example of a public blockchain, and it achieves consensus through "bitcoin mining." Computers on the bitcoin network, or “miners,” try to solve a complex cryptographic problem to create proof of work and thereby validate the transaction. Outside of public keys, there are few identity and access controls in this type of network.

Private blockchains use identity to confirm membership and access privileges and typically only permit known organizations to join. Together, the organizations form a private, members-only "business network." A private blockchain in a permissioned network achieves consensus through a process called "selective endorsement," where known users verify the transactions. Only members with special access and permissions can maintain the transaction ledger. This network type requires more identity and access controls.

When building a blockchain application, it’s critical to assess which type of network will best suit your business goals. Private and permissioned networks can be tightly controlled and preferable for compliance and regulatory reasons. However, public and permissionless networks can achieve greater decentralization and distribution.

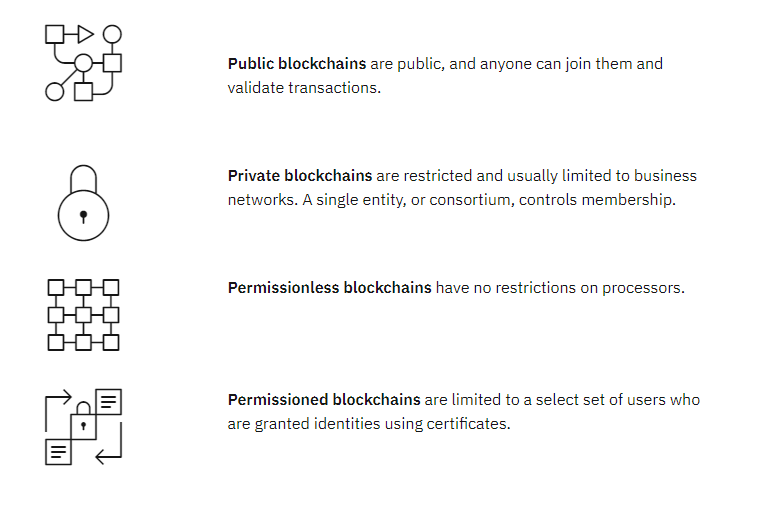
->

Blockchain công khai và riêng tư

Các mạng blockchain công cộng thường cho phép mọi người tham gia và người tham gia được ẩn danh. Một blockchain công khai sử dụng các máy tính được kết nối internet để xác thực các giao dịch và đạt được sự đồng thuận. Bitcoin có lẽ là ví dụ nổi tiếng nhất về một blockchain công khai và nó đạt được sự đồng thuận thông qua "khai thác bitcoin". Máy tính trên mạng bitcoin, hay còn gọi là "thợ đào", cố gắng giải quyết một vấn đề mật mã phức tạp để tạo bằng chứng về công việc và do đó xác thực giao dịch. Bên ngoài các khóa công khai, có rất ít điều khiển nhận dạng và truy cập trong loại mạng này.

Các blockchain riêng tư sử dụng danh tính để xác nhận tư cách thành viên và truy cập các đặc quyền và thường chỉ cho phép các tổ chức đã biết tham gia. Cùng với nhau, các tổ chức tạo thành một "mạng lưới kinh doanh" riêng tư, chỉ dành cho thành viên. Một blockchain riêng tư trong một mạng được phép đạt được sự đồng thuận thông qua một quy trình được gọi là "xác nhận có chọn lọc", trong đó những người dùng đã biết xác minh các giao dịch. Chỉ các thành viên có quyền truy cập và quyền đặc biệt mới có thể duy trì sổ cái giao dịch. Loại mạng này yêu cầu nhiều kiểm soát nhận dạng và truy cập hơn.

Khi xây dựng một ứng dụng blockchain, điều quan trọng là phải đánh giá loại mạng nào sẽ phù hợp nhất với mục tiêu kinh doanh của bạn. Các mạng riêng tư và được cấp phép có thể được kiểm soát chặt chẽ và thích hợp hơn vì các lý do tuân thủ và quy định. Tuy nhiên, các mạng công cộng và không được phép có thể đạt được sự phân cấp và phân phối lớn hơn.



**\* Cyberattacks and fraud**

While blockchain technology produces a tamper-proof ledger of transactions, blockchain networks are not immune to cyberattacks and fraud. Those with ill intent can manipulate known vulnerabilities in blockchain infrastructure and have succeeded in various hacks and frauds over the years. Here are a few examples:

->

Tấn công mạng và gian lận

Trong khi công nghệ blockchain tạo ra một sổ cái chống giả mạo các giao dịch, các mạng blockchain không miễn nhiễm với các cuộc tấn công mạng và gian lận. Những người có ý định xấu có thể thao túng các lỗ hổng đã biết trong cơ sở hạ tầng blockchain và đã thành công trong nhiều vụ hack và gian lận trong nhiều năm. Đây là vài ví dụ:

+ Code Exploitation

+ Stolen Keys

+ Employee Computer Hacked

+ Phishing attacks

+ Routing attacks

+ Sybil attacks

+ 51% attacks