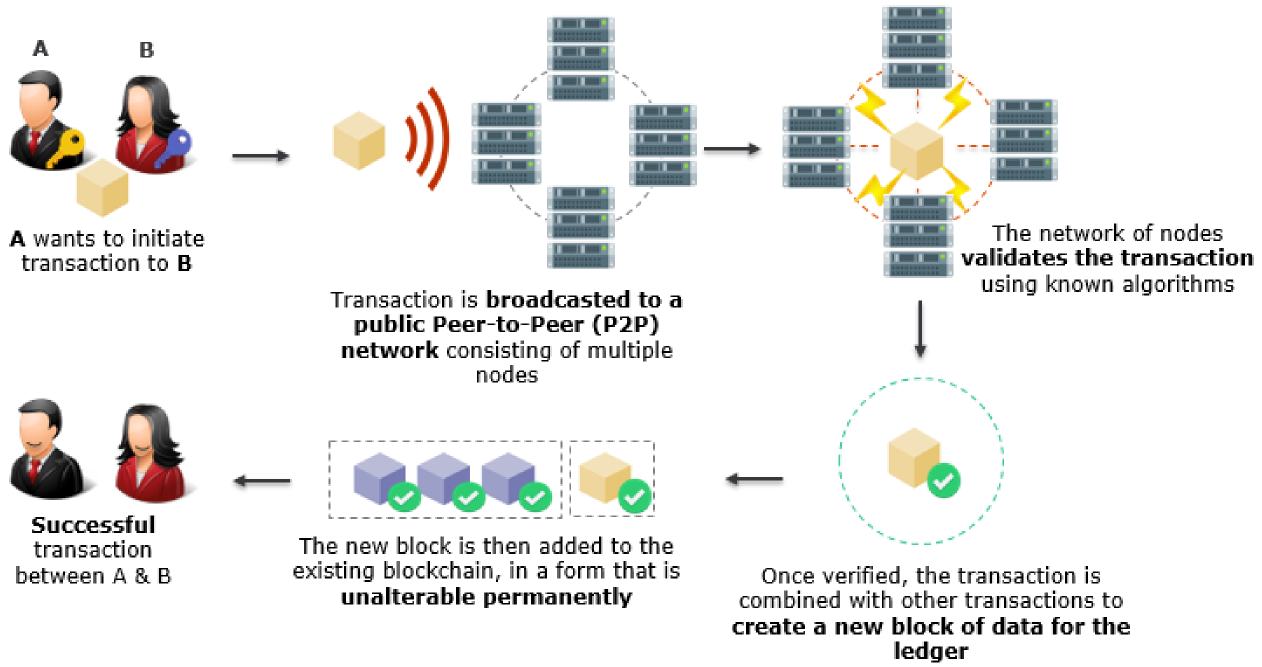
Future Blockchain Cyber Security Challenges

Blockchain is heralded as one of the most important inventions of the 21st century because it is widely seen as the future of all economic transactions—not just for monetary transactions, but for virtually everything of value.

As companies face greater data management and security challenges, blockchain may present a safer alternative than the current mechanisms that financial institutions use for peer-to-peer (P2P) transactions. More than 40 top financial institutions and a growing number of firms across industries are investing millions to experiment with blockchain-enabled distributed ledger technology.

These institutions aren't seeking just a secure and transparent way to digitally track the ownership of assets—they also want to lower the risk of sabotage and fraud. **But if blockchain is to become ubiquitous as the Internet, we must consider and incorporate cyber security principles into its implementation.**

How blockchain works:


A
B
A wants to initiate transaction to **B**
Transaction is **broadcasted to a public Peer-to-Peer (P2P) network** consisting of multiple nodes
The network of nodes **validates the transaction** using known algorithms
Once verified, the transaction is combined with other transactions to **create a new block of data for the ledger**
The new block is then added to the existing blockchain, in a form that is **unalterable permanently**
Successful transaction between A & B

Blockchain validates and facilitates secure transactions as illustrated above. We can infer that this technology can be potentially applied to any type of "peers"– transactions between individuals, organizations or government agencies.

For example, healthcare organizations are exploring blockchain concepts for peer-to-peer "transactions" to secure patient data; the supply chain industry is evaluating the use of blockchain to track the movement of assets through a manufacturer's supply chain, and for retailers to electronically initiate and enforce contracts with suppliers.

The conventional security nomenclature of blockchain is based on integrity, **but not much emphasis has been given to confidentiality and availability**. In my opinion, these areas require a more robust framework before blockchain can officially become the de facto standard for secure peer-to-peer transactions.

Potential blockchain cyber attack scenarios:

While blockchain could potentially change how we operate, we must bear in mind that **this "open distributed ledger" concept is available to consumers and malicious attackers too**. Given that all the information is made public, it's probably a matter of time before a hacker figures out how to circumvent current security measures.

Some of these vulnerabilities were outlined in a 2015 Black Hat Asia conference, where Kaspersky Labs and INTERPOL presented a live demonstration showing how arbitrary data can be injected into a digital currency decentralized database.

Blockchain attacks could be accomplished through:

- **User identify theft:** Malicious attackers could steal someone's identity and impersonate that individual on the blockchain ecosystem to perform fraudulent transactions
- **Fraudulent sender and receiver:** Malicious attackers could set up fictitious nodes (i.e., senders/receivers) and sabotage transactions
- A**sset/node theft or impersonation:** Malicious attackers could compromise a user's mobile phone/computer and impersonate the victim's role as a node to facilitate fraudulent transactions
- **Targeting of Bitcoin miners:** Malicious attackers will most certainly target Bitcoin miners given the level of privilege access that miners have; there are already cases of Bitcoin-mining malware received by miners via malicious downloads or social media
- **Availability of distributed nodes:** Malicious attackers could sabotage transactions by conducting "denial of service" attacks on the blockchain ecosystem and its applications to bring the service down
- **Injection of malicious code into a distributed ledger:** As demonstrated by Kaspersky Labs and INTERPOL, malicious code can be injected into nodes and propagate the rest of the network
- **Reputational risk:** The blockchain ecosystem will be built on the values of trust and integrity; malicious attackers could deliberately compromise the data in a few instances, causing consumers to lose confidence and

potentially leading to the catastrophic collapse of the entire system

- **Target reconnaissance:** The blockchain ecosystem embraces openness and everyone can see all transactions; malicious attackers could use this visibility to study the transaction behaviour of targets and develop an attack strategy
- **Bypassing the onboarding and offboarding** of nodes, users and miners could be a way for attackers to penetrate the blockchain system
- **Fictitious blockchain applications will appear** to steal transaction details/personal information/behaviour from nodes/individuals

For blockchain to fulfil its potential, it must first achieve widespread adoption. Gaining consumer trust will be one key driver, along with productivity and usability. Trust can only be instilled when consumers have peace of mind that the system is reliable and secure—and a blockchain with robust cyber security will most certainly achieve that. Measures to accomplish that goal include:

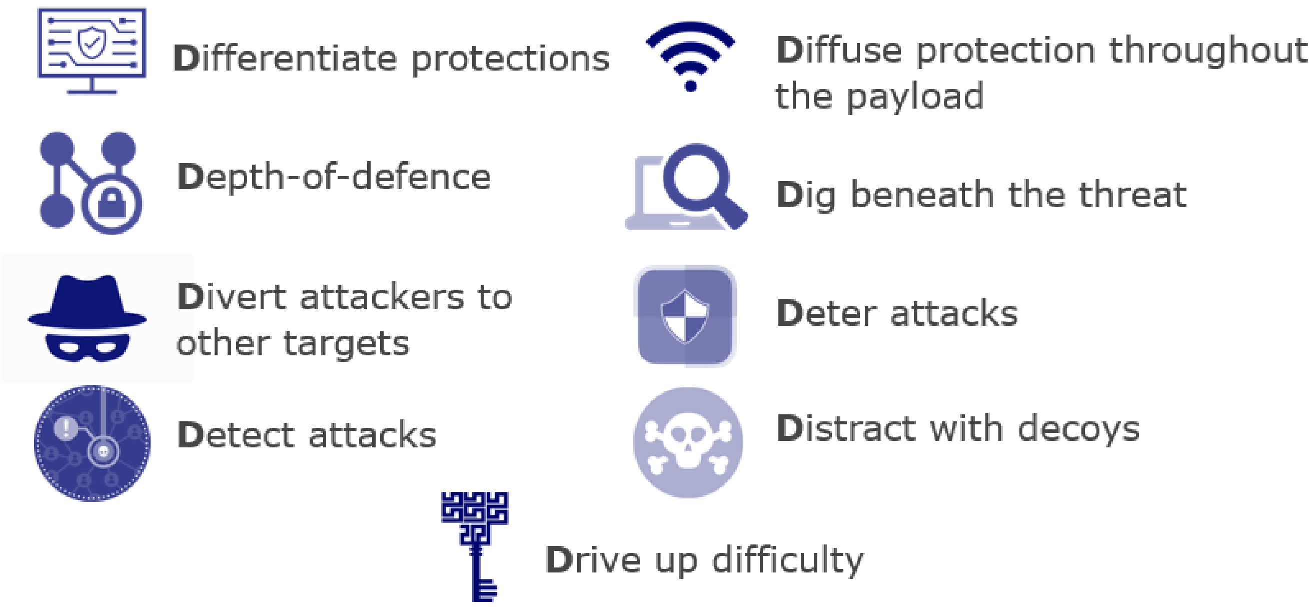
5-layer model of cyber security:

- Application layer/user access
- Operation system interface/system calls
- Operating system kernel, OS primary functionality
- Hardware interface/firmware/BIOS, boot kernel
- Hardware, CPUs, memory, interposers

Payload vs. protection

The payload can be defined as the functionality that is available to authorized users; protection is the control measures that ensure both trustworthy operation of the functionality and the functionality itself.

9 “Ds”of cyber security



Differentiate protections

Diffuse protection throughout the payload

Depth-of-defence

Dig beneath the threat

Divert attackers to other targets

Deter attacks

Detect attacks

Distract with decoys

Drive up difficulty

While the technology surrounding built into blockchain is going through a rapid “grow, learn and adapt” phase, I am positive that we are not far from witnessing how blockchain can bring about positive impacts to our society.