# Part 1: Intro to Blockchain

***By: Dr. Abdelhak Lefilef***

# Intro

- **History**:

- 1991: Stuart Haber described the first blockchain.
- 1998: Nick Szabo worked on the mechanism for digital currency.
- 2000: Stefan Konst published a general theory on the set of solutions for implementation.
- 2008: Santoshi Nakamoto First conceptualized blockchain.
- 2009: The Bitcoin network begins.
- 2013: Bitcoin really took off.
- 2016: ICICI Bank executes India's first transaction on blockchain.

# Intro

- **التاريخ:**
- **1991: أول وصف لفكرة البلوك تشين**

في عام 1991، قام ستيوارت هيبر بتقديم فكرة أولية عن "البلوك تشين". الفكرة كانت تتعلق بتسجيل المعلومات بطريقة آمنة جداً تمنع أي شخص من التلاعب بها.

- **1998: تطوير العملة الرقمية**

في عام 1998، بدأ نيك زابو العمل على آلية لعمل "العملة الرقمية"، وهي شكل من المال الذي يمكن تبادله عبر الإنترنت بدون الحاجة إلى بنوك أو وسطاء.

- **2000: نظريات جديدة للبلوك تشين**

في عام 2000، نشر ستيفان كونست نظريات حول كيفية بناء وتنفيذ "البلوك تشين" بشكل أفضل، حيث كان يدرس الطرق الممكنة لتطبيق الفكرة في الواقع.

- **2008: بداية مفهوم البلوك تشين الحديث**

في عام 2008، قام ساتوشي ناكاموتو بطرح فكرة "البلوك تشين" بشكل أوضح وأكثر تحديداً. هذه الفكرة أصبحت الأساس لظهور العملات الرقمية مثل "البيتكوين".

- **2009: بدء تشغيل شبكة البيتكوين**

في عام 2009، تم إطلاق أول شبكة "بيتكوين" بناءً على فكرة "البلوك تشين". كانت هذه بداية العملات الرقمية التي نعرفها اليوم.

- **2013: انطلاق البيتكوين بقوة**

في عام 2013، بدأت قيمة "البيتكوين" بالارتفاع، واهتم الكثيرون بهذا النوع الجديد من العملات الرقمية.

- **2016: أول معاملة بلوك تشين في الهند**

في عام 2016، قام بنك ICICIفي الهند بتنفيذ أول معاملة باستخدام تقنية "البلوك تشين". كانت هذه خطوة كبيرة لاستخدام البلوك تشين في الأعمال المصرفية.

- هذه هي الخطوات الرئيسية في تاريخ "البلوك تشين" وكيف تطورت مع الوقت.

# What is the Blockchain

- Before starting to know the meaning of Blockchain, we should know the types of networks.
- Network types:
  - Centralized Network
  - Decentralized Network
  - Distributed Network

# ماهو البلوك تشين ؟

- قبل أن نعرف ما هو "البلوك تشين"، يجب أن نفهم أنواع الشبكات:

1. **الشبكة المركزية Centralized Network :**

في هذه الشبكة، يكون هناك نقطة مركزية أو جهاز مركزي يتحكم بكل المعلومات ويتحكم في عملية تبادل البيانات بين المستخدمين. مثال على ذلك: البنوك التي تدير الأموال بشكل مركزي، حيث يعتمد الجميع على البنك لإتمام المعاملات.

2. **الشبكة اللامركزية Decentralized Network:**

في هذه الشبكة، لا توجد نقطة مركزية واحدة تتحكم في كل شيء. بدلاً من ذلك، يكون هناك العديد من العقد (أجهزة) التي تشارك في التحكم وتبادل المعلومات. كل عقدة يمكنها العمل بشكل مستقل، ولكنها تتعاون مع العقد الأخرى. مثال: بعض الأنظمة المصرفية الحديثة أو تطبيقات العملات الرقمية.

3. **الشبكة الموزعة Distributed Network:**

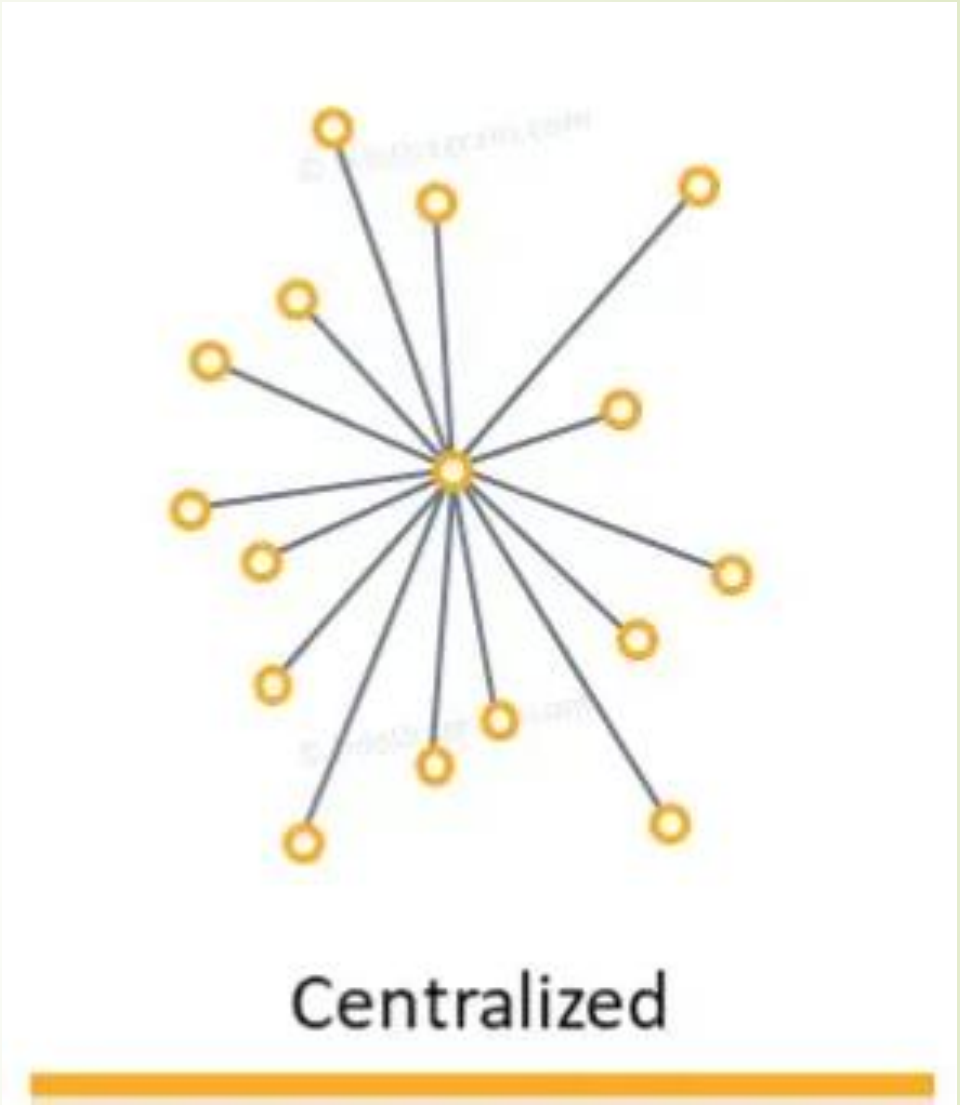
في الشبكة الموزعة، تكون البيانات موزعة على عدة أماكن أو أجهزة، ولا تعتمد على جهاز أو نقطة واحدة. جميع الأجهزة تعمل معاً لتبادل البيانات بدون نقطة تحكم واحدة. مثال: شبكة "البلوك تشين"، حيث يتم تخزين المعلومات على العديد من الأجهزة حول العالم بدلاً من مكان واحد.

- **ما هو البلوك تشين؟**

"البلوك تشين" هو نوع من الشبكات الموزعة. يعني أنه سجل أو دفتر رقمي يتم تخزينه عبر عدة أجهزة حول العالم. هذا الدفتر يسجل المعاملات بطريقة آمنة وشفافة، ولا يمكن تعديل هذه المعاملات بعد تسجيلها. يتم توزيع هذه البيانات على جميع المستخدمين في الشبكة لضمان عدم التلاعب بها.

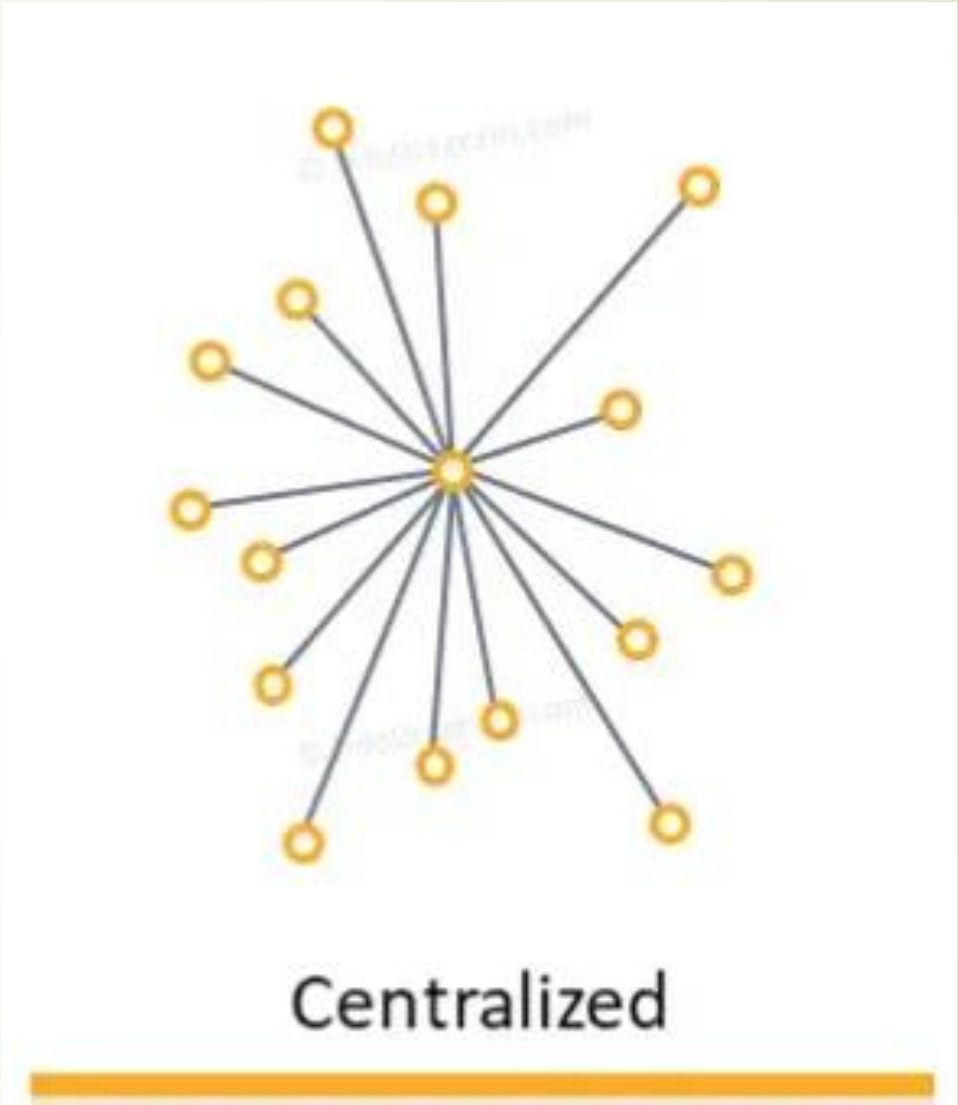
# Centralized Network

- A centralized system has a central node that controls other components communication in the system.
- Only special users can access the history of transactions or confirm the new one.



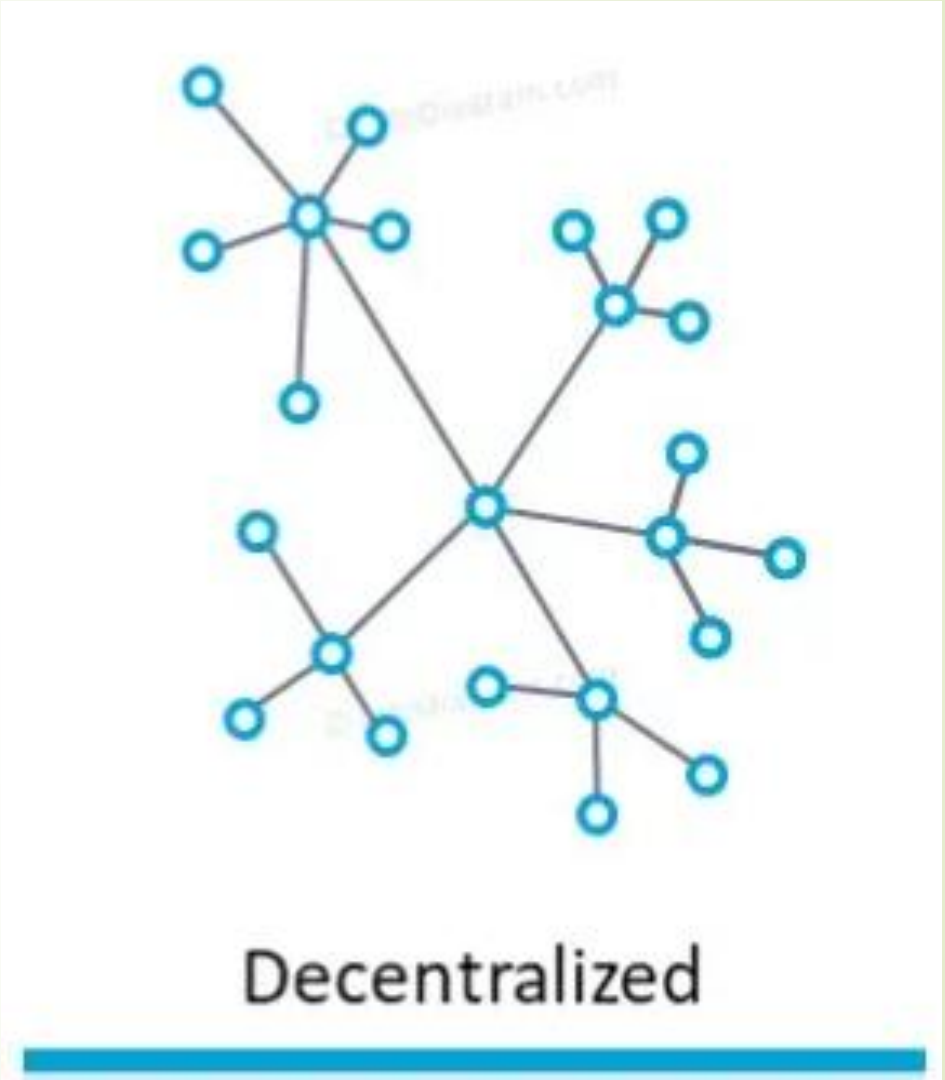
# الشبكة المركزية

- حيث يوجد جهاز أو عقدة مركزية تقوم بالتحكم في بقية المكونات والتواصل بينها. في هذا النوع من الشبكات، يتم التحكم بالبيانات من نقطة مركزية، ولا يستطيع الوصول إليها أو التحقق من صحة المعاملات سوى المستخدمين المخصصين لذلك.



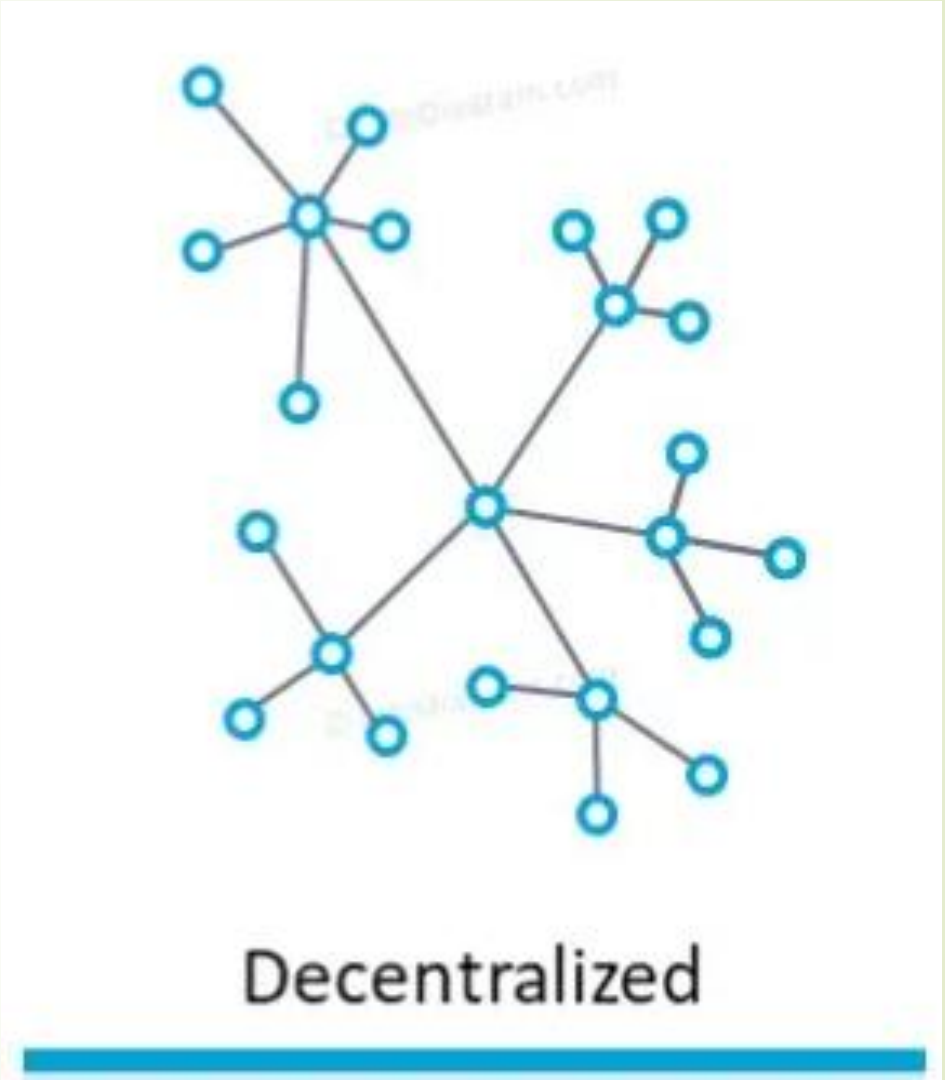
# Decentralized Network

- A decentralized system is connection of several component groups operating independently locally.
- Every participant in the network can access the history of transactions or confirms new one.



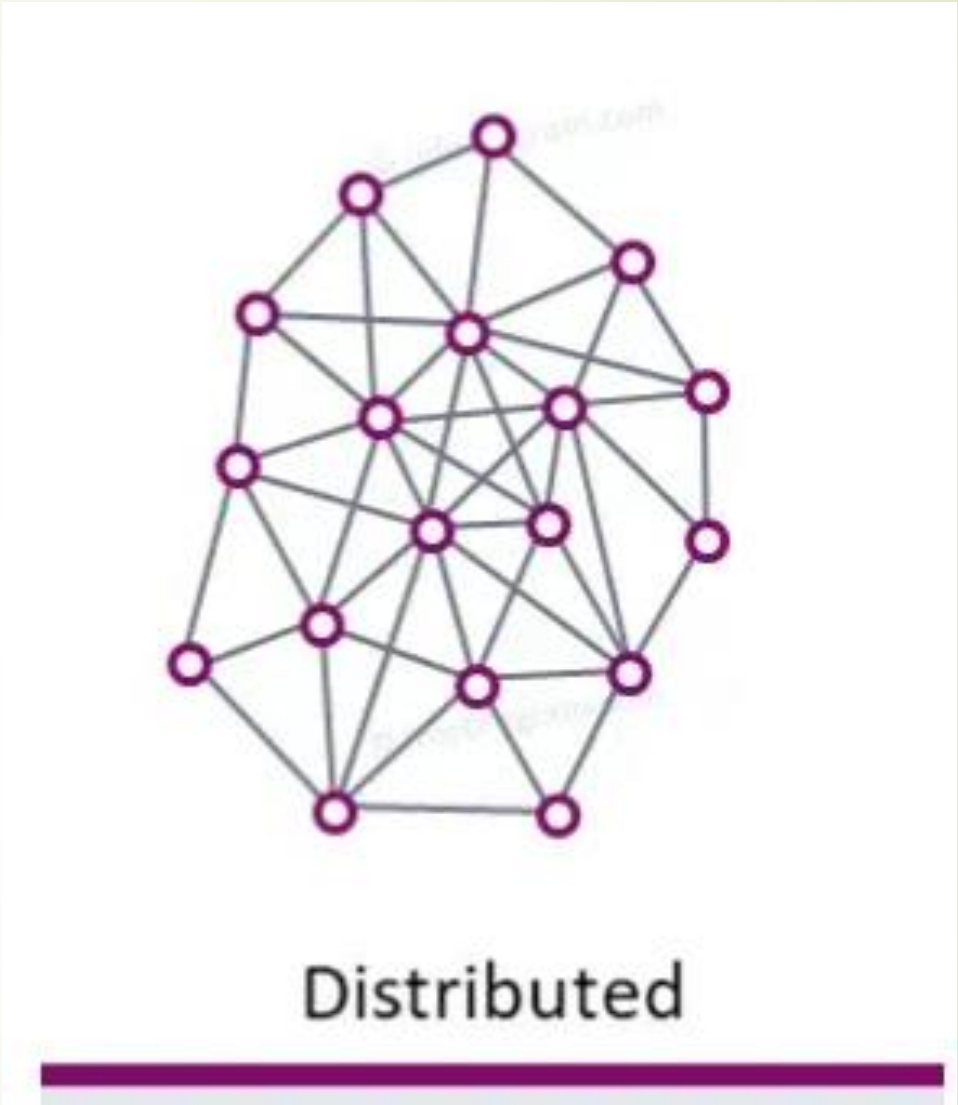
# الشبكة اللامركزية

- الشبكة اللامركزية هي نوع من الشبكات التي لا تعتمد على نقطة واحدة للتحكم أو الإدارة. بدلاً من ذلك، تتكون من عدة أجزاء أو مجموعات صغيرة تعمل بشكل مستقل عن بعضها البعض.مثال على ذلك هو الإنترنت، حيث لا يوجد مركز واحد يتحكم في جميع البيانات، ولكن يمكن لكل مستخدم الوصول إلى المعلومات والمشاركة في الشبكة بشكل مباشر.في هذه الشبكة، كل مشارك (أو جهاز) يمكنه الوصول إلى تاريخ العمليات (مثل المعاملات المالية أو البيانات) ويمكنه أيضاً تأكيد العمليات الجديدة، وهذا يعزز الشفافية والأمان.باختصار، الشبكات اللامركزية تجعل النظام أكثر قوة لأنه لا يعتمد على مكان واحد يمكن أن يفشل فيه، وكل شخص في الشبكة يمكنه أن يساهم في تشغيلها.



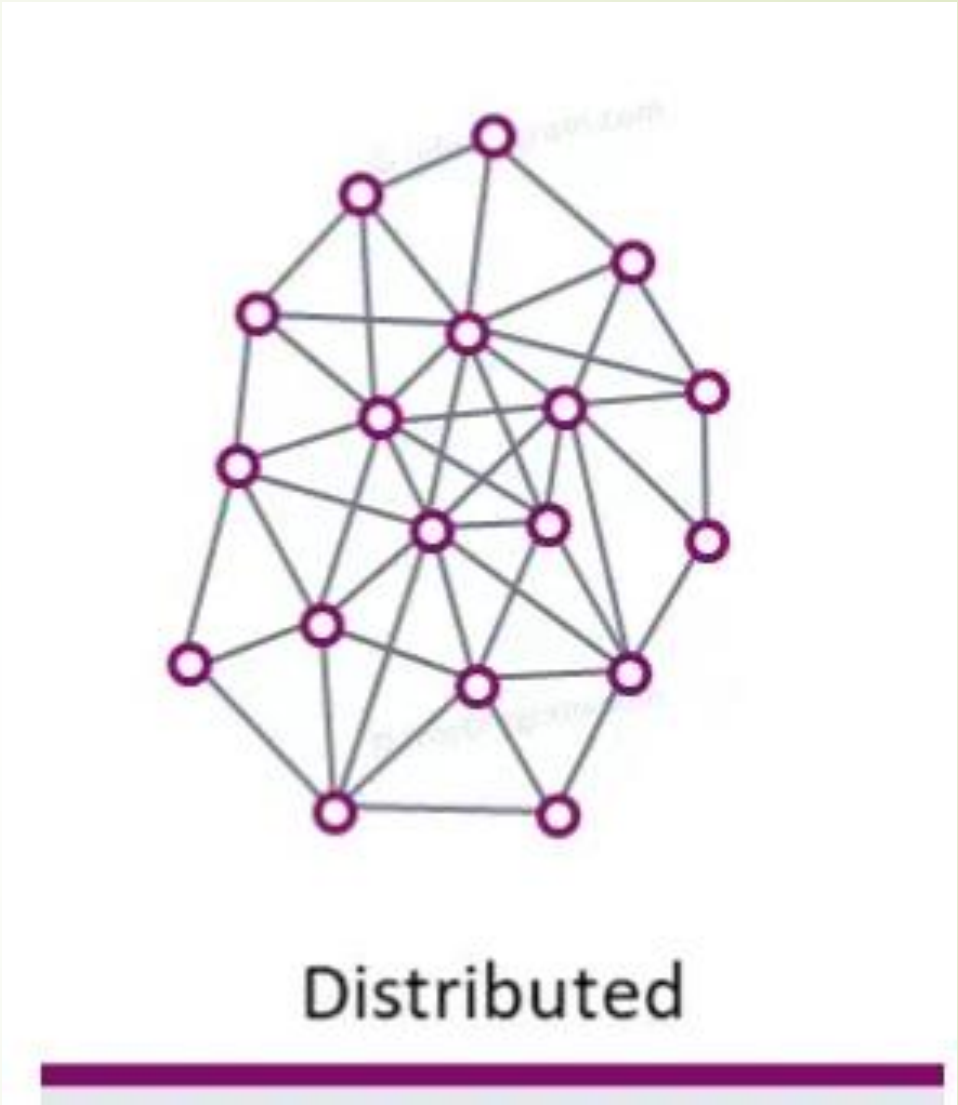
# Distributed Network

- Distributed systems are similar to decentralized systems in that they do not have a single point of control over the system since components are spread across multiple components.
- Distributed system has components located on different network computers. There is no global control and, thus, no single point of failure.



# الشبكة الموزعة

- الشبكة الموزعة تشبه إلى حد كبير الشبكة اللامركزية التي شرحناها سابقًا. الفكرة الأساسية هي أنه لا يوجد مركز تحكم واحد في النظام، ولكن المكونات (الأجزاء) موزعة على عدة أماكن أو حواسيب مختلفة. بمعنى آخر، المعلومات والبيانات موجودة في عدة حواسيب على الشبكة، وليس هناك مكان واحد يسيطر على كل شيء. وهذا يعني أن النظام لا يتأثر كثيرًا إذا تعطل جزء واحد منه، لأنه باقي الأجزاء تستمر في العمل. النظام الموزع هو طريقة ممتازة لجعل الشبكة أكثر أمانًا وقوة، حيث لا يوجد نقطة واحدة يمكن أن تفشل وتؤدي إلى انهيار النظام بأكمله.



# Blockchain

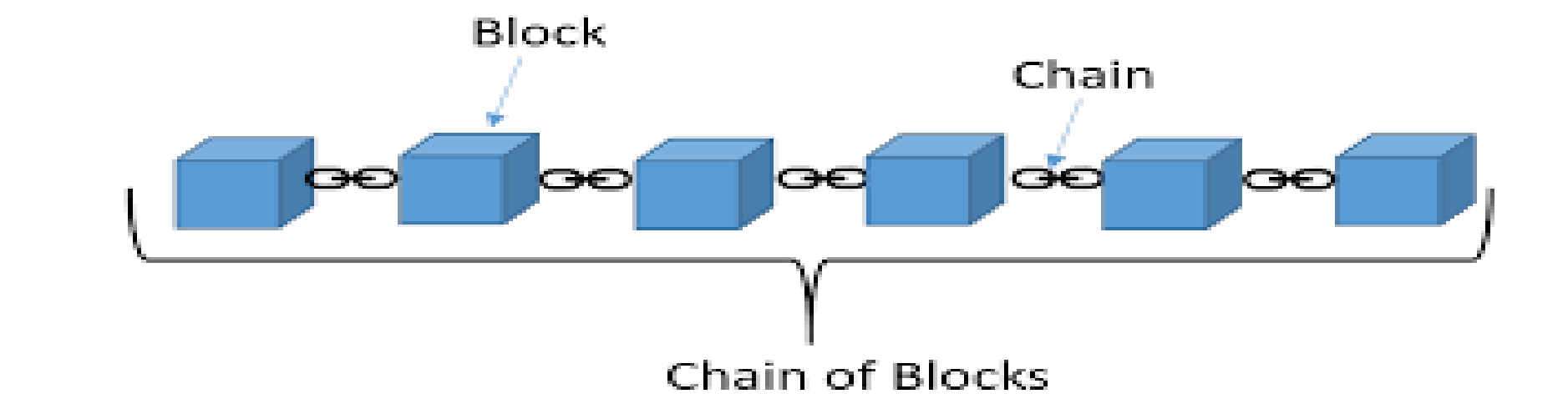
- Blockchain is a chain of data records that are distributed across a decentralized network of computers (peers), meaning that there is no central authority or single point.
- Each "block" contains data, and blocks are linked in a chronological "chain.“
- It is best known for its crucial role in cryptocurrency systems, maintaining a secure and decentralized record of transactions, but it is not limited to cryptocurrency uses.
- Blockchains can be used to make data in any industry immutable, meaning it cannot be altered.
- Since a block can’t be changed, the only trust needed is when a user or program enters data. This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make

# البلوكتشين

- البلوكتشين هو سلسلة من البيانات أو السجلات التي يتم توزيعها على شبكة لامركزية من الحواسيب. هذا يعني أنه لا يوجد مركز أو جهة واحدة تتحكم في هذه السجلات. كل "كتلة" block تحتوي على بيانات معينة، وتكون هذه الكتل مرتبطة ببعضها البعض بشكل تسلسلي لتكوين سلسلة. هذا يجعل البيانات مسجلة بطريقة يصعب تغييرها. البلوكتشين مشهور في الأنظمة الخاصة بالعملات الرقمية مثل البيتكوين، حيث يُستخدم لتسجيل العمليات المالية بشكل آمن وشفاف. ولكن استخداماته لا تقتصر على العملات الرقمية فقط، بل يمكن استخدامه في أي مجال لضمان أن البيانات لا يمكن تغييرها. عندما يتم إضافة كتلة جديدة، لا يمكن تعديلها، وهذا يزيل الحاجة إلى وجود طرف ثالث موثوق (مثل مراجع حسابات) للتأكد من صحة البيانات. هذا يقلل من التكلفة ويزيد من الثقة في النظام.

# البلوكتشين Blockchain

- كما ترى، البلوكتشين يتكون من "كتل"Blocks، وكل كتلة تحتوي على بيانات معينة. هذه الكتل متصلة ببعضها البعض عبر روابط لتشكيل سلسلة من الكتل Chain of Blocks الفكرة هنا هي أن كل كتلة تكون مرتبطة بالكتلة التي تسبقها، وهذا يجعل من الصعب تغيير أو تعديل أي كتلة لاحقة دون تعديل كل الكتل التي تأتي بعدها. هذه السلسلة تجعل البلوكتشين وسيلة آمنة لتخزين البيانات، حيث أن أي محاولة لتغيير البيانات في كتلة معينة ستظهر في النظام بأكمله.



# The Structure of Blockchains

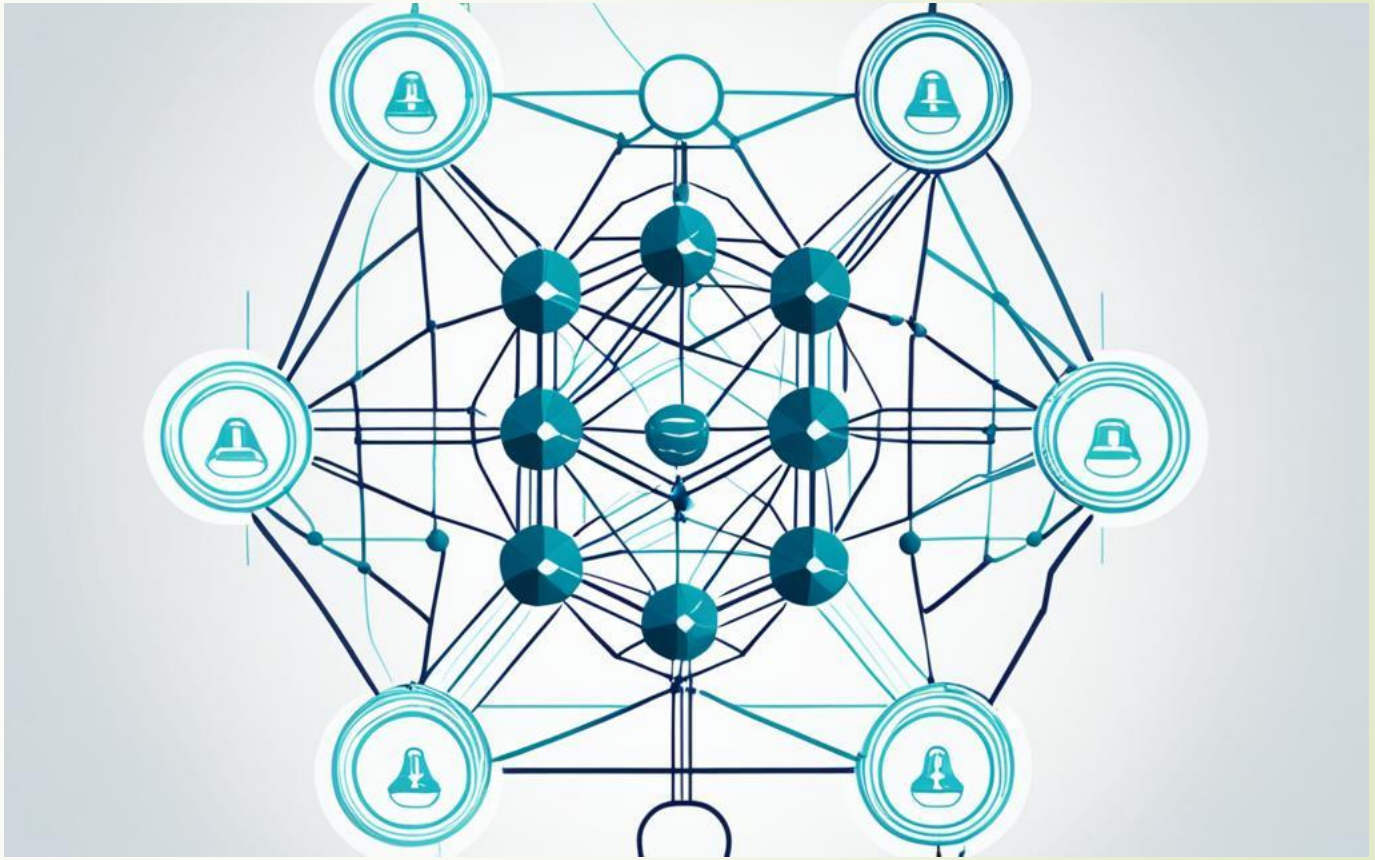
**Block**

**Chain**

**Network**

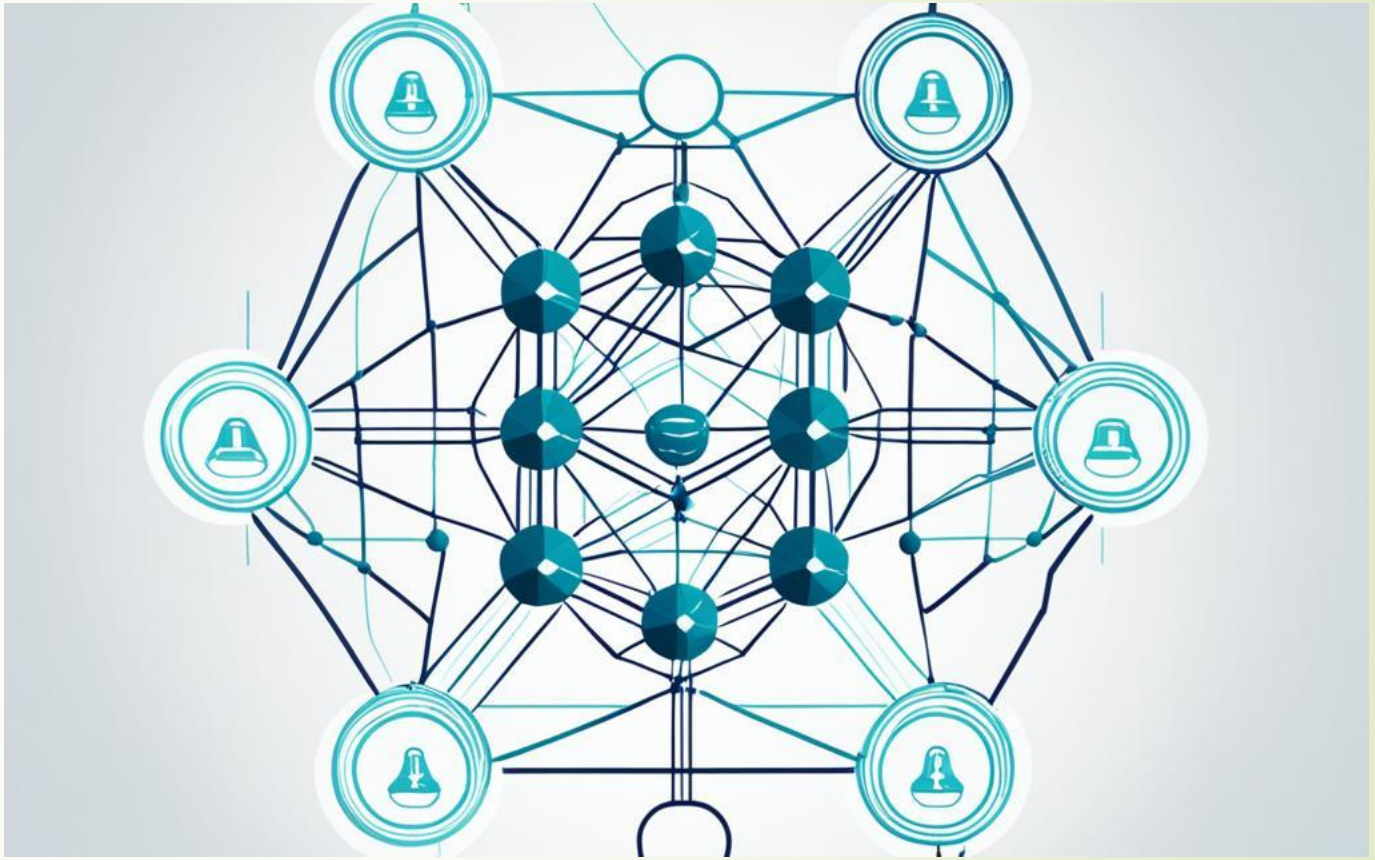
# What is the network?

- The network is composed of “full nodes.” Each node contains a complete record of all the transactions recorded in that blockchain.
- The nodes are everywhere, and anyone can run them. Operating a full node is difficult, expensive, and time-consuming.

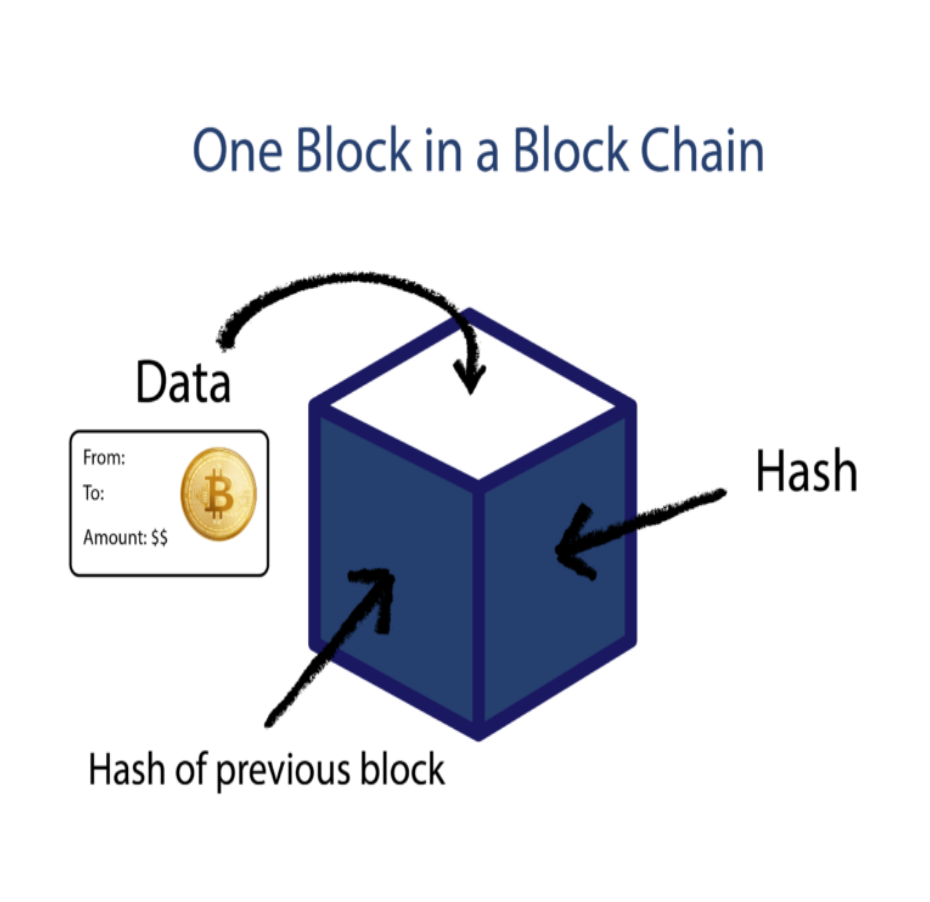


# ما هي الشبكة ؟

- الشبكة تتكون من ما يسمى "العُقد الكاملة" Full Nodes كل عقدة في الشبكة تحتوي على نسخة كاملة من جميع المعاملات التي تمت في البلوكتشين. هذا يعني أن كل عقدة لديها نفس البيانات، وهذا يساهم في حماية البيانات والتأكد من عدم التلاعب بها. العقد موجودة في كل مكان، ويمكن لأي شخص أن يقوم بتشغيل عقدة. لكن تشغيل عقدة كاملة قد يكون صعبًا ويحتاج إلى موارد كبيرة مثل وقت، مال، وطاقة. باختصار، العقد هي الأجهزة التي تعمل على الحفاظ على الشبكة وتسجيل المعاملات لضمان أمان النظام وشفافيته.

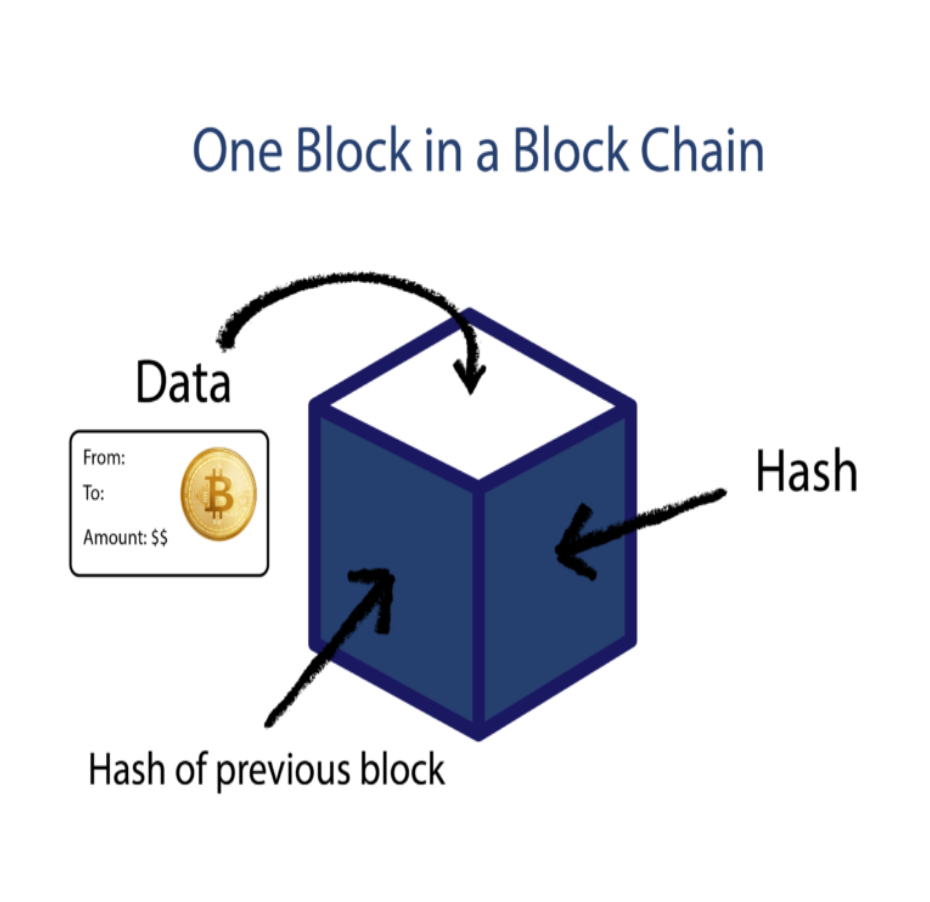


# What is a block (blockchain block)?




- A blockchain stores transaction data in blocks, which are permanent records. A block records some or all of the network's most recent unvalidated transactions. Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated.
- A block is thus a permanent store of records that, once written, cannot be altered or removed without changing all preceding or following blocks.
- The first block is called the "Genesis Block". If you tamper with block 2, it will change block 3's previous has, making the chain invalid.

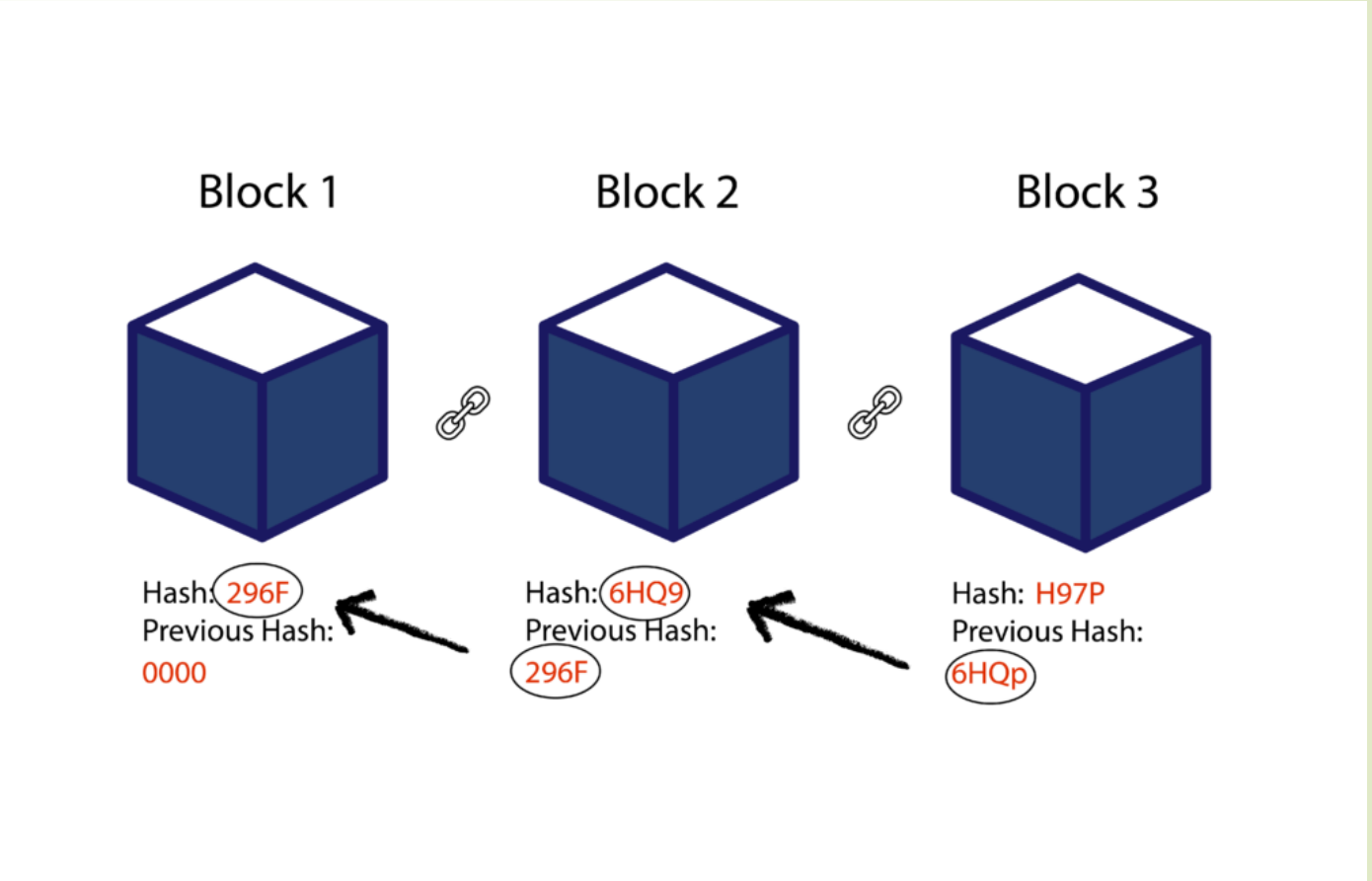
# What is a block (blockchain block)?




- الكتلة هي وحدة أساسية في البلوكتشين تحتوي على بيانات المعاملات التي تتم على الشبكة. كل كتلة تحتوي على معلومات مثل "من أرسل الأموال؟"، "إلى من؟"، و"كم المبلغ؟". بالإضافة إلى ذلك، تحتوي كل كتلة على رمز يسمى "هاش" وهو نوع من التوقيع الفريد الذي يربط الكتلة بالكتلة السابقة في السلسلة. عندما يتم التحقق من البيانات الموجودة في الكتلة، يتم إغلاقها، ولا يمكن تغييرها بعد ذلك. بعدها يتم إنشاء كتلة جديدة لتخزين معاملات جديدة. الكتلة الأولى في السلسلة تسمى "كتلة البداية" ( .(Genesis Blockإذا حاول شخص ما تعديل بيانات كتلة في منتصف السلسلة، سيتغير "الهاش" الخاص بها، وهذا سيؤدي إلى كسر السلسلة وجعلها غير صالحة. هذه الطريقة تضمن أن المعلومات الموجودة في البلوكتشين تبقى آمنة ولا يمكن تغييرها.

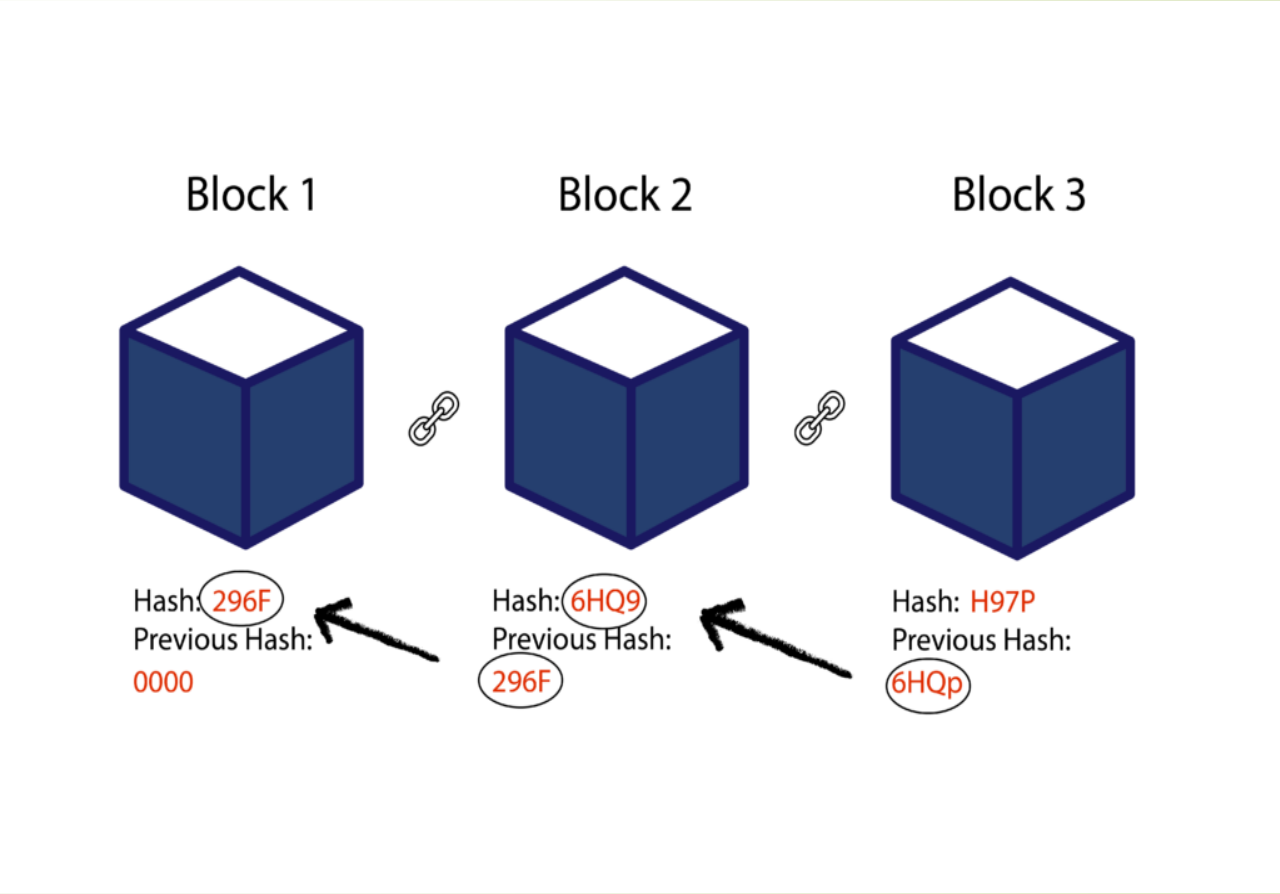
# What is a block (blockchain block)?

- **Each block holds a section of**
- **Data**
- **Hash**
- **Previous Hash**



# What is a block (blockchain block)?

- في هذه الصورة يتم توضيح ما تحتويه كل كتلة في البلوكتشين:
البياناتData : كل كتلة تحتوي على معلومات أو بيانات، مثل المعاملات أو العمليات التي تتم على الشبكة.الهاش Hash: الهاش هو رمز فريد يولد لكل كتلة، وهو يعمل كتوقيع خاص بالكتلة. إذا تم تغيير أي جزء من البيانات داخل الكتلة، سيتغير الهاش بشكل تلقائي، مما يجعل أي تغيير ملحوظًا. هاش الكتلة السابقة Previous Hashكل كتلة في البلوكتشين تحتوي أيضًا على الهاش الخاص بالكتلة السابقة لها. هذا الربط بين الكتل يجعل البلوكتشين عبارة عن سلسلة متصلة، ويضمن أنه إذا تم تغيير أي كتلة في السلسلة، فسيتغير الهاش الخاص بها والهاشات التي تتبعها، مما يؤدي إلى إبطال السلسلة.بمعنى آخر، هذه الآلية تجعل النظام أكثر أمانًا، حيث يصعب جدًا تغيير البيانات دون أن يتم كشف التغيير.



# What is the chain?

- A hash that links one block to another, mathematically “chaining” them together. This is one of the most challenging concepts in blockchain to comprehend.
- The magic also glues blockchains together and allows them to create mathematical trust.

# ماهي السلسلة

- السلسلة هي الطريقة التي يتم بها ربط الكتل معًا في البلوكتشين. يتم استخدام **الهاش** لربط كل كتلة بالكتلة التي تليها. هذا الارتباط الرياضي بين الكتل يسمى "السلسلة". وهو أحد المفاهيم المعقدة في البلوكتشين.

- هذا الربط بين الكتل هو الذي يعطي البلوكتشين قوته وأمانه. بحيث إذا تم التلاعب بكتلة واحدة، يتغير الهاش الخاص بها، مما يفسد السلسلة بأكملها. لذلك، تعتبر السلسلة أداة لإنشاء "الثقة الرياضية"، حيث يعتمد الأمان على الحسابات الرياضية وليس على شخص أو جهة معينة.

- بمعنى آخر، السلسلة تجعل البلوكتشين متماسكًا ومضمونًا، حيث يعتمد على الربط القوي بين الكتل عبر الهاش.

# Blockchain has five elements

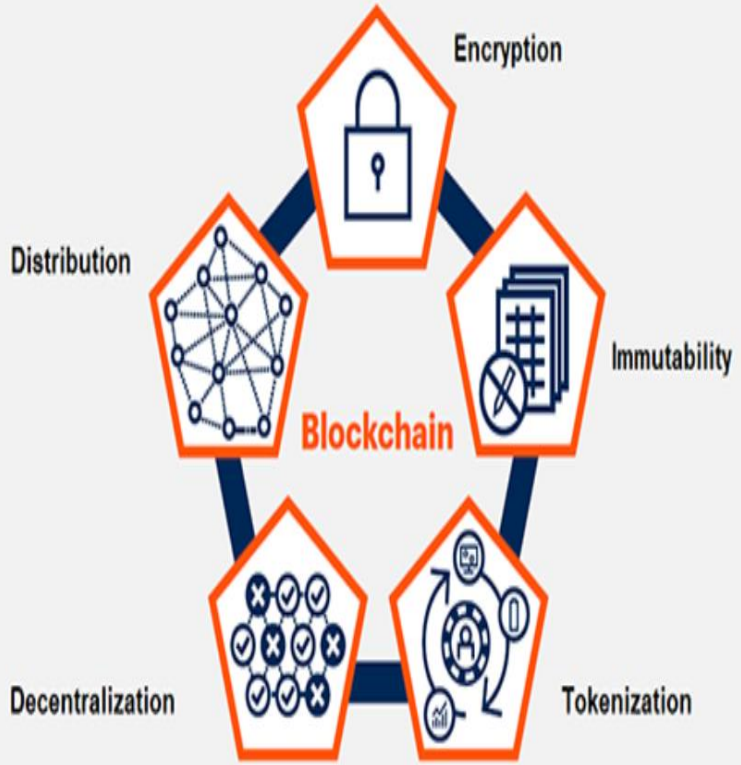
**Distribution**: Blockchain participants are located physically apart from each other and are connected on a network

**Encryption**: Blockchain uses technologies such as public and private keys to record the data in the blocks securely and semi-anonymously

**Immutability**: Completed transactions are cryptographically signed, time-stamped and sequentially added to the ledger

**Tokenization**: Transactions and other interactions in a blockchain involve the secure exchange of value

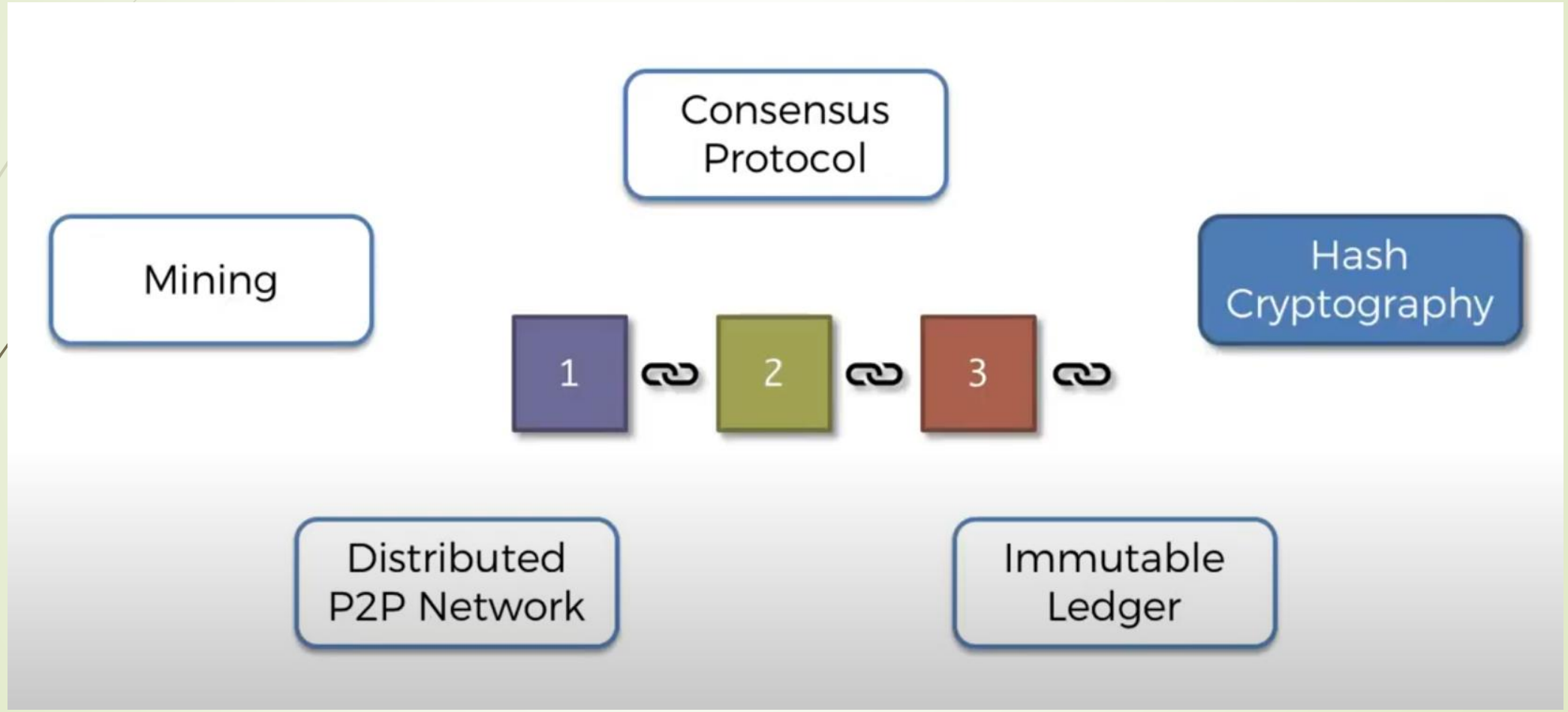
**Decentralization**: Both network information and the rules for how the network operates are maintained by nodes on the distributed network due to a consensus mechanism



# العناصر الخمسة الأساسية التي يتكون منها البلوك تشين

- في الصورة السابقة ، يتم شرح العناصر الخمسة الأساسية التي يتكون منها البلوكتشين: التوزيع **Distribution** المشاركون في البلوكتشين يكونون متواجدين في أماكن مختلفة ومتباعدة جغرافيًا، ولكنهم متصلون مع بعضهم البعض من خلال شبكة. التشفير **Encryption** يتم استخدام تقنيات التشفير مثل المفاتيح العامة والخاصة لتسجيل البيانات في الكتل بشكل آمن وشبه مجهول. عدم القابلية للتغيير **Immutability** بمجرد إكمال المعاملات في البلوكتشين، يتم توقيعها بشكل مشفر وتسجيلها مع الطابع الزمني، ولا يمكن تعديلها أو حذفها لاحقًا. اللامركزية **Decentralization** المعلومات والقواعد التي تحكم تشغيل الشبكة تُدار من قبل العقد (الحواسيب المتصلة بالشبكة)، وليس هناك جهة مركزية تتحكم بالنظام. يعتمد النظام على توافق الآراء بين المشاركين. الترميز **Tokenization** المعاملات والتفاعلات الأخرى داخل البلوكتشين تتضمن تبادل القيمة بشكل آمن من خلال الرموز أو العملات الرقمية. هذه العناصر الخمسة تجعل البلوكتشين آمنًا وشفافًا ولا مركزيًا، مما يعزز الثقة في النظام.

# The Map of Blockchain



# What's the Hash?

- A hash is generated from the data contained in each block using cryptography.
- Hashing is integral to blockchain security. It forms the basis for creating blocks, chaining them together, and generating digital signatures.
- It prevents tampering attempts, as altering a block requires recalculating the hashes of every subsequent block, a practically impossible feat that requires a lot of computing resources.
- In essence, hashing safeguards blockchain technology's transparency, trust, and security.

# What's the Hash?

- يتم إنشاء تجزئة ( Hashمن البيانات الموجودة في كل كتلة باستخدام علم التشفير، وتعتبر التجزئة جزءًا أساسيًا من أمان البلوك تشين. إذ تُمثل الأساس في إنشاء الكتل، وربطها معًا، وإنشاء التوقيعات الرقمية.
- تحمي التجزئة البلوك تشين من محاولات التلاعب، حيث إن تعديل أي كتلة يتطلب إعادة حساب التجزئات لجميع الكتل التي تليها، وهو أمر شبه مستحيل عمليًا ويتطلب موارد حاسوبية ضخمة.
  ببساطة، تضمن التجزئة شفافية وأمان وتوثيق التكنولوجيا في البلوك تشين.
- **مثال بسيط:**

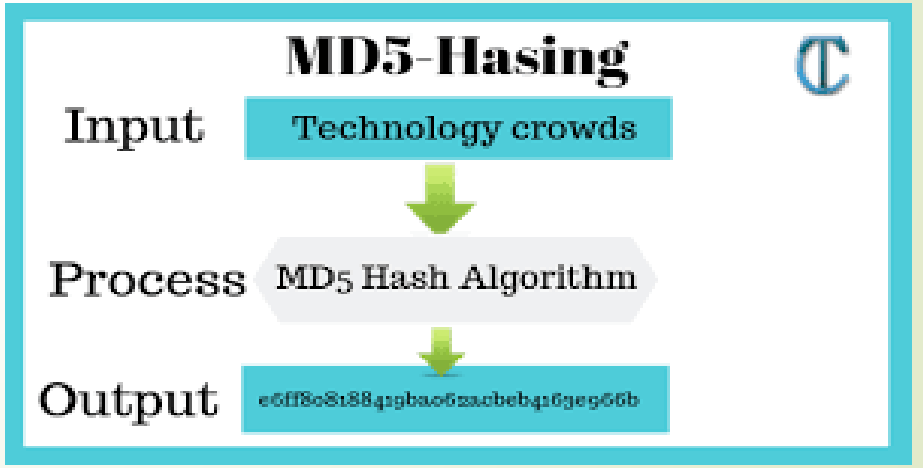
تخيل دفتر ملاحظات حيث تدون كل صفحة (تمثل كتلة) بمحتوياتها، وتوقّع على نهاية الصفحة بحرف معين (تجزئة) يمثل محتواها. إذا حاول أحد تغيير محتوى صفحة، فعليه تعديل الحرف في تلك الصفحة، وأيضًا على الصفحات التالية كي يبقى التسلسل منطقيًا، مما يجعل التلاعب بالمحتوى صعبًا للغاية.

# The security level of hash functions

- The current hash functions have a high level of security, but this does not mean they are infallible.

An excellent example of this is:

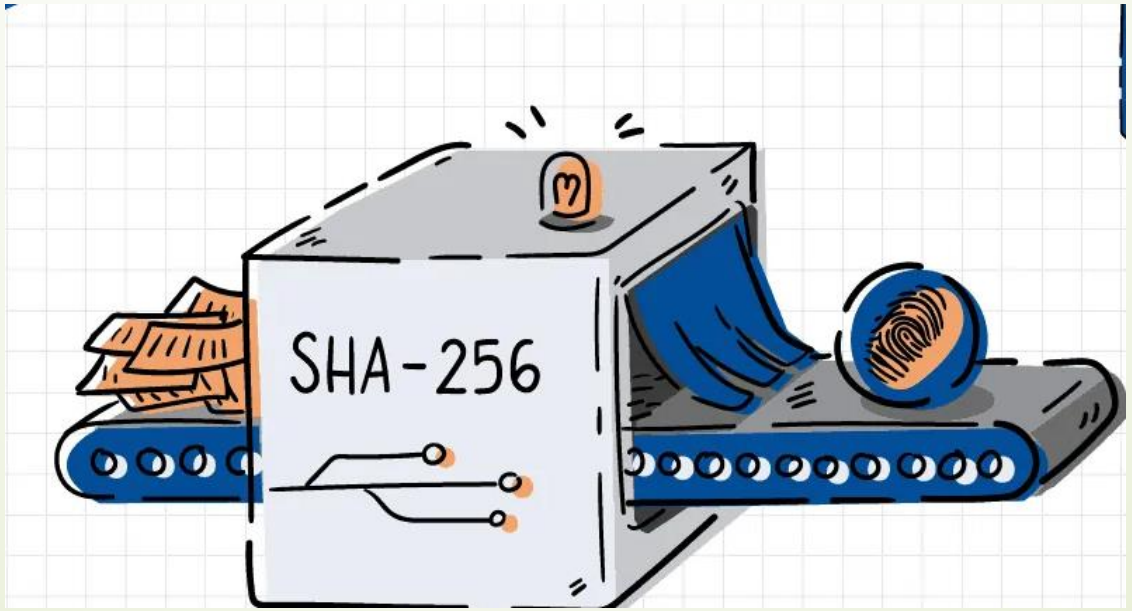
**1- The MD5 hash function.** The specifications promised very high security in principle. Its use spread on the Internet due to the need for a hashing system to maintain its security. But in 1996, the function's security could be broken. This made it obsolete, and it was recommended that it be abandoned.



# The security level of hash functions

**2- Functions RIPE MD-160 and SHA-256.** They are so complex that their safety is still guaranteed. For example, it is estimated that using current supercomputers would take thousands of years to break SHA-256's security.

The same applies to RIPE MD-160 and its consequent evolutions. This means both functions still provide high security and can be used without problems.



# SHA-256 Hash Algorithm

- The National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) jointly introduced SHA-256, a secure hash algorithm that belongs to the SHA-2 algorithm family, in 2001.
- Hash function converts text of any length to an almost-unique alphanumeric string of 256 bit.
- **Initialization:**

The initial hash values (eight 32-bit words) are set. These values are defined in the SHA-256 specification.

- **Processing in Blocks:**

Divide the padded message into 512-bit blocks. For each block, perform a series of bitwise operations, modular additions, and logical functions using the current hash value and the block.

- **Compression Function:**

A compression function is applied to each block, creating a new hash value. This function involves mixing the bits of the current hash value and the message block.

- **Iteration:**

Repeat the compression function for each block, using the output of each iteration as input for the next.

# SHA-256 Hash Algorithm

- **خوارزمية التجزئة SHA-256**

- قامت وكالة الأمن القومي الأمريكية ( (NSAوالمعهد الوطني للمعاييروالتكنولوجيا ( (NISTبتقديم خوارزمية SHA-256، وهي خوارزمية تجزئة آمنة تنتمي إلى عائلة خوارزميات SHA-2، في عام 2001.
- تقوم دالة التجزئة بتحويل أي نص إلى سلسلة أبجدية رقمية شبه فريدة بطول 256 بت.

- التفاصيل التقنية:

1. **التهيئة:**
   يتم تعيين قيم التجزئة الأولية (ثمان كلمات بطول 32 بت لكل منها) ويتم تعريف هذه القيم في مواصفات .SHA-256
2. المعالجة في كتل:
   يتم تقسيم الرسالة المحشوة إلى كتل بطول 512 بت. لكل كتلة، تُنفذ مجموعة من العمليات على مستوى البت، وجمعات معيارية، ودوال منطقية باستخدام قيمة التجزئة الحالية والكتلة.
3. **دالة الضغط:**
   تُطبق دالة ضغط على كل كتلة، مما يولد قيمة تجزئة جديدة. تتضمن هذه العملية خلط بتات قيمة التجزئة الحالية مع بتات الكتلة.
4. **التكرار:**
   يتم تكرارعملية الضغط لكل كتلة، حيث يُستخدم ناتج كل تكراركمدخل للتكرار التالي.

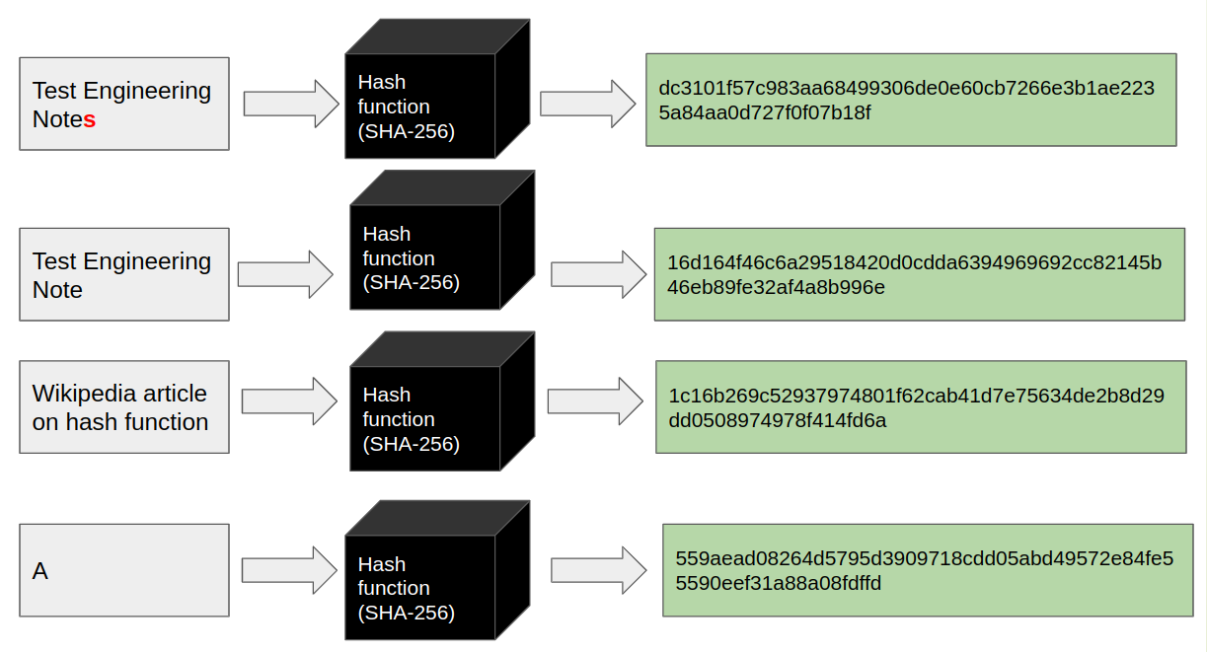
- **مثال بسيط:**
  تخيل أن لديك سلسلة من الحلقات، كل حلقة (كتلة) مكونة من رموزفريدة. عند تجميع هذه الحلقات بشكل متتابع، يتم تحويلها إلى سلسلة ثابتة، وفي حال أراد أحدهم تغييررمزفي إحدى الحلقات، سيتعين عليه تغييرجميع الحلقات الأخرى لتحقيق تناسق في السلسلة.

# SHA-256 Hash Algorithm

- **Output:**

The final hash value after processing all blocks becomes the SHA-256 hash of the original message.

This process involves many complex bitwise operations and transformations. The resulting SHA-256 hash for our simplified example would be a 256-bit, 64 hexadecimal characters.



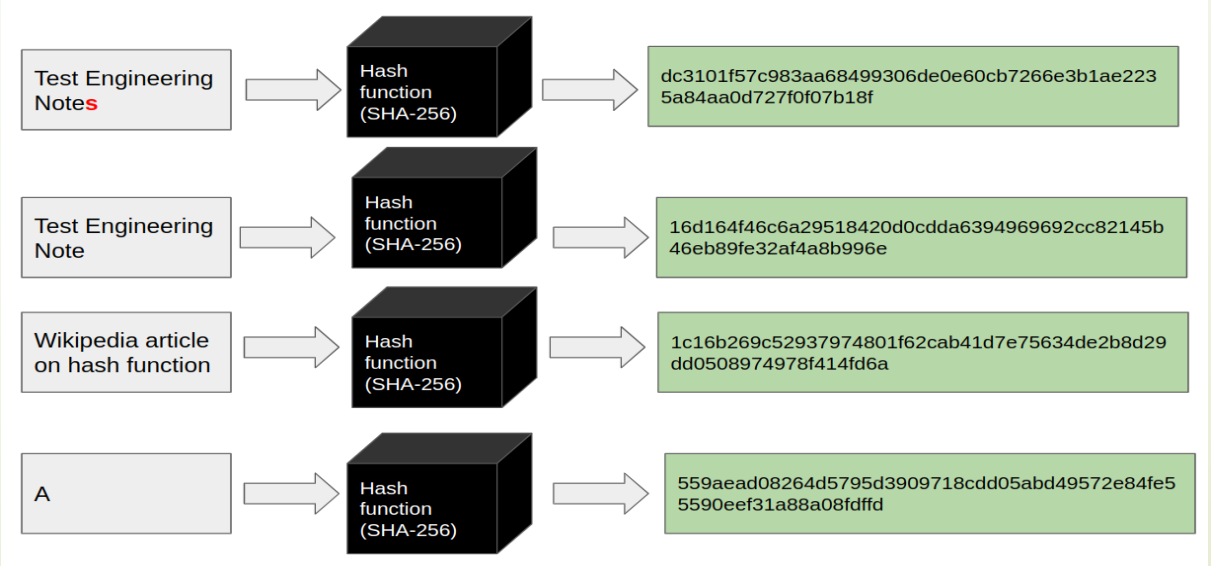
# SHA-256 Hash Algorithm

- خوارزمية التجزئة SHA-256
- **الناتج:**

القيمة النهائية للتجزئة بعد معالجة جميع الكتل تصبح هي تجزئة SHA-256للرسالة الأصلية.

- تتضمن هذه العملية العديد من العمليات المعقدة على مستوى البتّات وتحويلات مختلفة. الناتج النهائي لتجزئة SHA-256يكون بطول 256 بت، وهو ما يعادل 64 حرفًا بنظام العد السداسي العشري (.hexadecimal)
- **شرح بسيط:**

تخيل أن لديك نصوصًا مختلفة، وعندما تقوم بإدخال كل نص في دالة التجزئة SHA-256، تحصل على سلسلة فريدة من الأحرف (مثل البصمة). أي تغيير بسيط في النص المدخل سيؤدي إلى تغيير كامل في سلسلة الناتج، مما يجعلها أداة قوية للتحقق من سلامة البيانات.



# Characteristics of Hash Algorithm

- Among the main characteristics of the hash algorithm, the following can be mentioned:

- **One-Way.**
- **Deterministic.**
- **Fast Computation**.
- **The Avalanche effect.**
- **Must withstand collision.**

# Characteristics of Hash Algorithm

- **خصائص خوارزمية التجزئة**: من بين الخصائص الرئيسية لخوارزمية التجزئة يمكن ذكر ما يلي:**اتجاه واحد (One-Way)**:يعني أن من السهل توليد التجزئة من البيانات الأصلية، لكن من الصعب أو المستحيل استعادة البيانات الأصلية من التجزئة.حتمية (:(Deterministicيعني أن نفس المدخلات تعطي دائمًا نفس التجزئة، مما يضمن التناسق. **حساب سريع** (:(Fast Computation يجب أن تتم العملية بسرعة، بحيث لا تؤثر على الأداء. **تأثير الانهيار ( Avalanche Effect)**:أي تغيير بسيط في المدخلات يجب أن يؤدي إلى تغيير كبير في التجزئة، مما يزيد من الأمان. **مقاومة التصادم ( Must withstand collision)** :يجب أن تكون الخوارزمية مصممة بحيث يصعب إيجاد مدخلين مختلفين ينتجان نفس التجزئة

- **مثال بسيط**: تخيل قفلًا يمكنك فتحه بمفتاح معين (اتجاه واحد)، وكل مرة تضع نفس المفتاح، يُفتح القفل (حتمية). القفل يفتح بسرعة (حساب سريع)، وإذا قمت بتغيير بسيط في المفتاح، لن يعمل على الإطلاق (تأثير الانهيار)، ويجب أن يكون هناك أمان ضد إمكانية فتح القفل بمفتاح آخر مشابه (مقاومة التصادم).

# Characteristics of Hash Algorithm

- **One-Way:**

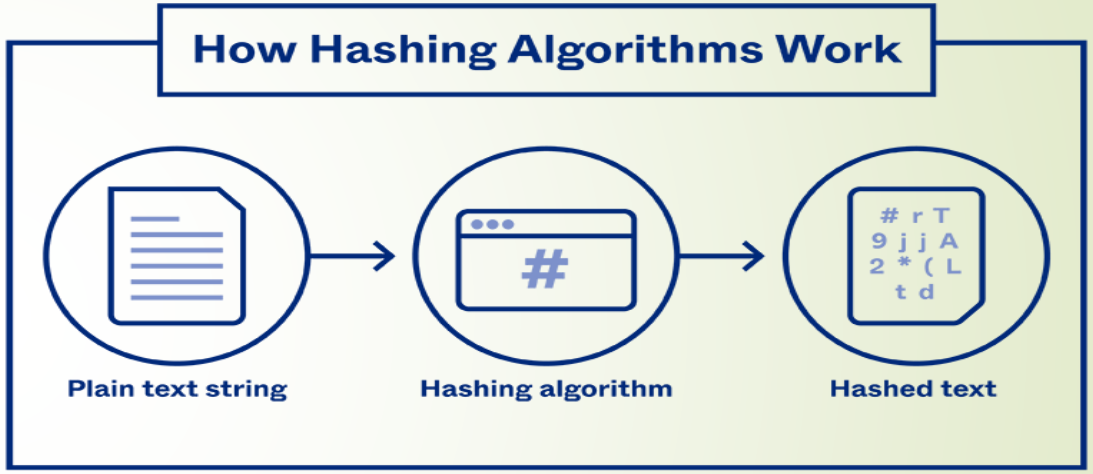
Once transformed by the algorithm, it's nearly impossible to revert the data to its original state.

- **Deterministic:**

The hash algorithm always produces the same output when given the same input, meaning that a specific input will consistently deliver the same hash value.

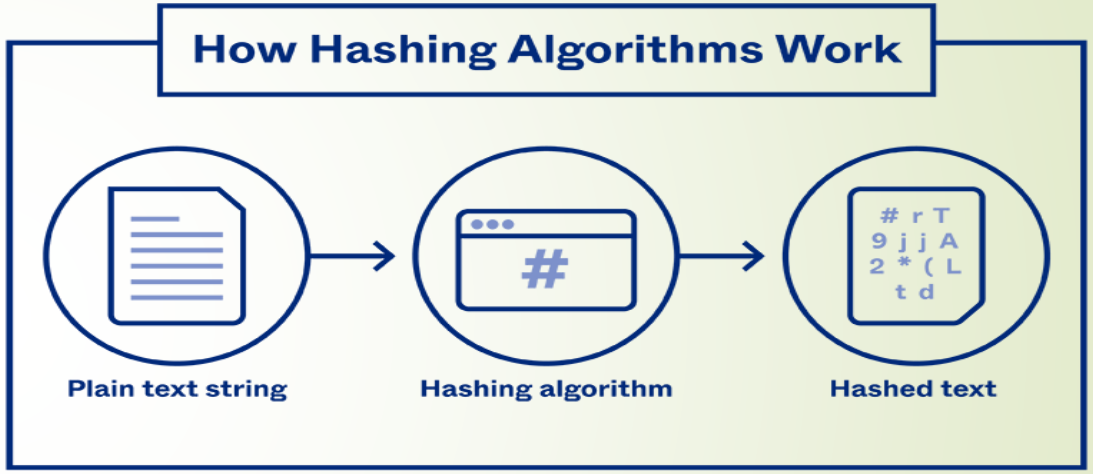
- **Easy to calculate:**

Hashing algorithms are very efficient and do not require large computing power to run.



# Characteristics of Hash Algorithm

- خصائص خوارزمية التجزئة اتجاه واحد (One-Way:) بمجرد تحويل البيانات بواسطة الخوارزمية، يصبح من شبه المستحيل إعادتها إلى حالتها الأصلية.حتمية (Deterministic:) دائمًا ما تُنتج خوارزمية التجزئة نفس النتيجة عند إعطائها نفس المدخلات، مما يعني أن مدخلًا معينًا سيعطي دائمًا نفس قيمة التجزئة.سهولة الحساب ( : ) Easy to calculate خوارزميات التجزئة فعالة جدًا ولا تتطلب طاقة حسابية كبيرة للتشغيل.شرح مبسط:تخيل أنك تكتب نصًا (مثل " Hello") وتدخله في خوارزمية التجزئة، فتُخرج الخوارزمية سلسلة معقدة من الأحرف (التجزئة). إذا أدخلت نفس النص مرة أخرى، ستحصل على نفس التجزئة (حتمية). ولا يمكنك استعادة النص " Hello" من هذه السلسلة، مما يجعلها آمنة (اتجاه واحد).



# Characteristics of Hash Algorithm

- **The Avalanche effect.**

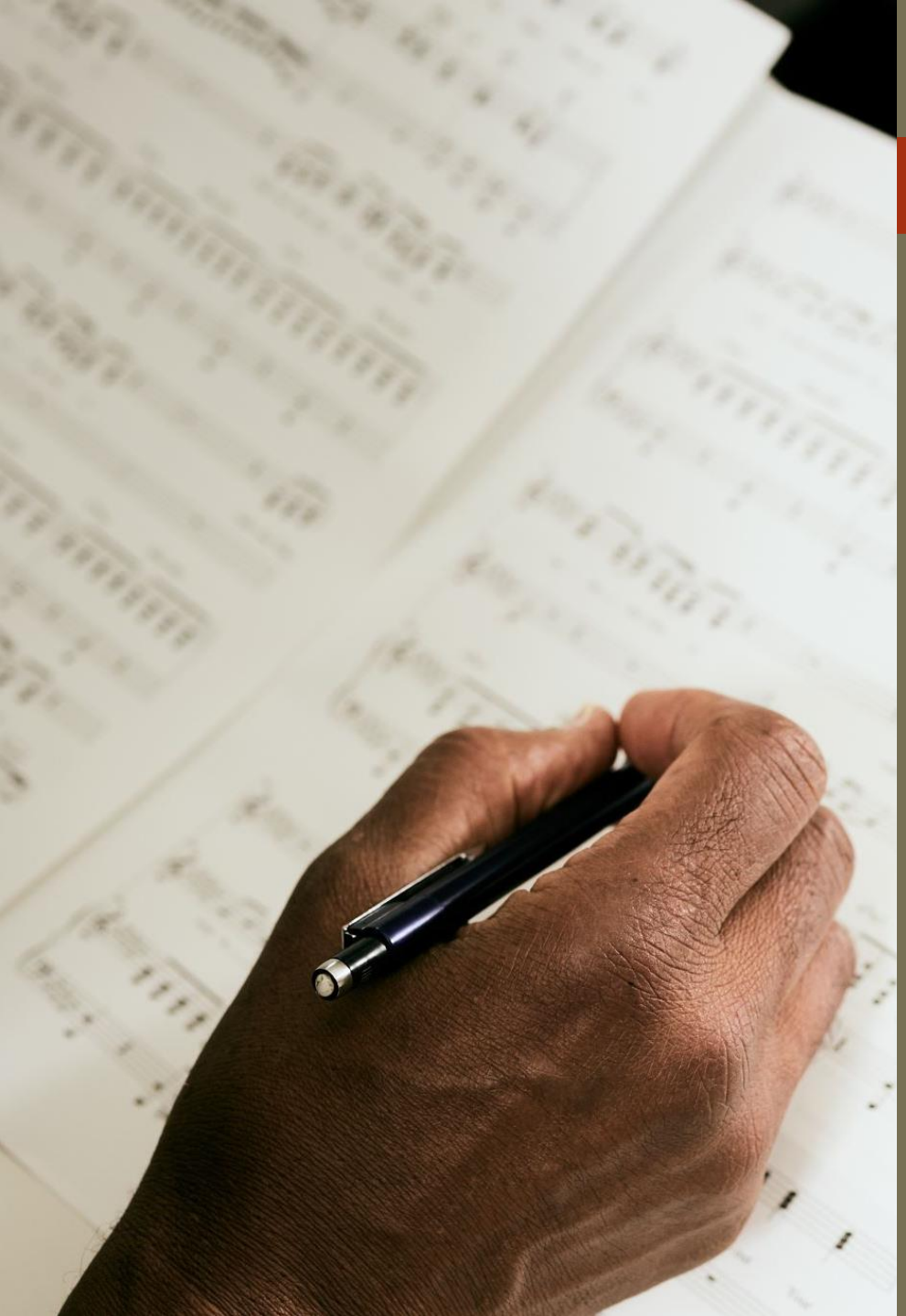
Any slight change in data entry results in a different hash than the original one.

- **Must withstand collision.**

Collisions are improbable: When using SHA-256, there are 2256 possible hash values, making it nearly impossible for two documents to accidentally have the same hash value.

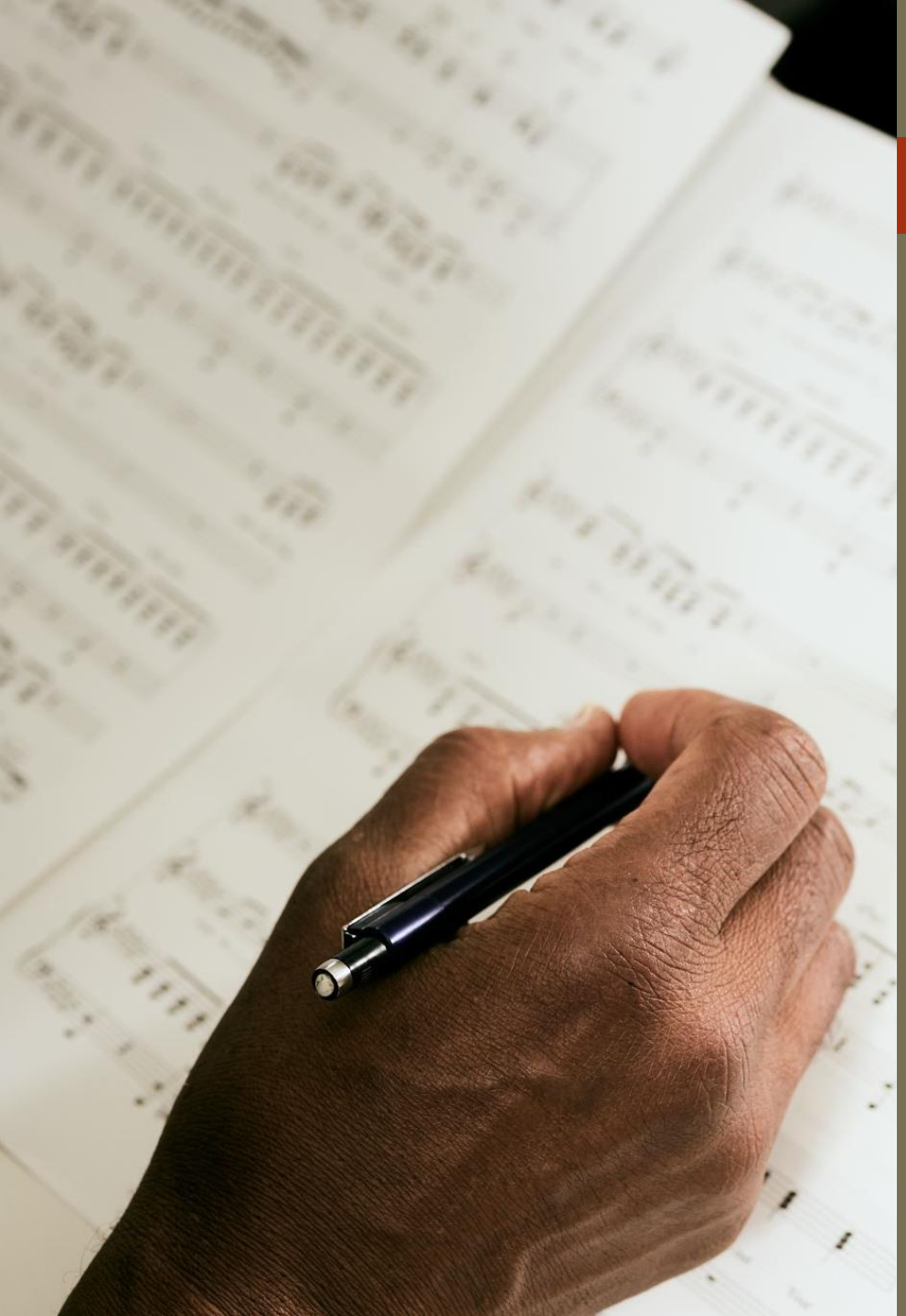
# Characteristics of Hash Algorithm

- **تأثير الانهيار The Avalanche effect أي تغيير طفيف في إدخال البيانات يؤدي إلى تجزئة مختلفة تمامًا عن الأصلية.مقاومة التصادم.**
- **Must withstand collision من الصعب للغاية حدوث تصادمات: عند استخدام SHA-256، يوجد 22562 256 قيمة تجزئة ممكنة، مما يجعل من المستبعد جدًا أن تتطابق تجزئتان لمستندين مختلفين عن طريق الخطأ.**
- **شرح بسيط: تخيل أنك تكتب كلمة، ولو غيرت حرفًا واحدًا فيها، ستحصل على نتيجة مختلفة تمامًا (تأثير الانهيار). وبسبب العدد الهائل من القيم الممكنة، يكاد يكون من المستحيل الحصول على نفس النتيجة لكلمتين مختلفتين، وهذا يعني أنها آمنة ضد التكرار العرضي**



# Immutable ledger

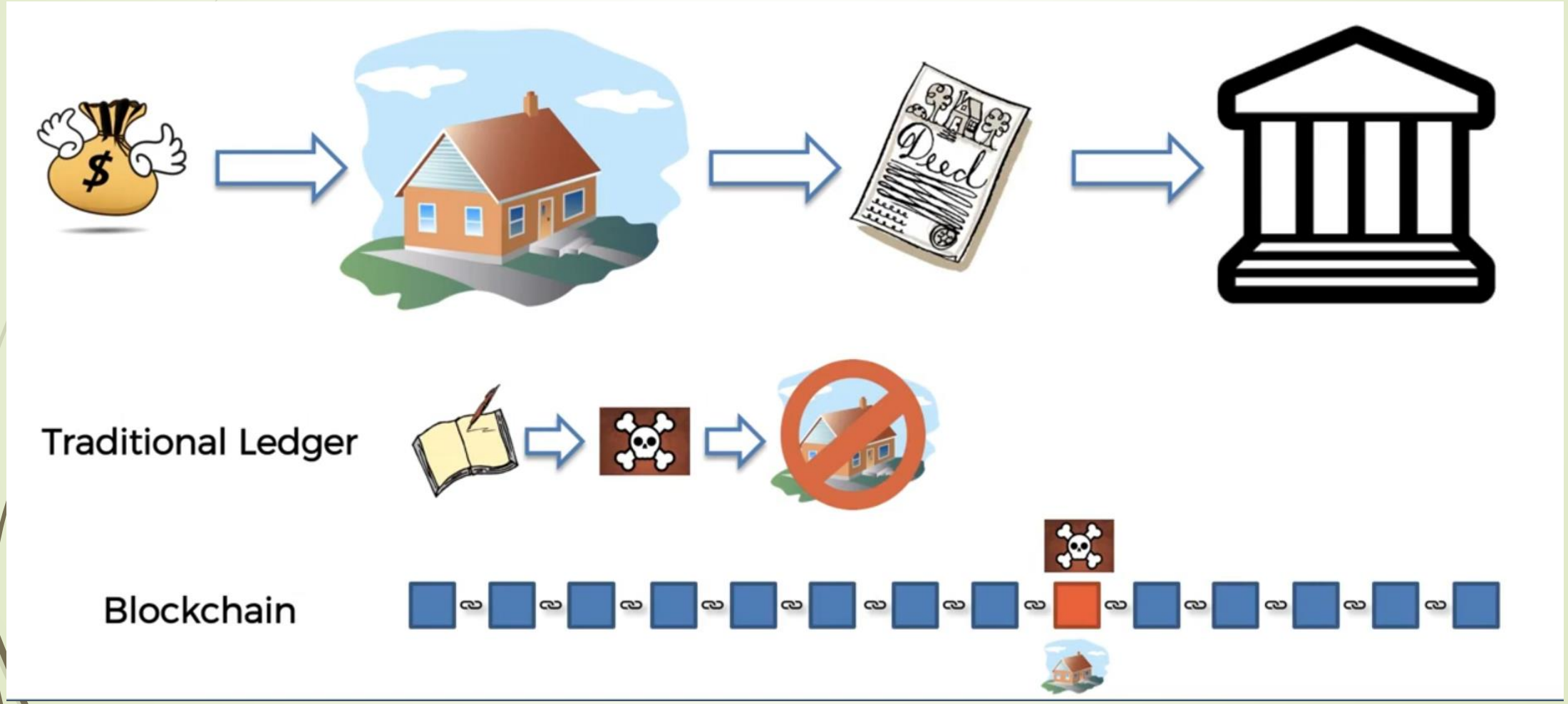
- An immutable ledger is a record-keeping system where the data entered can't be altered, tampered with, or deleted.
- It ensures that all transactions or entries made in the ledger are permanently recorded and maintained in their original state, creating a transparent and trustworthy record of events.

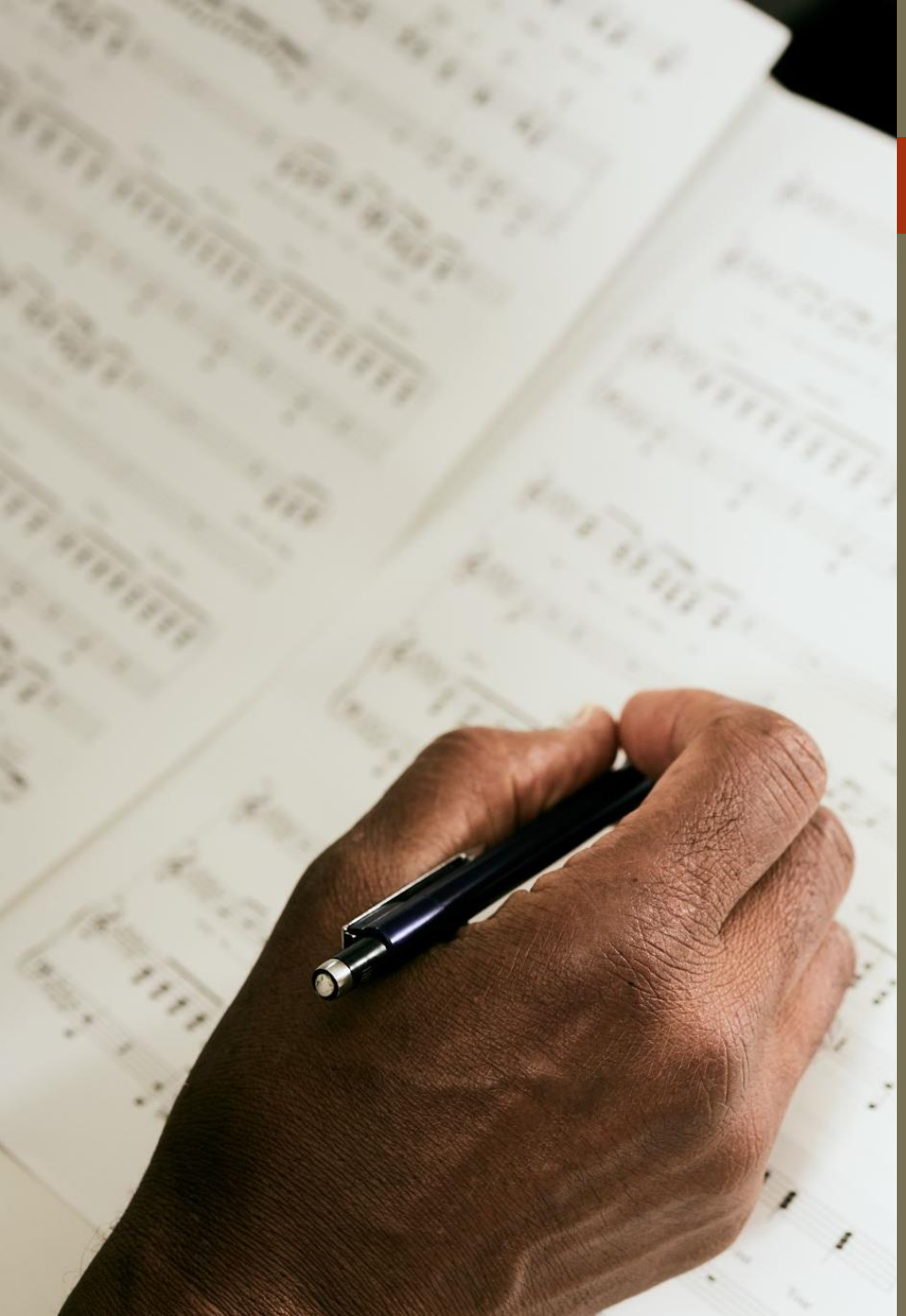


# السجل غير القابل للتعديل

- **السجل غير القابل للتغيير Immutable Ledger** السجل غير القابل للتغيير هو نظام لحفظ السجلات حيث لا يمكن تعديل البيانات المدخلة أو العبث بها أو حذفها. يضمن هذا النظام أن جميع المعاملات أو الإدخالات التي تُسجَّل فيه تبقى مسجلة بشكل دائم وبحالتها الأصلية، مما يخلق سجلاً شفافًا وموثوقًا للأحداث.
- **شرح مبسط**: تخيل دفترًا تُدَوَّن فيه جميع المعلومات بقلم دائم، ولا يمكن محوها أو تعديلها. هذا الدفتر يمثل سجلًا يمكن الوثوق به لأنه يُظهر جميع التعديلات بشكل صادق ويصعب التلاعب به.

# Immutable ledger





# السجل غير القابل للتعديل

- السجل التقليدي (Traditional Ledger):يظهر في الجزء العلوي من الصورة. تبدأ العملية بمبلغ مالي يُستخدم لشراء منزل، ويتم توثيق العملية في السجلات، ولكن يمكن التلاعب بها أو تغيير الملكية، مما يجعل السجلات عرضة للتزوير أو الفقدان.
- البلوك تشين (Blockchain):في الجزء السفلي، يتم تمثيل البلوك تشين كأشرطة متصلة ببعضها. كل كتلة ( (blockتمثل خطوة أو عملية مسجلة، ولا يمكن تغييرها. إذا حاول أحدهم تغيير أي كتلة (مثل الكتلة الحمراء في الصورة)، ستبقى محاولته فاشلة، لأن كل الكتل متصلة ببعضها بتسلسل لا يسمح بالتغيير، مما يضمن أمان وموثوقية السجل.شرح مبسط:تخيل أن كل عملية يتم تسجيلها في سلسلة من الحلقات (الكتل)، وإذا حاول أحد تغيير حلقة واحدة، فإن السلسلة بأكملها ستُظهر الخلل، مما يجعلها غير قابلة للتلاعب.

# Benefits of Immutable Ledger in Blockchain

- Security is Tight in Blockchain.
- Ensures Authenticity and High Quality
- Readily Benefits Supply Chain Management
- Higher Level of Privacy

# Benefits of Immutable Ledger in Blockchain

**فوائد السجل غير القابل للتغيير في البلوك تشين:**

**تعزيز الأمان في البلوك تشين:** يوفر البلوك تشين مستوى أمان عالي يصعّب من التلاعب بالبيانات.

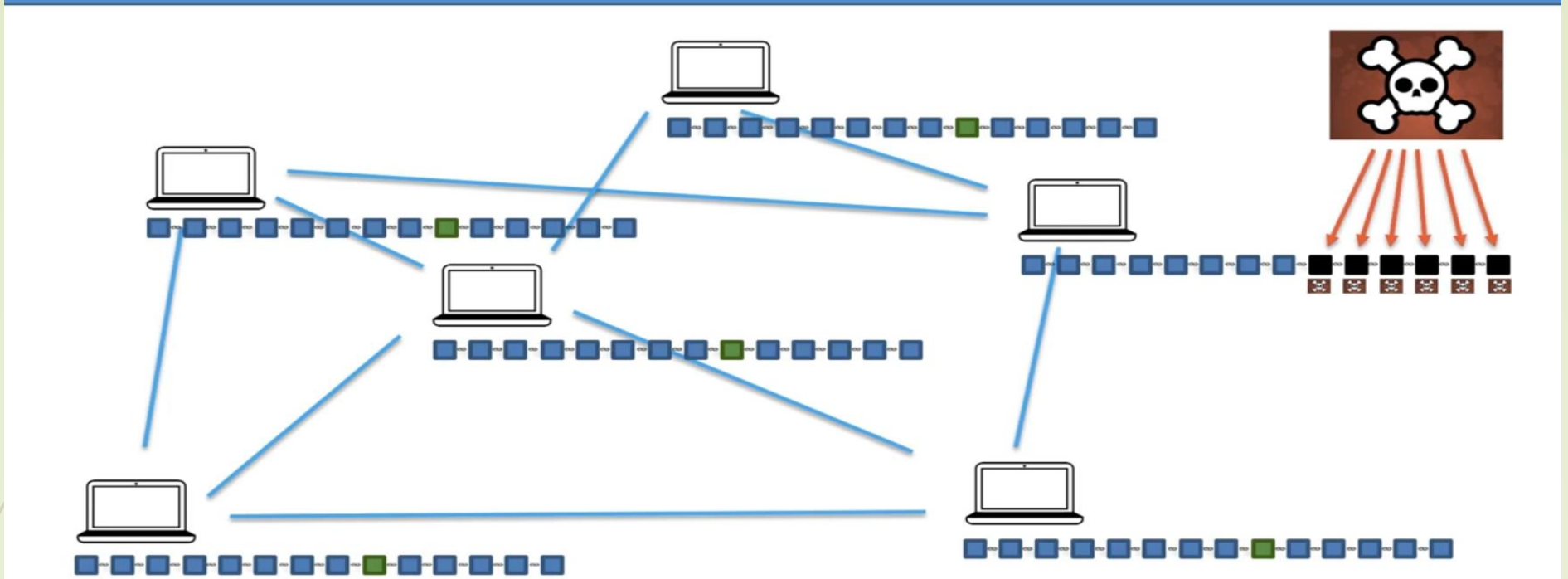
**يضمن الأصالة والجودة العالية:** يسهم في ضمان أن البيانات أصلية وغير معدلة، مما يرفع من موثوقية النظام. **يعود بالفائدة على إدارة سلسلة التوريد:** يجعل من السهل تتبع المنتجات والتحقق من جودتها على طول سلسلة التوريد، مما يعزز الشفافية.

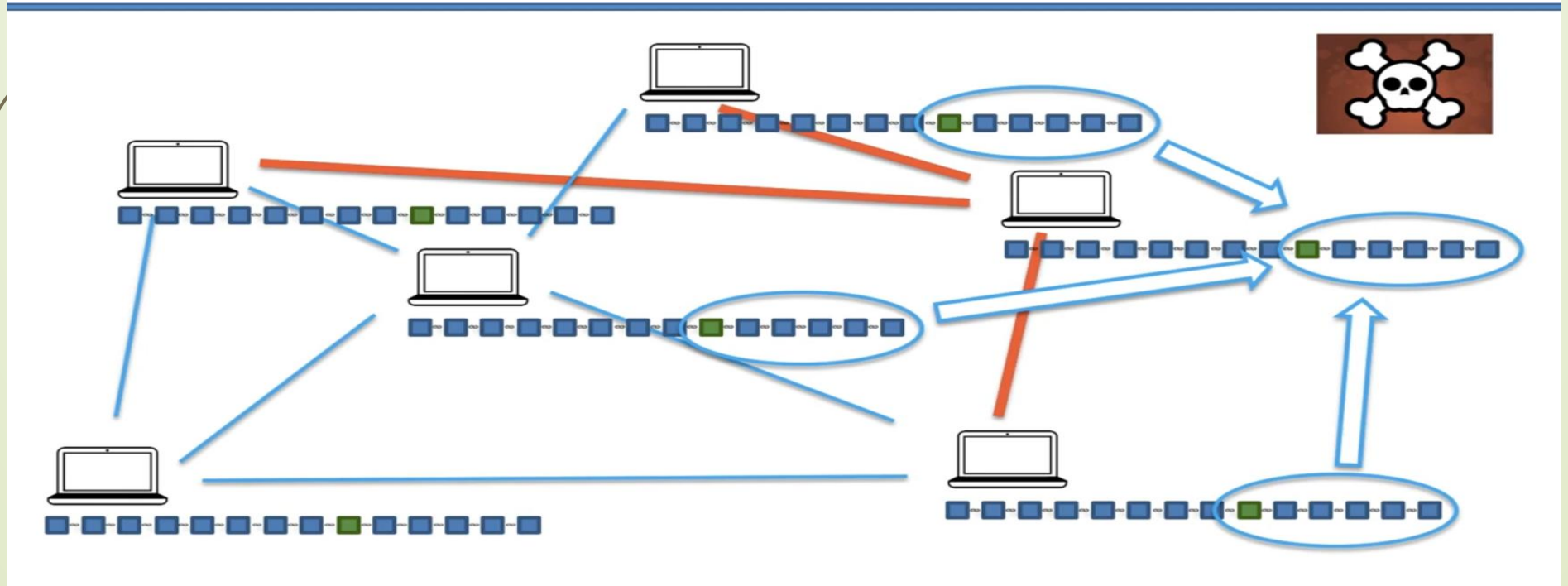
**مستوى أعلى من الخصوصية:** يوفر نظام البلوك تشين حماية عالية للخصوصية، مما يجعل البيانات متاحة فقط لأصحاب الصلاحيات.

**شرح مبسط:** تخيل أنك تملك دفترًا آمنًا لا يمكن لأحد تغييره، ويسمح لك بتوثيق جميع الأحداث أو المنتجات بدقة. يساعد هذا في تأكيد صحة البيانات ويسمح لك بتتبع كل خطوة في عملية الإنتاج أو التوريد، مع ضمان حماية بياناتك الخاصة.

# Distributed P2P Network

- Blockchain is a P2P network that acts as a decentralized ledger for one or more digital assets. It refers to a decentralized peer-to-peer system in which each computer keeps a complete copy of the ledger and verifies its authenticity with other nodes to guarantee the data's accuracy.
- Group of devices call nodes.
- When P2P networks are established over the internet, the size of the network and the files available allow vast amounts of data to be shared.





# P2P

- **شبكة P2P** موزعة البلوك تشين هو شبكة من نوع P2Pتعمل كسجل لا مركزي لأصل رقمي أو أكثر. تشير هذه الشبكة إلى نظام لامركزي من نظير إلى نظير، حيث يحتفظ كل جهاز بنسخة كاملة من السجل ويؤكد صحته مع الأجهزة الأخرى (العقد) لضمان دقة البيانات. مجموعة الأجهزة في هذه الشبكة تُعرف بـ"العقد" (nodes).عندما يتم إنشاء شبكات P2Pعبر الإنترنت، يتيح حجم الشبكة وتوفر الملفات فيها مشاركة كميات ضخمة من البيانات.

- **شرح مبسط:** تخيل شبكة من الأصدقاء، حيث يمتلك كل شخص نسخة من نفس القائمة، ويتحقق كل شخص مع الآخرين لضمان أن كل شيء متماثل وصحيح. إذا أراد أحد الأعضاء إجراء تغيير، يجب أن يوافق الجميع، مما يجعل النظام موثوقًا وآمنًا.

# Mining

- Mining

A peer-to-peer computer process. Blockchain mining is a computation process performed to confirm and verify transactions trustfully and to get the new blocks added to the blockchain.

# التعدين

- **التعدين Mining** عملية حوسبة من نوع نظير إلى نظير P2P يُعتبر تعدين البلوك تشين عملية حسابية يتم من خلالها تأكيد والتحقق من المعاملات بأمان، بهدف إضافة كتل جديدة إلى البلوك تشين.
- **شرح مبسط:** تخيل أن لديك مجموعة من الأشخاص يعملون معًا لحل لغز معين. عندما يحل أحدهم اللغز، يتم تسجيل الإجابة في سجل مشترك (البلوك تشين)، ويمنح الشخص الذي حل اللغز مكافأة. هذا هو ما يحدث في التعدين، حيث تُستخدم قوة الحوسبة لحل مسائل معقدة بهدف تأكيد المعاملات وإضافة كتل جديدة.

# Intro to Mining

- Where does cryptocurrency (e.g., Bitcoin) come from? With paper money, a government decides when to print and distribute money. Bitcoin doesn't have a central government.

- With Bitcoin, miners use special software to solve math problems and are issued a certain number of bitcoins in exchange. This provides a smart way to issue the currency and incentivises more people to mine.

- Bitcoin miners help keep the Bitcoin network secure by approving transactions. More miners means a more secure network.

# مقدمة حول التعدين

- **مقدمة حول التعدين:** من أين تأتي العملات الرقمية (مثل البيتكوين)؟ في العملات الورقية، تقرر الحكومة متى تطبع وتوزع الأموال. أما البيتكوين فلا يملك حكومة مركزية.في نظام البيتكوين، يستخدم المعدنون برامج خاصة لحل مسائل رياضية ويُكافأون بعدد معين من البيتكوينات. يوفر هذا النظام طريقة ذكية لإصدار العملة ويشجع المزيد من الأشخاص على التعدين.يساعد معدنو البيتكوين في الحفاظ على أمان الشبكة من خلال الموافقة على المعاملات. زيادة عدد المعدنين يعني زيادة أمان الشبكة.شرح مبسط:تخيل أن لديك لغزًا رياضيًا، وعند حله تحصل على جائزة (بيتكوين). كلما زاد عدد الأشخاص الذين يحاولون حل الألغاز، يصبح النظام أكثر أمانًا لأن الجميع يتحققون من صحة الأجوبة ويحافظون على دقة النظام.

# How Mining works?

- The Nonce “Number only used once”.
- **How is the nonce used?** Nonces are used as the changing variable. Cryptocurrency workers use the nonce to validate the information contained within a block. The mining program appends a random nonce to the block header and hashes it. If this number exceeds the network target, the miner tries again with another randomly generated nonce. If the resulting hash value is equal to or less than the target hash, the miner has created a solution and receives the block as a reward. The block is closed, and a new one that includes the previous block's hash is opened.

# كيف يتم التعدين ؟

- كيف يعمل التعدين؟ الـ " Nonceرقم يُستخدم مرة واحدة فقط":يُستخدم الـ Nonceكمتغير متغير. يستخدم عمال التعدين في العملات الرقمية هذا الرقم للتحقق من صحة المعلومات الموجودة داخل الكتلة. يقوم برنامج التعدين بإضافة Nonceعشوائي إلى رأس الكتلة وتجزئته. إذا تجاوز هذا الرقم الهدف الذي حددته الشبكة، يحاول المعدّن مرة أخرى باستخدام Nonceجديد يتم إنشاؤه عشوائيًا. إذا كانت قيمة التجزئة الناتجة تساوي أو تقل عن قيمة الهدف، يكون المعدّن قد وجد الحل ويحصل على الكتلة كمكافأة. يتم إغلاق الكتلة وفتح كتلة جديدة تحتوي على تجزئة الكتلة السابقة.

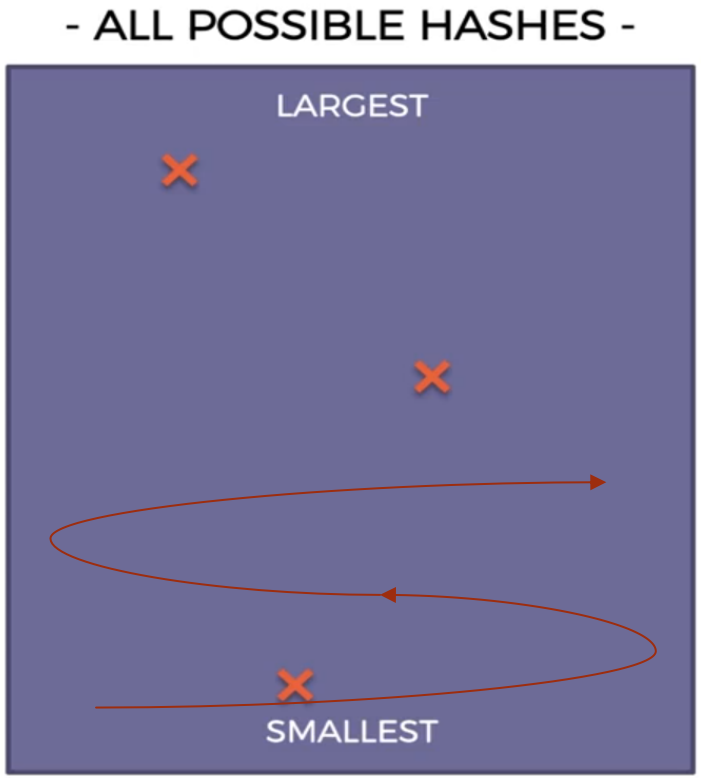
- **شرح مبسط:** تخيل أنك تحاول فتح قفل بأرقام سرية متعددة، كل مرة تجرب رقمًا عشوائيًا ( (Nonceللتحقق مما إذا كان يطابق الرقم المطلوب. إذا لم يتطابق، تحاول مجددًا برقم آخر حتى تصل إلى الرقم الصحيح، عندها يُفتح القفل وتكافأ بجائزة (كتلة جديدة).

# How Mining works?

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

0000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F



- **التعدين** يعتمد بشكل أساسي على حل ألغاز التشفير التي يحددها بروتوكول البلوك تشين. يقوم البروتوكول بتحديد قيمة هدف كعنصر أساسي في هذه العملية. لكي ينجح المعدّن في تعدين كتلة، يجب عليه توليد تجزئة تتوافق مع معايير محددة بالنسبة إلى هذا الهدف. بشكل خاص، تُعتبر التجزئات التي تكون أقل من هذا الهدف صالحة. إذا تجاوزت التجزئة الهدف، فإنها تُعتبر غير صالحة ولا تُدرج في البلوك تشين.إذا أنتج المعدّن تجزئة: فإن وجود هذا الهدف ليس له أي غرض اقتصادي أو حسابي سوى فرض تحدٍّ على المعدّنين. يعمل هذا كعقبة يجب على المعدّنين تجاوزها لتأكيد وإضافة كتلة جديدة إلى البلوك تشين. على سبيل المثال، إذا أنتج المعدّن تجزئة أعلى من الهدف المحدد، فلن تُقبل، ولن يتمكن المعدّن من إنشاء كتلة. أما إذا كانت التجزئة أقل من الهدف، فسيُسمح للمعدّن بإنشاء الكتلة ويعتبر قد أكمل عملية التعدين بنجاح.
- **شرح مبسط:** تخيل أن لديك بوابة لا تُفتح إلا إذا كنت تحمل بطاقة بأرقام معينة أقل من حد معين. إذا كانت أرقام البطاقة أقل من الحد، يمكنك الدخول (تأكيد الكتلة)، وإذا كانت أعلى من الحد، فسيتم رفضك، مما يجعل التحدي في العثور على بطاقة تحمل الأرقام المناسبة.

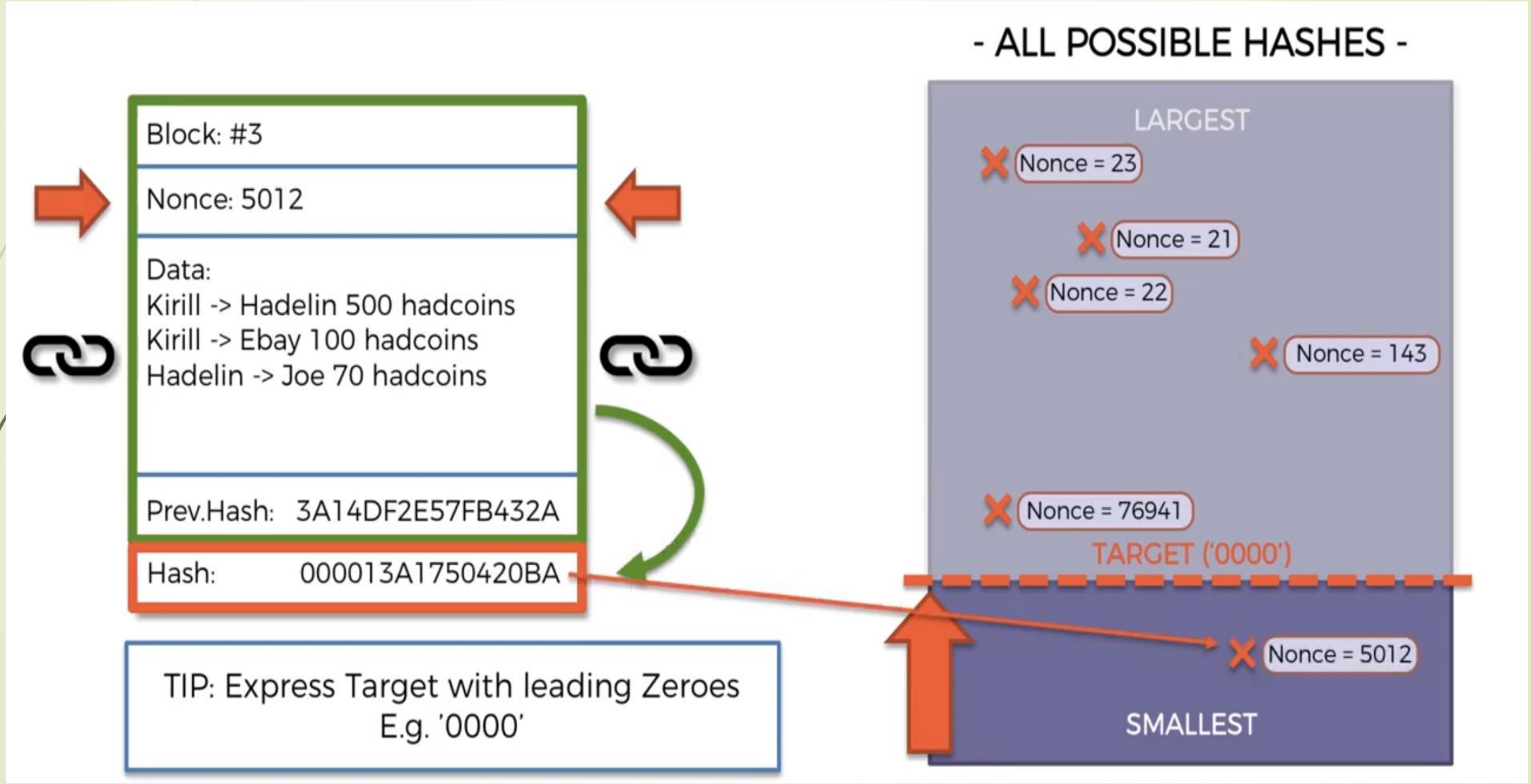
# كيف يتم التعدين ؟

- **جميع التجزئات الممكنة All Possible Hashes** يظهر الرسم البياني جميع التجزئات الممكنة مرتبة من الأكبر إلى الأصغر.
- **التجزئة المستهدفة :Target Hash** الهدف من التعدين هو إيجاد تجزئة تساوي أو تقل عن قيمة محددة. تكون هذه القيمة عادة صغيرة جدًا (قريبة من الأصغر) مما يجعل العثور على التجزئة المناسبة تحديًا.
- **عملية المحاولة والتكرار:** يقوم المعدّنون بتجربة العديد من التجزئات المختلفة Nonce بشكل عشوائي حتى يصلوا إلى تجزئة تساوي أو تقع ضمن الهدف المطلوب. إذا حصل المعدّن على التجزئة المطلوبة، يتم إغلاق الكتلة ويكافأ المعدّن.
- **شرح مبسط:** تخيل أنك تحاول العثور على رقم أقل من عدد معين، وكلما كان الرقم المطلوب أصغر، كان العثور عليه أصعب. التعدين هو عملية البحث عن هذا الرقم المطلوب من خلال تجارب متعددة إلى أن تصل للرقم الصحيح المطلوب.

- Mining primarily involves solving cryptographic puzzles defined by the blockchain algorithm. The blockchain protocol has set a target value as the central component of this process. To successfully mine a block, a miner must generate a hash that meets specific criteria relative to this target value. Specifically, only hashes that are below this target are considered valid. If the generated hash exceeds the target, it is deemed invalid and is not included in the blockchain.

- If a miner produces a hash: The existence of this target is arbitrary and serves no intrinsic economic, logical, computational, or cryptographic purpose other than to impose a challenge on miners. This mechanism functions as a hurdle that miners must overcome to validate and add a new block to the blockchain. For instance, if a miner produces a hash above the set target, it will not be accepted, and the miner will be unable to create a block. Conversely, if the hash is below the target, the miner is permitted to generate the block and is considered to have successfully mined it.

# How Mining works?



- **الكتلة Block** : لدينا الكتلة رقم 3، والتي تحتوي على بيانات المعاملات مثل تحويل العملات بين المستخدمين، وأيضًا تحتوي على تجزئة الكتلة السابقة.الـ Nonce: هو الرقم 5012 في هذه الحالة. يتم تغيير هذا الرقم عدة مرات حتى يتم العثور على تجزئة تتوافق مع شروط الهدف.

- **التجزئة Hash:** يظهر في الأسفل تجزئة الكتلة الحالية، والتي يجب أن تبدأ بأصفار وفقًا لقيمة الهدف المحددة (مثال: "0000").

- **قيمة الهدف Target** موضح باللون البرتقالي في الرسم البياني، ويمثل الحد الأدنى لقيمة التجزئة المقبولة. إذا كانت التجزئة أقل من الهدف، يعتبر المعدّن قد نجح.

- **شرح مبسط:** تخيل أنك تحاول العثور على رقم يبدأ بأربعة أصفار باستخدام تركيبات مختلفة من الأرقام. الـ Nonceهو الرقم الذي يتغير في كل محاولة حتى تحقق الرقم المطلوب.

# Mining Difficulty

- When more miners join the network, the math problems will be solved faster, so the network increases the difficulty of these problems.
- When the difficulty increases, the process of mining Proof-of-Work solving becomes more costly and time-consuming.
- For example, in the Bitcoin network, the mining difficulty automatically adjusts when each 2,016 blocks are created.
- So, the average mining time remains 10 minutes per block, depending on the number of people actively mining on the network.

# Mining Difficulty

# صعوبة التعدين

- **صعوبة التعدين Mining Difficulty** عندما ينضم المزيد من المعدّنين إلى الشبكة، تصبح المسائل الرياضية تُحل بشكل أسرع، وبالتالي تزيد الشبكة من صعوبة هذه المسائل.
- **عند زيادة الصعوبة**، تصبح عملية التعدين باستخدام إثبات العمل Proof-of-Work أكثر تكلفة وتستغرق وقتًا أطول. **على سبيل المثال**، في شبكة البيتكوين، يتم تعديل صعوبة التعدين تلقائيًا بعد إنشاء كل 2016 كتلة.لذلك، يبقى متوسط وقت التعدين حوالي 10 دقائق لكل كتلة، وذلك اعتمادًا على عدد الأشخاص الذين يقومون بالتعدين على الشبكة.
- **شرح مبسط:** تخيل سباقًا حيث ينضم المزيد من المتسابقين الأقوياء، مما يجعل السباق يُنهي بسرعة. لذلك، يقوم المنظمون بإضافة عقبات لزيادة الصعوبة حتى يبقى الوقت المطلوب لإنهاء السباق ثابتًا. في التعدين، كلما زاد عدد المعدّنين، زادت صعوبة المسائل للحفاظ على وقت ثابت لإضافة الكتل إلى الشبكة.

# What's the Consensus Algorithm?

- Blockchains are powerful tools because they create honest systems that self-correct without needing a third party to enforce the rules. They accomplish the enforcement of rules through their consensus algorithm.

- **The consensus algorithm** methodology enables blockchain to offer unique benefits without sacrificing speed and low transaction costs.
- **Consensus algorithms** serve as the fact-checkers and guardians of any blockchain system, ensuring that any predetermined transaction conditions are met perfectly. Moreover, consensus algorithms are aptly named, as they confirm that all the participant nodes in the system agree to a specific outcome, which is a favourable state for the entire network.

## ماهي خوارزمية الاجماع ؟

### ما هي خوارزمية الإجماع؟

- تقنية البلوكشين قوية لأنها تتيح إنشاء أنظمة نزيهة تستطيع تصحيح نفسها دون الحاجة إلى طرف ثالث لفرض القواعد. يتم تحقيق الالتزام بالقواعد عبر استخدام "خوارزمية الإجماع".
- **خوارزمية الإجماع** تسمح للبلوكشين بتقديم مزايا فريدة مثل السرعة وتكلفة المعاملات المنخفضة دون التضحية بهما.
- تعمل **خوارزميات الإجماع** كمدققي حقائق وحماة لأي نظام بلوكشين، حيث تتأكد من أن جميع الشروط المحددة مسبقًا للمعاملات تتحقق بدقة. وبما أن خوارزميات الإجماع تعتمد على موافقة جميع الأطراف المشاركة، فهي تضمن أن جميع العقد (النقاط المشتركة) تتفق على نتيجة محددة، مما يحقق الاستقرار للشبكة بالكامل.
- **مثال توضيحي بسيط:** تخيل أنك وأصدقاءك تريدون أن تقرروا معًا أي مطعم ستذهبون إليه. كل شخص يقترح خيارًا، ولكن في النهاية تتفقون جميعًا على مطعم واحد. في البلوكشين، تعمل خوارزمية الإجماع بطريقة مشابهة: تحتاج جميع الأطراف المشتركة إلى الموافقة على المعلومات أو المعاملات قبل اعتمادها وإضافتها إلى النظام.

# What's the Consensus Algorithm?

- **Consensus algorithms** guarantee that transactions will go through if all the relevant conditions satisfy all involved parties. Consensus algorithms utilize thousands of nodes within a blockchain system to carry out an astronomically complex mathematical equation, ensuring that every node complies with the conditions.
- the most popular types of consensus algorithms:

1. **Proof-of-Work Algorithm.**
2. **Proof-of-Stake Algorithm**

# ماهي خوارزمية الاجماع

## ما هي خوارزمية الإجماع؟

- خوارزميات الإجماع تضمن أن تتم المعاملات إذا كانت جميع الشروط المطلوبة تحقق رضا جميع الأطراف المعنية. تعتمد خوارزميات الإجماع على آلاف العقد داخل نظام البلوكشين لحل معادلات رياضية معقدة، مما يضمن أن كل عقدة تلتزم بالشروط المحددة.
- الأنواع الأكثر شيوعًا من خوارزميات الإجماع:
  - **خوارزمية إثبات العمل Proof-of-Work**
  - **خوارزمية إثبات الحصة Proof-of-Stake**

مثال توضيحي بسيط:تخيل أنك تريد تحويل أموال لصديقك، ولكن يجب أن يوافق كل شخص في فريقك على صحة التحويل قبل إتمامه. هذا يشبه كيفية عمل إثبات العمل؛ حيث يقوم الجميع بحل مشكلة للتحقق من التحويل. أما في إثبات الحصة، ففقط الأشخاص الذين يملكون حصة كافية يحق لهم التحقق من التحويل، مما يجعل العملية أسرع وأقل تكلفة.

# Proof-of-Work Algorithm.

- Many blockchains, like Bitcoin and Ethereum, use a “proof of work” consensus. In this kind of blockchain, the consensus algorithm determines whether new data entered into the system agrees with it and examines whether the new data is valid. Public blockchains need a robust system because anyone can add data to them. Their consensus mechanism is the rule set that determines what makes a block valid and what chain should be trusted.
- When a blockchain network has a PoW algorithm, each participant is required to complete a certain amount of computational problems. These problems are presented as exceedingly tricky mathematical equations that a computer can only solve. Whoever solves these math puzzles first is entitled to propose the next node in the expansive blockchain network.

# خوارزمية اثبات العمل

- **خوارزمية إثبات العمل Proof-of-Wprk**
- العديد من شبكات البلوكشين، مثل بيتكوين وإيثريوم، تستخدم "إثبات العمل" كوسيلة للتوافق. في هذا النوع من البلوكشين، تحدد خوارزمية الإجماع ما إذا كانت البيانات الجديدة التي تم إدخالها إلى النظام تتوافق مع المعايير، وتتحقق مما إذا كانت هذه البيانات صحيحة. تحتاج شبكات البلوكشين العامة إلى نظام قوي لأن أي شخص يمكنه إضافة بيانات إليها. ومن هنا تأتي أهمية خوارزمية الإجماع التي تحدد قواعد ما يجعل البيانات صالحة وأي سلسلة يجب الوثوق بها.

- عندما يحتوي نظام البلوكشين على خوارزمية إثبات العمل، يجب على كل مشارك إكمال مجموعة معينة من المشكلات الحسابية. هذه المشكلات تتخذ شكل معادلات رياضية صعبة لا يمكن إلا للحاسوب حلها. والشخص الذي يحل هذه الألغاز أولاً يكون له الحق في اقتراح الكتلة التالية في الشبكة.
- **مثال توضيحي بسيط:** تخيل أن لديك مسابقة بين عدة أشخاص لحل لغز رياضي معقد، وأول شخص يحل اللغز يفوز بجائزة. في نظام البلوكشين، هذه الجائزة هي حق إضافة الكتلة التالية من المعاملات إلى الشبكة. هذا بالضبط ما يحدث في "إثبات العمل"؛ كلما زادت سرعة الحل، كان للمشارك فرصة أكبر في إضافة المعاملة وكسب مكافأة.

# Proof-of-Work Algorithm.

- While the POW approach is a tried-and-tested method for ensuring security and verifying blockchain transactions, it has certain disadvantage:
- First, it requires a lot of computational power, forcing participants to spend significant amounts of energy in the process. As a result, the POW method is costly financially and damages the environment, as it causes massive carbon emissions every year.
- Moreover, POW has become slower over the years due to the sheer complexity of computational requirements. With blockchain networks becoming more popular, POW has slowed down significantly.
- Lastly, the POW method requires high startup costs for aspiring crypto miners since the equipment is expensive.

# خوارزمية اثبات العمل

- على الرغم من أن نهج إثبات العمل هو أسلوب مجرب وفعال لضمان الأمان والتحقق من المعاملات في شبكات البلوكشين، إلا أنه يحتوي على بعض العيوب:

1. **استهلاك عالي للطاقة**: يتطلب إثبات العمل قوة حسابية كبيرة، مما يجبر المشاركين على استهلاك كميات كبيرة من الطاقة. ونتيجة لذلك، فإن هذه الطريقة مكلفة من الناحية المالية وتضر بالبيئة، لأنها تتسبب في انبعاثات كربونية ضخمة كل عام.
2. **البطء**: أصبح إثبات العمل بطيئًا مع مرور الوقت بسبب التعقيد المتزايد للعمليات الحسابية. ومع ازدياد شعبية شبكات البلوكشين، أصبح إثبات العمل أبطأ بشكل ملحوظ.
3. **التكلفة العالية للبداية**: تتطلب طريقة إثبات العمل تكاليف بدء عالية للأشخاص الراغبين في تعدين العملات الرقمية، وذلك لأن المعدات اللازمة باهظة الثمن.
4. **مثال توضيحي بسيط**: تخيل أنك تحتاج إلى حل لغز صعب للغاية باستخدام جهاز كمبيوتر قوي، لكن هذا اللغز يستغرق الكثير من الوقت والطاقة. وكلما حاولت حل ألغاز أكثر، زادت صعوبة وسعر حلها، وكذلك زاد استهلاك الطاقة. هذا يشبه تمامًا خوارزمية إثبات العمل، التي تزداد تكلفتها وتعقيدها مع الوقت، مما يجعل الأمر صعبًا على المشاركين الجدد الدخول في التعدين الرقمي.

# Proof-of-Stake Algorithm

- In a proof-of-stake model, nodes are chosen pseudo-randomly, with the possibility of being selected increasing based on their stake in the network. Their stake is measured by the amount of cryptocurrency in their possession. The main benefit of the change will be the reduction in the cost of energy associated with proof of work. This may make it more attractive for individuals to run nodes in the network, which would increase decentralization and increase security.
- The proof-of-stake methodology absolves the network participants from time-consuming and energy-intensive computational work. Instead of creating new network nodes by solving complex mathematical equations, the POS approach enables the network participants to stake a minimum amount of a particular crypto.

# خوارزمية اثبات الحصة

- في نموذج إثبات الحصة، يتم اختيار العقد (المشاركين) بطريقة شبه عشوائية، مع زيادة احتمال اختيارهم بناءً على الحصة التي يمتلكونها في الشبكة. يتم قياس هذه الحصة بكمية العملات الرقمية التي يمتلكونها. الميزة الأساسية لهذا التغيير هي تقليل تكلفة الطاقة المرتبطة بإثبات العمل. قد يجعل هذا الأمر أكثر جاذبية للأفراد لتشغيل العقد في الشبكة، مما يزيد من اللامركزية ويعزز الأمان. تعفي منهجية إثبات الحصة المشاركين في الشبكة من العمل الحسابي المرهق الذي يستغرق وقتًا ويتطلب طاقة كبيرة. بدلاً من إنشاء عقد جديدة عن طريق حل معادلات رياضية معقدة، يتيح نظام إثبات الحصة للمشاركين تأمين حد أدنى من العملات الرقمية كشرط للمشاركة.
- **مثال توضيحي بسيط:** تخيل أنك في مسابقة، ولديك فرصة أكبر للفوز كلما زاد عدد النقاط التي تراهن بها. في "إثبات الحصة"، الأشخاص الذين يملكون عددًا أكبر من العملات الرقمية لديهم فرصة أكبر للمشاركة في تأمين الشبكة وكسب المكافآت، دون الحاجة إلى استخدام طاقة كبيرة لحل مشكلات معقدة كما هو الحال في "إثبات العمل".

# Public and privet Blockchain

- **A Public Blockchain**, also known as a permissionless Blockchain, is open to all, and everyone can read as well as write over the data. In a public Blockchain, you don't need any authorization as you have open access to all the data. Moreover, if the Blockchain is public, the rules are very complicated, along with a complex consensus algorithm for better security.
- In this guide, we will discuss complex consensus algorithms in detail, along with Proof-of-Work and Proof-Stake. Miners use these algorithms to confirm transactions over the Blockchain.
- A public Blockchain has more complex consensus algorithms as compared to a private Blockchain because, in a private Blockchain, the permission is limited to a group of people who are accessing the network.

# البلوكشين العام و الخاص

- **البلوكشين العام**: ويعرف أيضًا باسم البلوكشين المفتوح، وهو متاح للجميع، حيث يمكن لأي شخص قراءة وكتابة البيانات فيه. لا يتطلب البلوكشين العام أي إذن للوصول إلى البيانات، حيث يمكنك الوصول المفتوح إلى جميع البيانات. وبما أن هذا النوع من البلوكشين عام، تكون القواعد معقدة للغاية، إلى جانب استخدام خوارزميات إجماع معقدة لتحقيق أمان أعلى.
- في هذا الدليل، سنناقش خوارزميات الإجماع المعقدة بالتفصيل، مثل **إثبات العمل** و**إثبات الحصة**، حيث يستخدم المعدنون هذه الخوارزميات لتأكيد المعاملات على البلوكشين.
- **البلوكشين العام** يحتوي على خوارزميات إجماع أكثر تعقيدًا مقارنةً بـ **البلوكشين الخاص**، لأن في البلوكشين الخاص يكون الوصول محدودًا على مجموعة معينة من الأشخاص الذين يمتلكون إذنًا للوصول إلى الشبكة.
- **مثال توضيحي بسيط:** تخيل أن لديك مكتبة عامة يمكن لأي شخص الدخول إليها والاطلاع على الكتب، وهذا يمثل البلوكشين العام. أما البلوكشين الخاص فهو يشبه المكتبة الخاصة التي تتطلب دعوة أو عضوية للوصول إلى الكتب الموجودة فيها، مما يجعلها متاحة لمجموعة محددة فقط.

- In the case of a complex consensus algorithm, they are computationally more expensive to mine into a block.
- No one owns a public Blockchain; hence, it has no central authority or a single person holding it.
- Al the public Blockchains are open, which means no one owns them, and you can read and write data over it.
- The Bitcoin Blockchain and Ethereum Blockchain are the best examples of public Blockchains

- في حالة خوارزميات الإجماع المعقدة، تكون عملية التعدين أكثر تكلفة من الناحية الحسابية لإضافتها إلى كتلة جديدة. لا يمتلك أي شخص البلوكشين العام؛ لذلك، لا توجد سلطة مركزية أو شخص واحد يتحكم فيه. جميع شبكات البلوكشين العامة مفتوحة، مما يعني أن لا أحد يمتلكها، ويمكنك قراءة وكتابة البيانات عليها.تعد بلوكشين البيتكوين وبلوكشين الإيثيريوم من أفضل الأمثلة على البلوكشين العام.

# Private Blockchain

- Private Blockchain, as the name suggests, is for personal use. It can be used with your existing applications to make them even more secure. Such networks allow you to provide significant permissions, like authorizing the nodes connecting to the network.
- Nodes are different computers connected inside the peer-to-peer network running the Blockchain codes.
- In a private blockchain, you don't need miners to solve a complex problem, wasting precious time because the data must be confirmed quickly.
- Permissioned ledgers limit contributions to a limited set of users given permission. Depending on the settings of the ledger, access to view records can be restricted or public. Many different aspects of the blockchain can be customized to meet different needs. These are likely to be the most useful for the public sector.

# البلوكشين الخاص

- **البلوكشين الخاص**، كما يشير الاسم، مخصص للاستخدام الشخصي. يمكن استخدامه مع التطبيقات الحالية لزيادة الأمان. تسمح هذه الشبكات بتوفير أذونات محددة، مثل السماح للعقد بالاتصال بالشبكة.
- العقد هي أجهزة حاسوب مختلفة متصلة داخل شبكة ند لند ( peer-to-peer) لتشغيل أكواد البلوكشين.
- في البلوكشين الخاص، لا تحتاج إلى معدنين لحل مشكلات معقدة، حيث يجب تأكيد البيانات بسرعة.
- **السجلات المأذونة** تحد من المشاركة إلى مجموعة محدودة من المستخدمين المصرح لهم. وبحسب إعدادات السجل، يمكن أن يكون الوصول لعرض السجلات مقيدًا أو عامًا. يمكن تخصيص العديد من الجوانب في البلوكشين لتلبية احتياجات مختلفة، مما يجعله مفيدًا جدًا للقطاع العام.
- مثال توضيحي بسيط:تخيل مؤسسة تمتلك قاعدة بيانات خاصة لا يستطيع الوصول إليها إلا الموظفون المصرح لهم. هذا يشبه البلوكشين الخاص، حيث يمكن فقط للأشخاص الذين حصلوا على إذن الوصول إلى الشبكة والمساهمة فيها، مما يعزز الأمان ويحافظ على الخصوصية.

# What are the Blockchain Use Cases in the Financial Sector?

- **Capital Markets**
- **Asset Management**
- **Payments and remittances**
- **Banking and Lending**
- **Insurance**

# ماهي حالات استخدام البلوكشين

- **ما هي حالات استخدام البلوكشين في القطاع المالي؟**

- **أسواق رأس المال:**
استخدام البلوكشين لتحسين كفاءة التداولات وتقليل الوقت اللازم لتسوية المعاملات.

- **إدارة الأصول:**
استخدامه لتسجيل وتحديث ملكية الأصول بشكل آمن وشفاف.

- **المدفوعات والتحويلات:**
تسهيل عمليات الدفع والتحويل عبر الحدود بطريقة أسرع وبتكاليف أقل.

- **الخدمات المصرفية والإقراض:**
تحسين عمليات الإقراض وجعلها أكثر شفافية ومرونة.

- **التأمين:**
تسهيل وتسريع إجراءات المطالبات وتسجيل عقود التأمين بشكل آمن.

# Capital Markets

- Capital markets refer to the pairing of issuers with demand for capital to investors with corresponding risk and return profiles. Raising capital can be challenging whether issuers are entrepreneurs, startups, or large organizations. Firms face increasingly tough regulations, longer times to get to market, volatility from interest rates, and liquidity risk. Particularly in emerging markets, they must navigate the lack of rigorous monitoring, thorough regulation, and sufficient market infrastructure for issuing, settlement, clearing, and trading.
- Blockchain offers multiple benefits for several capital market use cases:

- Elimination of a single point of failure through decentralized utilities
- Facilitation of capital market activities streamlining processes, reducing costs and decreasing settlement times
- Digitization of processes and workflows, reducing operational risks of fraud, human error, and overall counterparty risk
- Digitization or tokenization of assets and financial instruments, making them programmable and much easier to manage and trade. In token form, they gain wider market access through increased connectivity and the possibility of fractionalized ownership. This results in increased liquidity and decreased cost of capital.

# أسواق رأس لمال

- **أسواق رأس المال**
- تشير أسواق رأس المال إلى ربط المُصدرين الذين يحتاجون إلى رأس المال بالمستثمرين الذين يتطلعون لتحقيق العوائد، مع موازنة المخاطر والفرص. يُعتبر جمع رأس المال تحديًا سواء كان المُصدرون من رواد الأعمال أو الشركات الناشئة أو المنظمات الكبيرة. تواجه الشركات لوائح صارمة، وأوقات طويلة للوصول إلى السوق، وتقلبات في أسعار الفائدة، ومخاطر السيولة. في الأسواق الناشئة، يجب على الشركات تجاوز التحديات المتعلقة بالمراقبة الصارمة والتنظيم الشامل والبنية التحتية المناسبة لإصدار وتصفية وتداول الأوراق المالية.
- يوفر البلوكشين العديد من الفوائد في حالات استخدام متعددة في أسواق رأس المال، ومنها:

- **إزالة نقطة فشل واحدة** من خلال اعتماد الأنظمة اللامركزية.
- **تسهيل أنشطة أسواق رأس المال** من خلال تحسين العمليات وتقليل التكاليف وتقليص أوقات التسوية.
- **رقمنة العمليات وسير العمل**، مما يقلل من مخاطر الاحتيال والأخطاء البشرية والمخاطر التشغيلية.
- **رقمنة أو تحويل الأصول والأدوات المالية إلى رموز رقمية**، مما يجعلها قابلة للبرمجة وأسهل في الإدارة والتداول. تساعد هذه الرموز على الوصول إلى أسواق أوسع، وزيادة السيولة، وتقليل تكلفة رأس المال.
- **مثال توضيحي بسيط:** تخيل أنك تمتلك عقارًا وتريد بيعه، ولكن بدلاً من بيع العقار بالكامل لشخص واحد، تقوم بتقسيمه إلى حصص صغيرة يستطيع العديد من الأشخاص شراؤها كاستثمار. باستخدام تقنية البلوكشين، يمكنك تحويل هذا العقار إلى رموز رقمية، وكل رمز يمثل جزءًا صغيرًا من العقار، مما يتيح لمزيد من المستثمرين المشاركة بسهولة وتحسين سيولة الاستثمار.

# Asset Management

- Venture capital firms, private equity firms, real estate funds, and specialty markets are facing demands to improve liability risk management, adapt more dynamic decision-making structures, and address the increasing complexity of ever-changing regulations. Blockchain can effectively streamline asset and stakeholder management. It allows:
- Automated fund launch
- Seamless stakeholder engagement with digital assets and services
- Digitization of portfolio and existing holdings for broader market access, liquidity, and fractionalization
- Customizable built-in privacy settings for transaction confidentiality
- Voting and other shareholder rights and obligations are programmed into digital assets, resulting in a seamless user experience and reduced risks of human error.
- Improved governance and transparency for investors and stakeholders
- Automated fund administration and transfer agency in asset management

# إدارة الأصول

- **إدارة الأصول**
- تواجه شركات رأس المال الاستثماري، وشركات الأسهم الخاصة، وصناديق العقارات، والأسواق المتخصصة ضغوطًا لتحسين إدارة مخاطر الالتزامات، وتكييف هيكليات قرارات أكثر ديناميكية، والتعامل مع التعقيد المتزايد للوائح المتغيرة باستمرار. يمكن للبلوكشين أن يعزز بشكل فعال كفاءة إدارة الأصول وأصحاب المصلحة، حيث يتيح:

- إطلاق الصناديق بشكل آلي.
- تفاعل سلس مع أصحاب المصلحة باستخدام الأصول والخدمات الرقمية.
- رقمنة المحافظ والاستثمارات الحالية لتوسيع الوصول إلى السوق وزيادة السيولة وتجزئة الأصول.
- إعدادات خصوصية قابلة للتخصيص لحماية سرية المعاملات.
- برمجة حقوق والتزامات المساهمين الرقمية، مما يوفر تجربة مستخدم سلسة ويقلل من مخاطر الأخطاء البشرية.
- تحسين الحوكمة والشفافية للمستثمرين وأصحاب المصلحة.
- إدارة آلية للصناديق وخدمات نقل الوكالة في إدارة الأصول.
- **مثال توضيحي بسيط:** تخيل أنك تمتلك مجموعة من الاستثمارات في العقارات، والأسهم، والأصول الأخرى. باستخدام تقنية البلوكشين، يمكنك رقمنة هذه الأصول وتوفير وصول أوسع للمستثمرين عبر الإنترنت. هذا يزيد من سيولة الأصول ويسمح للمستثمرين بامتلاك جزء من استثمارك الكبير، مما يسهل عليهم الاستثمار ويمنحك مرونة أكبر في إدارة أصولك.

# Payments and remittances

- Several intermediaries carry out international payments and remittances today, charging tolls for their services. It takes 2 to 7 days and costs a global average of 6.94% to send $200 between countries. This means that fees, intermediaries, and financial institutions directly reduce remittances by $48 billion. Blockchain can streamline payment and remittance processes, significantly reducing settlement times and costs. It allows:
- Rapid and secure domestic retail payments and cross-border payments.
- Reduce the transaction cost
- Managing time between banks, customers, and exchange companies.
- Multiple forms of payment-enabled on the blockchain: Crypto token, stablecoin, and cryptocurrency

# المدفوعات و التحويلات

- **المدفوعات والتحويلات**
- تقوم العديد من الجهات الوسيطة حاليًا بتنفيذ المدفوعات الدولية والتحويلات، حيث تفرض رسومًا على خدماتها. يستغرق التحويل من يومين إلى سبعة أيام، ويكلف متوسط رسوم عالمي يصل إلى 6.94٪ لإرسال مبلغ 200 دولار بين الدول. هذا يعني أن الرسوم التي تفرضها الجهات الوسيطة والمؤسسات المالية تقلل من قيمة التحويلات بمقدار 48 مليار دولار سنويًا. يمكن للبلوكشين تبسيط عمليات الدفع والتحويل، مما يقلل بشكل كبير من أوقات التسوية والتكاليف، ويتيح:

- مدفوعات سريعة وآمنة داخل الدولة وعبر الحدود.
- تقليل تكلفة المعاملات.
- إدارة الوقت بين البنوك والعملاء وشركات الصرافة.
- دعم أشكال متعددة من المدفوعات عبر البلوكشين، مثل الرموز المشفرة ((Crypto token، العملات المستقرة ((Stablecoin، والعملات الرقمية.
- **مثال توضيحي بسيط:** تخيل أنك تريد إرسال مبلغ من المال لأحد أفراد عائلتك في بلد آخر. باستخدام الطرق التقليدية، قد يستغرق التحويل عدة أيام مع خصم جزء من المبلغ كرسوم. لكن باستخدام البلوكشين، يمكنك تحويل الأموال بسرعة وبتكلفة أقل، كما يمكن استخدام العملات الرقمية لتسهيل هذه العملية بشكل مباشر وآمن.

# Banking and Lending

- Blockchain impacts banking and lending by increasing transparency, reducing costs, and improving efficiency.
- Through its decentralized ledger, blockchain enables secure, immutable records, reducing fraud and enhancing trust.
- Cross-border payments become faster and cheaper by eliminating intermediaries, while smart contracts automate loan agreements, speeding up processing and reducing reliance on third parties.
- Blockchain also streamlines KYC/AML processes by securely sharing customer data between institutions, improving compliance and reducing duplication.
- Asset tokenization allows for more efficient collateral management, and peer-to-peer lending through decentralized finance (DeFi) platforms enables individuals to lend and borrow without traditional banks.

# الخدمات المصرفية و الاقراض

## الخدمات المصرفية والإقراض

- تؤثر تقنية البلوكشين على الخدمات المصرفية والإقراض من خلال زيادة الشفافية، وتقليل التكاليف، وتحسين الكفاءة.
- من خلال السجل اللامركزي، تُمكن البلوكشين من إنشاء سجلات آمنة وغير قابلة للتغيير، مما يقلل من الاحتيال ويعزز الثقة.
- تصبح المدفوعات عبر الحدود أسرع وأقل تكلفة عن طريق التخلص من الوسطاء، في حين تتيح العقود الذكية أتمتة اتفاقيات القروض، مما يسرّع من العمليات ويقلل الاعتماد على الأطراف الثالثة.
- تعمل البلوكشين أيضًا على تبسيط عمليات التحقق من الهوية ( (KYCومكافحة غسيل الأموال ( (AMLمن خلال مشاركة بيانات العملاء بشكل آمن بين المؤسسات، مما يحسن الامتثال ويقلل من التكرار.
- تتيح عملية ترميز الأصول ( (Tokenizationإدارة الضمانات بشكل أكثر كفاءة، وتمكن منصات التمويل اللامركزي ( (DeFiالأفراد من الإقراض والاقتراض دون الحاجة إلى البنوك التقليدية.

**مثال توضيحي بسيط:** تخيل أنك تحتاج إلى قرض، ولكن بدلاً من التوجه إلى البنك، يمكنك استخدام منصة تعتمد على البلوكشين. تقوم بإيداع بعض العملات الرقمية كضمان، وتتيح لك المنصة الاقتراض مباشرة من شخص آخر دون الحاجة إلى وسطاء. هذه العملية أسرع وأقل تكلفة مقارنةً بالنظام التقليدي، وهذا هو تأثير تقنية البلوكشين في مجال الإقراض والخدمات المصرفية.

# Insurance

Property and casualty insurance claims are prone to fraud; claim assessments can take long periods. Blockchain can securely streamline data verification, claims processing, and disbursement, reducing processing time significantly. It allows:

- Authenticated documentation and KYC/AML data, reducing the risk of fraud and facilitating claim assessments
- Automated claims processing with the use of smart contracts
- Automated parameterized contracts to pay out upon occurrence of certain risk
- Automated disbursement of insurance payments
- Tokenized reinsurance markets to facilitate policy reinsurance in open marketplaces, stepping away from traditional broker and relationship-based systems

# التأمين

- تتعرض مطالبات التأمين على الممتلكات والحوادث للاحتيال، وقد تستغرق عمليات تقييم المطالبات وقتًا طويلًا. يمكن لتقنية البلوكشين أن تبسط بشكل آمن عمليات التحقق من البيانات ومعالجة المطالبات وصرف التعويضات، مما يقلل من وقت المعالجة بشكل كبير. وتتيح:

- توثيق البيانات والتحقق من بيانات التحقق من الهوية ( (KYCومكافحة غسيل الأموال ((AML، مما يقلل من مخاطر الاحتيال ويسهل تقييم المطالبات.
- معالجة المطالبات تلقائيًا باستخدام العقود الذكية.
- العقود المؤتمتة المشروطة التي تدفع التعويضات عند حدوث خطر معين.
- صرف تعويضات التأمين بشكل آلي.
- ترميز أسواق إعادة التأمين لتسهيل إعادة التأمين على الوثائق في أسواق مفتوحة، بعيدًا عن الوسطاء التقليديين والأنظمة المعتمدة على العلاقات.

**مثال توضيحي بسيط:** تخيل أنك تقدمت بمطالبة تأمين بعد حادث معين. باستخدام البلوكشين، يتم التحقق من بياناتك تلقائيًا باستخدام العقود الذكية، ويتم صرف التعويض مباشرةً إذا كانت الشروط مستوفاة، دون الحاجة لانتظار الموافقات الطويلة من الوسيط أو شركة التأمين.