تقنيات التكنولوجيا المالية 1: البلوك تشين blockchain

1) البلوك تشين:

المقدمة: تعتبر تقنية البلوك تشين من أهم الابتكارات في عالم التكنولوجيا الحديثة، وهي تمثل قاعدة بيانات لامركزية تسجل المعاملات بطريقة آمنة وموزعة. في هذا الدرس، سنتعرف على مفهوم البلوك تشين، مكوناتها الرئيسية، وكيفية عملها.

1-1) تعريف البلوك تشين: البلوك تشين هو دفتر حسابات عام يعمل بنظام نظير إلى نظير(P2P) ، حيث يتم صيانته عبر شبكة موزعة من أجهزة الكمبيوتر المتصلة ببعضها البعض. هذه الشبكة لا تحتاج إلى سلطة مركزية أو وسطاء خارجيين، مما يعني أنه يمكن إجراء المعاملات مباشرة بين الأطراف المشاركة دون الحاجة إلى بنك أو مؤسسة مالية.

تتمثل فكرة البلوك تشين في تسجيل المعاملات بشكل آمن ودائم، من خلال إنشاء كتل (Blocks) تحتوي على معلومات حول المعاملات التي تم إجراؤها في وقت معين، وتخزينها بشكل سلسلة من الكتل المتتابعة.

1-2) مكونات البلوك تشين:

-**المعاملة:** هي الأساس الذي تبنى عليه كل عملية في البلوك تشين. تتضمن المعاملة معلومات حول من أرسل المال، إلى من أرسل، وفي أي وقت حدثت المعاملة.

-**سجل المعاملة:** كل معاملة تتم يتم تسجيلها في سجل عام يمكن الوصول إليه من قبل أي شخص على الشبكة. هذا السجل لا يمكن تغييره بسهولة، مما يوفر نزاهة للمعلومات.

-**نظام التحقق والتخزين:** يتم التحقق من صحة المعاملات وتخزينها بواسطة برنامج مفتوح المصدر. كل معاملة يتم التحقق منها من قبل عقد الشبكة (Nodes) قبل أن تُضاف إلى السلسلة.

1-3) كيفية عمل البلوك تشين: يتم إنشاء الكتل وتسجيل المعاملات باستخدام برنامج مفتوح المصدر، حيث يحتوي كل كتلة على معلومات حول المعاملات التي حدثت في فترة زمنية معينة. هذه الكتل ترتبط ببعضها البعض عبر الهاش (Hash) الذي يشير إلى الكتلة السابقة، مما يؤدي إلى تكوين سلسلة من الكتل.

1-4) نموذج من السلسلة: كل كتلة تحتوي على:

-رقم مرجعي طويل (تجزئة) للكتلة السابقة. الرقم المرجعي الطويل (التجزئة) للكتلة هو قيمة فريدة تمثل محتويات الكتلة في البلوك تشين. يتم حساب هذه التجزئة باستخدام خوارزميات تجزئة مثل SHA-256، وهي تعمل على تأمين البيانات وضمان تكاملها، وبالتالي فهي جزء أساسي من أمان وشفافية تكنولوجيا البلوك تشين.

-بيانات المعاملة مثل الأطراف المعنية في المعاملة.

-الطابع الزمني (Timestamp) للمعاملة. لتوقيت الزمني أو "Timestamp" هو تمثيل رقمي لوقت محدد. عادةً ما يستخدم للإشارة إلى نقطة معينة في الزمن، ويتم تخزينه عادةً كرقم يمثل عدد الثواني أو الملي ثانية التي مرت منذ وقت معين. في الأنظمة الحاسوبية، يتم استخدام التوقيت الزمني لتسجيل أحداث أو عمليات معينة، مثل تسجيل وقت إنشاء ملف أو تحديثه أو وقوع حدث في قاعدة بيانات.

تُكرر هذه الكتل على خوادم في جميع أنحاء العالم، مما يجعل من المستحيل تعديل أي كتلة بشكل سري.

1-5) مزايا تقنية البلوك تشين:

-**إنشاء الثقة بدون وسطاء:** البلوك تشين يتيح للأشخاص التعاون وتبادل المعلومات بشكل آمن، دون الحاجة إلى وسيط موثوق أو جهة تحكيم.

-**الشفافية:** لأن سجل المعاملات متاح للجميع، يمكن لأي شخص مراجعة التاريخ الكامل للمعاملات والتحقق من صحتها.

-**أمان عالي:** من الصعب جدًا تعديل أو تغيير أي معاملة تم تسجيلها في البلوك تشين، حيث أن تغيير أي جزء من السلسلة يتطلب إعادة حساب جميع التجزئات التي تلي الكتلة المعدلة.

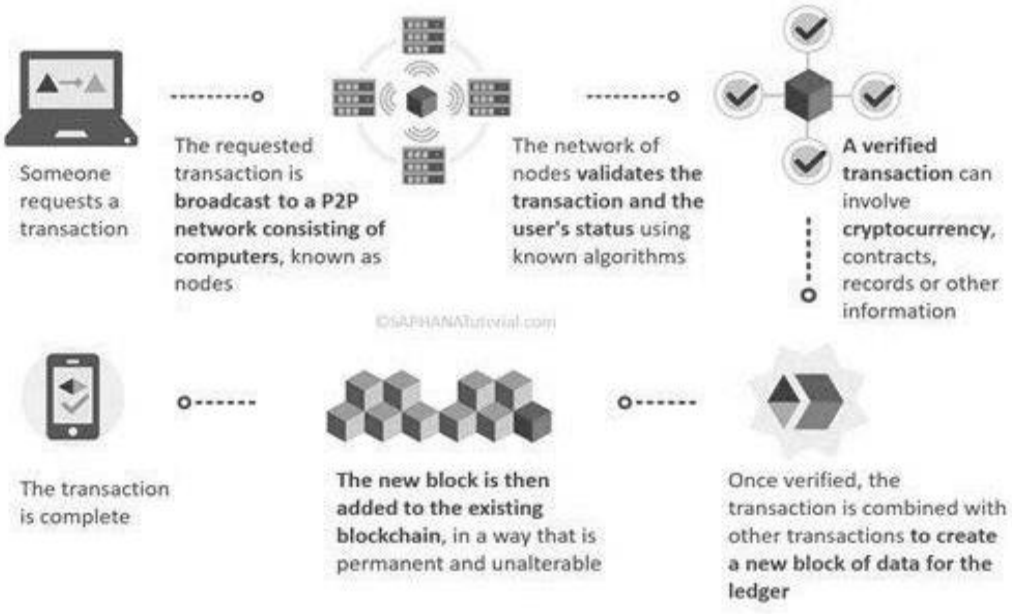
-**استمرارية المعلومات:** البلوك تشين يحتوي على كل المعاملات التي تم تنفيذها في الماضي، مما يجعل من الممكن الوصول إلى تاريخ المعاملات في أي وقت.

1-7) تطبيقات البلوك تشين: على الرغم من أن البلوك تشين بدأ في العمل مع العملات المشفرة، إلا أن تطبيقاته تتعدى ذلك بكثير. يمكن استخدامه في:

-**العقود الذكية:** وهي عقود رقمية يمكن تنفيذها تلقائيًا دون تدخل طرف ثالث.

-**إدارة سلسلة الإمداد:** يمكن تتبع المنتجات من المنشأ إلى الوجهة النهائية عبر البلوك تشين.

-**التصويت الإلكتروني:** يمكن استخدام البلوك تشين لضمان نزاهة عملية التصويت وحمايتها من التلاعب.



1- شخص ما يطلب معاملة

2- يتم بث المعاملة المطلوبة إلى شبكة نظير إلى نظير (P2P) مكونة من أجهزة كمبيوتر، تعرف بالعقد (Nodes)."

3- الشبكة تتحقق من صحة المعاملة وحالة المستخدم باستخدام الخوارزميات المعروفة

4- المعاملة المُحققة يمكن أن تتضمن العملات الرقمية، العقود، السجلات، أو معلومات أخرى

5- بمجرد التحقق منها، يتم دمج المعاملة مع معاملات أخرى لإنشاء كتلة جديدة من البيانات للسجل.

6- ثم تتم إضافة الكتلة الجديدة إلى البلوك تشين الحالي بطريقة دائمة ولا يمكن تعديلها.

7- تمت المعاملة.

2) عملية التحقق في نظام البلوكتشين

2-1) مقدمة

في نظام البلوكتشين، لا يمكن إضافة كتلة جديدة إلى السلسلة دون عملية التحقق. هذه العملية، التي تُعرف أيضًا بـ التعدين، تعتبر أساسًا لعمل البلوكتشين. فهي لا تقتصر فقط على تأكيد صحة المعاملات، بل

تساعد أيضًا في تحديد ترتيب هذه المعاملات بشكل زمني، وتضمن حيادية النظام، كما أنها تُمكّن الأجهزة المختلفة (أو ما يُعرف بـ العقد) من الاتفاق على حالة النظام في لحظة معينة.

2-2) التحقق والتعدين

في البلوكتشين، يتطلب الأمر عملية تحقق دقيقة قبل إضافة أي كتلة جديدة. هذه العملية، التي تتم عن طريق عمال المناجم، تتضمن التحقق من صحة المعاملات المعلقة. بمعنى آخر، عند إجراء معاملة مثل تحويل عملة رقمية من شخص إلى آخر، لا يمكن قبول المعاملة في الشبكة إلا بعد أن يتم التحقق منها.

2-3) دور عمال المناجم في الشبكة

عند قيام الأشخاص بشراء أو بيع عملات البيتكوين أو أي عملة رقمية أخرى، تُرسل المعاملة إلى النظام، حيث يتم بث مفتاح سري أو رمز عبر الشبكة. عندها يتولى عمال المناجم عملية التحقق.

يتم التحقق من صحة المعاملات بواسطة العقد، وهي أجهزة الكمبيوتر المتصلة بشبكة البلوكتشين. هؤلاء العمال يحققون المعاملات باستخدام نسخ من معلومات البلوكتشين التي تتوفر علنًا. ولكن لا يمكن قبول المعاملة إلا بعد أن يُثبت عمال المناجم صحتها عبر آلية خاصة تُسمى إثبات العمل.

2-4) إثبات العمل work proof والتجزئة التشفيرية hash

عملية إثبات العمل تعتمد على دالة تجزئة تشفيرية معقدة، وهي خوارزمية خاصة تُستخدم للتحقق من المعاملات بشكل آمن. هذه الخوارزمية توفر حماية عالية، حيث تضمن أن المعاملة لا يمكن تعديلها أو التلاعب بها. وعليه، تُعتبر هذه العملية حجر الزاوية الذي يحمي النظام من الهجمات أو التلاعبات.

في سياق تعدين العملات الرقمية مثل "بتكوين"، يتم استخدام "قيمة التجزئة (Hash) "للتأكد من صحة المعاملات وحمايتها. قيمة التجزئة هي سلسلة مكونة من أرقام وحروف تمثل معلومات معينة بطريقة غير قابلة للتعديل.

الهدف من التعدين هو العثور على قيمة تجزئة معينة تطابق معيارًا محددًا تفرضه الشبكة، وهو يسمى "التجزئة المستهدفة .(Target Hash) "للوصول إلى هذه القيمة، يقوم عمال المناجم بتغيير جزء من البيانات المستخدمة في عملية التجزئة.

2-5) "nonce

الـ) nonce اختصار لـ "Number Only Used Once" أو "رقم يُستخدم مرة واحدة فقط") هو قيمة عددية يتم إضافتها إلى البيانات التي سيتم تجزئتها. عند إجراء عملية تجزئة، تكون هذه القيمة جزءًا من المدخلات التي تُعطى للدالة الرياضية التي تُنتج التجزئة. الفكرة هي أنه عندما يُغير عمال المناجم هذه القيمة (الـ nonce)، سيؤدي ذلك إلى تغيير النتيجة الناتجة من عملية التجزئة.

2-6) طريقة عمل التعدين ؟

البيانات الأساسية: عمال المناجم لديهم معاملة معينة (مثلاً، تحويلات بين الأشخاص) بالإضافة إلى رأس الكتلة (Block Header) الذي يحتوي على بعض المعلومات مثل:

التجزئة الخاصة بالكتلة السابقة.

الطابع الزمني.(Timestamp)

القيمة المستهدفة.(Target Hash)

تغيير الـ :"nonce" يبدأ عامل التعدين بمحاولة تجزئة البيانات بعد إضافة قيمة nonce معينة، يبدأ عادةً من 0.

حساب التجزئة: يتم حساب التجزئة باستخدام خوارزمية تجزئة مثل .SHA-256 هذه الخوارزمية تحول البيانات المدخلة (بما في ذلك قيمة الـ nonce) إلى سلسلة طويلة من الأرقام والحروف (قيمة التجزئة

مقارنة النتيجة: يتم مقارنة التجزئة الناتجة مع "التجزئة المستهدفة" التي تحددها الشبكة. الهدف هو أن تكون قيمة التجزئة الناتجة أصغر من أو تساوي هذه القيمة المستهدفة.

الاستمرار في التغيير: إذا كانت التجزئة الناتجة لا تطابق الهدف، يقوم عامل التعدين بزيادة قيمة الـ nonce) مثلاً من 0 إلى 1، ثم إلى 2، وهكذا) ويحاول مرة أخرى. تتكرر هذه العملية حتى يصل إلى تجزئة تفي بالشرط المطلوب.

اكتشاف الحل: بمجرد أن يجد عامل التعدين قيمة nonce التي تولد تجزئة تتطابق مع التجزئة المستهدفة، يُعتبر قد حلّ اللغز، ويتم إضافة الكتلة إلى سلسلة البلوكتشين، ويحصل على مكافأة.

الخطوات باستخدام مثال عملي:

1. إعداد البيانات:

لديك بيانات معينة تريد تجزئتها، مثل المعاملات في شبكة البلوكتشين.

أيضًا، لديك رأس الكتلة الذي يحتوي على بعض المعلومات مثل:

التجزئة الخاصة بالكتلة السابقة.

الطابع الزمني.

قيمة nonce التي سنبدأ بتعديلها.

تجزئة مستهدفة تحددها الشبكة.

2. تحديد الهدف: نفترض أن التجزئة المستهدفة هي تجزئة تبدأ بـ أربعة أصفار (0000.)

3. بدء التعدين: يبدأ عامل التعدين بمحاولة إيجاد قيمة nonce التي تجعل التجزئة الناتجة تبدأ بأربعة أصفار. في هذا المثال، نبدأ بـ nonce = 0.

البيانات المدخلة للتجزئة هي مزيج من المعاملات السابقة، الطابع الزمني، التجزئة السابقة، و nonce. لنفترض أن البيانات هي كالتالي:

Data = "Previous Block Hash + Transactions + Timestamp + Nonce"

عندما نحسب التجزئة باستخدام الـ SHA-256 مثلاً (خوارزمية التجزئة المستخدمة في البتكوين)، سنحصل على ناتج مثل:

SHA-256("Previous Block Hash + Transactions + Timestamp + Nonce = 0") = ""abcd1234efgh5678

هذه التجزئة abcd1234efgh5678 لا تبدأ بـ 4 أصفار، لذلك لا تطابق الهدف.

4. زيادة الـ nonce ومحاولة جديدة:

الآن، يقوم عامل التعدين بزيادة قيمة الـ nonce بمقدار واحد، ويقوم بحساب التجزئة مرة أخرى:

Data = "Previous Block Hash + Transactions + Timestamp + Nonce = 1

ونحسب التجزئة:

SHA-256("Previous Block Hash + Transactions + Timestamp + Nonce = 1") = "efgh5678ijkl9012"

هذه التجزئة أيضًا لا تبدأ بـ 4 أصفار.

-تكرار العملية:

يستمر عامل التعدين في زيادة قيمة الـ nonce وحساب التجزئة حتى يصل إلى قيمة حيث تكون التجزئة الناتجة تبدأ بـ 4 أصفار. لنفترض أن بعد عدة محاولات وصل إلى:

البيانات المدخلة مع:nonce = 2500

"Data = "Previous Block Hash + Transactions + Timestamp + Nonce = 2500

عندما يحسب التجزئة لهذه البيانات:

SHA-256("Previous Block Hash + Transactions + Timestamp + Nonce = 2500") = "0000abcdef123456"

هذه التجزئة تبدأ بـ 4 أصفار، وبالتالي تطابق الهدف!

إضافة الكتلة إلى البلوكتشين:

بمجرد أن يجد عامل التعدين هذه التجزئة الصحيحة (التي تبدأ بـ 4 أصفار)، يُعتبر قد حل اللغز وأكمل عملية التعدين بنجاح. يتم إضافة الكتلة الجديدة إلى سلسلة البلوكتشين، ويحصل عامل التعدين على المكافأة (مثلًا بعض البتكوين.(

توضيح أكثر:

الـ "nonce" هو الرقم الذي يقوم العامل بتعديله باستمرار في محاولاته المختلفة.

التجزئة هي النتيجة التي تنتج عن تطبيق خوارزمية SHA-256 على بيانات المدخلات (التي تشمل الـ "nonce").

التجزئة المستهدفة هي قيمة تكون أصغر من أو تساوي التجزئة المستهدفة التي تحددها الشبكة، وفي المثال الذي ذكرناه، الهدف هو أن تكون التجزئة تبدأ بـ 4 أصفار.

لماذا هذه العملية صعبة؟

الخوارزمية التي تُستخدم لحساب التجزئة هي خوارزمية رياضية معقدة، وبمجرد أن تقوم بتغيير الـnonce ، تتغير التجزئة بشكل كامل. بمعنى آخر، تغيير قيمة صغيرة جدًا في البيانات المدخلة (مثل زيادة nonce بمقدار 1) يؤدي إلى تغيير جذري في النتيجة.

هذا يجعل العثور على التجزئة الصحيحة عملية صعبة ومستهلكة للوقت، وتحتاج إلى ملايين المحاولات (أو أكثر) للوصول إلى الحل.

التعويض لعمال المناجم

في المقابل، يُكافأ عمال المناجم على جهودهم في تقديم قوة الحوسبة التي تحافظ على أمان الشبكة. هذا التعويض يُعتبر الحافز الأساسي لهم، وهو ما يعفي البلوكتشين من الحاجة إلى نظام مركزي للتحقق من المعاملات.

البروتوكولات البديلةRipple :

على الرغم من فعالية نظام البلوكتشين القائم على التعدين، توجد بروتوكولات جديدة مثلRipple ، التي تعتمد على إجماع بين العقد بدلاً من الحاجة إلى عمال مناجم. في هذا النظام، يمكن للعقد الاتفاق على التغييرات في الشبكة في غضون ثوانٍ، دون الحاجة إلى إثبات العمل. هذه البروتوكولات الجديدة تقدم حلولًا أسرع وأكثر كفاءة من النظام التقليدي القائم على التعدين.

مستقبل البلوكتشين

مع تقدم تقنيات البلوكتشين، من المتوقع أن تصبح هذه الأنظمة أكثر كفاءة وفعالية. من خلال تحسينات مستمرة في الخوارزميات وتقنيات التحقق، ستتمكن الشبكات اللامركزية من تقديم خدمات أسرع وأكثر أمانًا، مما يجعل استخدامها في مختلف المجالات أكثر شيوعًا وفاعلية.