



البلوك تشين Blockchain

دليل المبتدئين لفهم التقنية التي تقوم
عليها البيتكوين والعملات الرقمية الأخرى

م. إيلي القزي

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الفهرس

كلمة الناشر

4

المقدمة

6

الفصل الأول

11 نبذة تاريخية عن تقنية البلوك تشين

الفصل الثاني:

أساسيات البلوك تشين: إدارة المعاملات

15 الرقمية

18 كيف نتعامل مع المعاملات المالية؟

20 ما هو دفتر الحسابات الموزع (Distributed ledger)؟

26 البلوك تشين والبيتكوين

27 بلوك تشين البيتكوين

28 التشفير

الفصل الثالث

30 SHA-256 Hashing Algorithm

36 دور المعدنين

41 تعدين البيتكوين بنظام الدفع من أجل التشغيل

44 استخدام البلوك تشين خارج نطاق البيتكوين

الفصل الرابع

- 46 العملات الرقمية المشفرة بخلاف البيتكوين
 47 الإيثريوم (Ethereum)
 54 الجوليم (Golem)
 57 الريبيل (Ripple)

الفصل الخامس

- تطبيقات البلوك تشين: تخزين البيانات الكبيرة
 والخصوصية والبيانات الشخصية
 61
 69 تحقيق الربح من تقنيات البلوك تشين
 82 عقبات وتحديات تقنية البلوك تشين
 83 السرعة
 85 التطوير
 88 الحوسبة الكمية (Quantum computing)

الفصل السادس

- 90 اللمسة الإنسانية أو مشكلة نسبة 51%
 94 مستقبل البلوك تشين

الخلاصة

- 97



كلمة الناشر

للحصول دورًا هامًا في تبني الموضوعات الهامة المتعلقة بالتوفير والادخار، وترشيد الاستهلاك، وإدارة الميزانية الشخصية، وتوضيح المفاهيم الاقتصادية بشكل مبسط، وتجنب الوقوع في الأزمات المالية والديون، والتعريف بالبنوك وما يتعلق بها، وكيفية تنمية الأموال بفهم جيد وذكاء من خلال فتح مصادر رزق جديدة، والعمل على مساعدة الفرد والمجتمع على التسلح بكل هذه الأمور، وتحقيقها بكفاءة بكافة السبل والإمكانات المتاحة.

كما تهدف الحصة إلى نشر الوعي والثقافة بين الأفراد والمجتمعات بأهمية هذه الأمور، وكيفية تفعيلها بأفضل الطرق الممكنة، وتوعيتهم بأحدث التقنيات المالية المستقبلية.

وعطفا على كل ذلك ارتأى فريق عمل الحصة أن يقدم هذه المادة للمساهمة في رفع الوعي بالعمليات والمحافظ الرقمية، حيث أنها ستأخذ مساحة من حياتنا خلال السنوات القادمة، ومن المهم أن نكون على وعي بها.



المقدمة

نظرًا للانتشار الواسع الذي تكتسبه العملات الرقمية المشفرة مثل البيتكوين حول العالم كل يوم، فقد أدى الاهتمام المتزايد من وسائل الإعلام الكبيرة إلى إزالة الغموض وإلقاء الضوء على مصطلح «البلوك تشين».

لقد أصبح مصطلح «البلوك تشين» أحد المصطلحات الرنانة في عالم التكنولوجيا والقطاعات المالية كما يتزايد استخدامه في مجالات متعددة.

هناك كثير من الغموض يحيط بمفهوم البلوك تشين..

- فماذا يعني مصطلح البلوك تشين؟
- وما تقنية البلوك تشين؟
- وما الذي تقدمه البلوك تشين؟
- وكيف تعمل؟
- وما أهمية البلوك تشين بالنسبة لنا؟

لا تتم الإجابة على هذه الأسئلة عادةً بشكل كافٍ في المجلات و«المقالات التحليلية» التي تتعامل مع العملات الرقمية والتطبيقات الأخرى التي تستخدم

البلوك تشين؛ ونتيجة لذلك فالكثير من الناس لا يفهمون بصورة كاملة هذه التقنية الجديدة لتحويل الأموال وتطبيقاتها في المستقبل.

أحد التحديات التي تواجه من يحاول تعلم البلوك تشين هي أن الكثير من التفاصيل الخاصة بهذه التقنية تتضمن عمليات رياضية معقدة يصعب استيعابها بالنسبة لمن لا يملك شهادات علمية متقدمة في علوم الحاسوب الآلي أو من ليس لديهم خلفية مسبقة في عالم العملات الرقمية المشفرة.

إن لم تخطط لأن تصبح مطوّرًا وأن تنشئ تطبيقات بلوك تشين خاصة بك، فيمكنك أن تكتفي بفهم شامل لكيفية عمل البلوك تشين على المستوى العملي دون الحاجة لتعلم تطبيق أي خوارزميات.

هدف هذا الكتاب ليس التعمق في المعادلات الرياضية المستخدمة في تشفير التطبيقات المعتمدة على البلوك تشين، ولكن هدفه هو أن يكون مقدمة لنطاق

أوسع ومقدمة للمفاهيم التي تقوم عليها تقنية البلوك تشين.

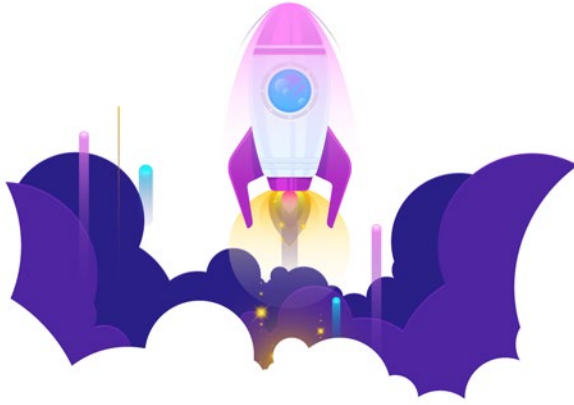
فإننا سنتخذ منهجية عملية في شرح كيفية استخدام البلوك تشين في الحياة العملية وكيفية عملها، ولماذا يتم إدخال هذه التقنية كتطوير ثوري في عالم التكنولوجيا بواسطة الكثير من الآراء البارزة حول العالم؟

مع ظهور الإنترنت تغيرت حياتنا اليومية تمامًا، ويعتقد كثير من الناس بأن تطبيقات تقنية البلوك تشين ستصبح نموذجًا مشابهًا لما قام به الإنترنت في حياتنا؛ فالبلوك تشين هي تكنولوجيا أساسية يمكنها إعادة تشكيل طبيعة المؤسسات والصناعات والاقتصاد العالمي، وقبل أن نمضي قُدُمًا في الحديث عن البلوك تشين لنرجع مرة أخرى إلى بعض الأساسيات:

ما البلوك تشين؟ وكيف تعمل؟ وما الذي تقوم به بالضبط؟

هذه هي بعض الأسئلة الأساسية التي سنجيب عليها من خلال هذا الكتاب، ولكن أولاً قبل أن نبدأ في استكشاف تقنية المستقبل؛ فمن المفيد أن نلقي نظرة عامة على تاريخ هذه التقنية.

من أين أتت فكرة البلوك تشين؟



الفصل الأول

نبذة تاريخية عن تقنية البلوك تشين

ظهر مفهوم «البلوك تشين» لأول مرة في عام 2008 بواسطة شخص يدعى «ساتوشي ناكاموتو - Satoshi Nakamoto» كجزء من الفكرة الخاصة بعملة البيتكوين الرقمية، نشر «ساتوشي» دراسة تقنية وأرسلها إلى البريد الإلكتروني الخاص بقائمة من المعروفين باهتمامهم بالعملات الرقمية المشفرة، وقد وَصَّحَتْ هذه الدراسة المبادئ الأساسية التي تقوم عليها كل من عملة البيتكوين وتقنية البلوك تشين التي تعتمد عليها البيتكوين.

بعد ذلك بفترة قصيرة، في عام 2009م، تم وضع أول تقنية بلوك تشين موضع التنفيذ عندما قام «ساتوشي» بتعيين أول عملة بيتكوين وطرحها للتداول، وقد حققت البيتكوين اليوم شهرة عالمية، وتم قبولها كعملة معترف بها بواسطة العديد من الجهات، ويمكنك الآن شراء أي شيء بداية من تذاكر الطيران حتى الدورات التعليمية على الإنترنت باستخدام البيتكوين، حتى شركة مطاعم «كنتاكي» بدأت في قبول البيتكوين!

وقد ظهرت الكثير من العملات الرقمية على مدار السنوات العشر الماضية والتي تعرف عادة باسم «العملات الرقمية المشفرة»، والتي تستخدم تقنية البلوك تشين لإدارة المعاملات المالية، وسنلقي نظرة على بعض من هذه العملات في الفصول التالية لهذا الكتاب، ولكن من المهم أن نتذكر دائماً بأن تطبيقات البلوك تشين قد وصلت إلى ما هو أبعد من عالم العملات الرقمية.

بينما كانت العملات الرقمية المشفرة وخاصة البيتكوين أولى التطبيقات التي تستخدم البلوك تشين، فقد بدأت الكثير من الصناعات الأخرى في استكشاف تقنية البلوك تشين واستخدامها كطريقة للقيام بمجموعة كبيرة من العمليات، والتي تشمل العقود الذكية وتخزين البيانات وإدارة الموارد، ومن خلال هذا الكتاب سنلقي نظرة على العديد من الطرق المختلفة التي تم استخدام تطبيقات البلوك تشين فيها، سواء للحصول على عملات رقمية مشفرة أم في غيرها من المجالات.

من أكثر التفاصيل الغامضة في تاريخ تقنية البلوك تشين هي هوية من قام بإنشائها، فعلى الرغم من وجود الكثير من النظريات إلا أنه لم يتمكن أحد من كشف الهوية الحقيقية لهذا الشخص الذي يُدعى «ساتوشي ناكاموتو - Satoshi Nakamoto» وسواء كان «ساتوشي» فردًا واحدًا أم مجموعة من الأشخاص فلا نعرف هويته مطلقًا، ومع ذلك فالشيء الأكيد هو أن مساهمة هذا الشخص أو هذه المجموعة في مستقبل التكنولوجيا هي مساهمة عظيمة بشكل لا يوصف؛ فالكثير من المفكرين البارزين من داخل مجال التكنولوجيا يتنبئون بالإمكانية الثورية التي ستحدثها تقنية البلوك تشين ولديهم كل الأسباب المنطقية لذلك!



الفصل الثاني

أساسيات البلوك تشين إدارة المعاملات الرقمية

يوجد العديد من المفاهيم الأساسية التي تجعل من تقنية البلوك تشين مناسبة تمامًا لإدارة المعاملات الرقمية؛ ففي هذه الأيام يعتبر مجال العملات الرقمية المشفرة هو التطبيق الأشهر والأكثر شيوعًا للبلوك تشين؛ حيث يتم استخدام البلوك تشين في إدارة المعاملات المالية التي تتم بصورة رقمية بمبدأ الند للند (Peer to Peer).

وعلى الرغم من أن تطبيقات البلوك تشين غير مقتصرة على المعاملات المالية الرقمية إلا أننا سنبدأ هنا في استكشاف استخدام البلوك تشين في العالم الواقعي، ولقد ظهرت العملات الرقمية وعلى رأسها البيتكوين كنوع جديد من الأصول المالية الفريدة من نوعها، وقبل ظهور الأصول المالية كان إطار البلوك تشين يقدم نموذجًا لإعادة هيكلة المؤسسات وكيفية تنظيم القدرة وتوزيع القيمة، ولكننا ما زلنا في المراحل المبكرة من استكشاف إمكانيات تقنية البلوك تشين، وما زال المجال قيد التطوير بطريقة متسارعة، ولا نستبعد قدرة البلوك تشين على إعادة تشكيل طبيعة

الحكومات والشركات الفردية والاقتصاد العالمي خلال العقد القادم.

ومن أجل تكوين صورة أوضح عن كيفية عمل البلوك تشين فمن الجيد أن نبدأ بإلقاء نظرة على العملات الرقمية مثل البيتكوين، فتعتبر العملات الرقمية حتى الآن أكثر التطبيقات الراسخة لتقنية البلوك تشين، ففي حالة العملات الرقمية، أو "العملات المشفرة"، فإن تقنية البلوك تشين تُستخدَم لإدارة المعاملات المالية، وقبل أن نلقي الضوء على كيفية عمل نموذج البلوك تشين فمن المفيد أن نلقي نظرة على تاريخ إدارة المعاملات المالية.

كيف يمكننا إدارة المعاملات المالية؟

لطالما اعتمدنا منذ قرون على مؤسسات مركزية، مثل البنوك والحكومات للعمل كوسطاء لحفظ وتحويل الأصول المالية.

يحتفظ معظم الناس بأكثر أموالهم في البنوك، وتوجد الكثير من المميزات لهذا الأمر؛ فعلى سبيل المثال إذا كانت كل مدخراتك المالية التي جمعتها طوال عمرك مدفونة تحت أرضية منزلك ثم تعرض هذا المنزل لحريق فلا شك أنك ستكون في ورطة كبيرة. فتقدم البنوك وعدًا بتأمين وحماية أصولك المالية في مقابل رسوم تحويل مختلفة، فنحن نثق في الاحتفاظ بأموالنا آمنة في البنوك في مقابل نسبة من أموالنا، وبمرور الوقت فقد أصبح هذا النموذج من الاحتفاظ بالأموال في البنوك هو السائد، وفي هذا العالم الرقمي المتسارع فإن الكثير من الأشخاص قد بدّءوا في البحث عن بدائل للنموذج التقليدي لحفظ الأموال في المؤسسات المركزية.

واليوم حيث تتم المعاملات أكثر فأكثر بصورة رقمية، فقد أصبح الاحتياج أكبر لضمان الثقة وتأمين هذه المعاملات؛ فتوجد معظم المعلومات المالية في شكل بيانات، والمعاملات المالية هي في النهاية عبارة عن عمليات نقل للملفات التي تحمل هذه البيانات، وبدون وجود عملية آمنة فسيكون من السهل جدًا التلاعب بهذه البيانات؛ حيث تقوم القراصنة بشكل منظم بتعطيل خدمات البنوك وماكينات ATM وغيرها من الأماكن التي يتم فيها حفظ وإجراء المعاملات المالية، وأحد أكبر التحديات لإدارة المعاملات المالية بمبدأ الند للند هي «مشكلة الإنفاق المزدوج»، أو كيفية ضمان عدم قيام شخص بصرف نفس الأموال مرتين!

عند وصول البييتكوين إلى الساحة، فقد قدمت حلًا لهذه المشكلة وجعلت المعاملات المالية المباشرة بنظام الند للند ممكنة بطريقة آمنة، لا تتطلب وجود ثقة بين الطرفين أو الوثوق في طرف ثالث وسيط مثل البنوك، وكان هذا الحل هو البلوك تشين.

ما دفتر الحسابات الموزع (Distributed Ledger)؟

في الوقت الذي مهدت فيه البيتكوين الطريق لتقنية البلوك تشين، فقد ظهرت الكثير من التطبيقات اللاحقة التي تشمل -على سبيل المثال لا الحصر- العملات الرقمية الأخرى والتي تعتمد على إطار عمل تقنية البلوك تشين، وأحد المفاهيم الأساسية التي أدت إلى نجاح تقنية البلوك تشين هي استخدامها لنظام دفتر الحسابات الموزع.

إذن فما دفتر الحسابات الموزع؟

يعني دفتر الحسابات الموزع ببساطة كما يظهر من معنى الكلمة، أنه مجرد قائمة من الملفات، ببدلاً من الحفاظ على هذه القائمة في مكان واحد كما هي الآن في البنوك والمؤسسات المالية المركزية، فإن دفتر الحسابات الموزع يتم تخزينه في كثير من الأماكن المختلفة تلقائياً، وليست كل أشكال دفاتر الحسابات الموزعة عبارة عن بلوك تشين، ولكن كل تقنيات البلوك تشين تستخدم إصدارًا ما من دفتر الحسابات الموزع.

تعتبر اللامركزية أحد المفاهيم الأساسية التي تعتمد عليها تقنية البلوك تشين، فمن خلال الاحتفاظ بعدة نسخ من ملف المعاملات المالية في أماكن مختلفة حول العالم والتي تكون مرئية لأي شخص، لم تعد هناك حاجة إلى طرف ثالث «موثوق فيه» للعمل كوسيط لإدارة المعاملات.



شبكة اتصال مركزية



شبكة اتصال لا مركزية

ولكي نتعمق أكثر في كيفية عمل دفتر الحسابات الموزع فلنتخيل موقفًا افتراضيًا: افترض أن لديك ملفًا تقوم فيه بتدوين كل معاملاتك المالية التي قمت بها خلال السنة، وكنت تقوم في أي وقت تكسب أو تنفق فيه أي أموال بتدوين كل هذه التفاصيل في هذا الملف، مع العلم أنه لا يوجد سوى هذا الملف، وكنت تحتفظ به في مكتبك، وهنا فإنه توجد الكثير من الأمور التي قد تحدث في مثل

هذا السيناريو؛ فقد يتعرض منزلك لحريق، أو قد يقوم لص بالتسلل إلى منزلك والتلاعب بهذه المعلومات، كما أنك قد تنسى إضافة بعض المستندات، وتصل في النهاية إلى حسابات غير منطقية، وينتهي بك الأمر إلى وضع مؤسف.

بدلاً من وجود ملف واحد، تخيل أن لديك مئات الآلاف من النسخ المتطابقة لنفس الملف وموجودة على مكاتب الكثير من الأشخاص حول العالم، وفي أي وقت يتم فيه إضافة أي تفاصيل إلى الملف، فسيتم فحص كل المعلومات في كل النسخ للتأكد من إضافة الأرقام بطريقة صحيحة، وسيتم إضافة المعلومات الجديدة إلى كل النسخ في نفس الوقت، وفي حالة وجود ملف يحتوي على معاملة غير موجودة في باقي الملفات الأخرى فيمكننا افتراض وجود خطأ في هذا الملف.

والآن؛ لكي يتمكن أي شخص من التلاعب بمعلوماتك فيجب عليه أن يتلاعب بكل واحدة من هذه الملفات الموجودة في كل أنحاء العالم في نفس الوقت.

من الواضح أن استخدام نظام حفظ الملفات في المكاتب هو أمر غير عملي، ولكن في العالم الافتراضي يُعدّ هذا التشبيه وصفًا دقيقًا لكيفية عمل دفتر الحسابات الموزع.

إن كل معاملة مالية في تقنية البلوك تشين سواء كانت صغيرة أم كبيرة فإنه يتم تسجيلها في «بلوك»، وكل بلوك يحتوي على طابع زمني خاص يرتبط بالبلوك السابق، ويسمح ذلك لأجهزة الحاسب الآلي بفحص كل معاملة مالية محتملة مقارنة بالمعاملة السابقة، وإذا لم يتم إضافة الطوابع الزمنية بطريقة صحيحة في معظم أجهزة الحاسب الآلي فإن المعاملة سيتم رفضها، وإذا توافقت معظم الطوابع الزمنية فإن هذا المعاملة المقترحة سيتم اعتبارها صحيحة، وسيتم التحقق من هذه المعاملة وإضافتها إلى بلوك جديد في السلسلة أو كملف جديد على دفتر الحسابات. وبعد ذلك، فإن أي معاملة تالية سيتم مراجعة مطابقتها للطابع الزمني الخاص بالبلوك السابق وهكذا.

ولكي يتمكن أي شخص، قرصان على سبيل المثال من إدخال معلومات زائفة في البلوك تشين فيجب عليه تغيير المعلومات ليس في هذا البلوك فقط ولكن في كل بلوك فردي موجود على كل البلوك تشين تلقائيًا عبر معظم أجهزة الحاسب الآلي المشاركة حول العالم، وحتى في ظل هذه التقنية الحالية فإنه من أجل القيام بذلك فسوف يتطلب ذلك كمية هائلة من القوة الحاسوبية وهو أمر يستحيل توفيره؛ لذلك فإن دفتر الحسابات الموزع الخاص بتقنية البلوك تشين مصمم بطريقة آمنة.

ونظرًا لأن كل معاملة يتم مطابقتها مع التاريخ الكامل للمعاملات المالية السابقة من خلال العديد من الأجهزة الموزعة على مستوى العالم، فمن المستحيل لأي شخص أن «يخدع» تقنية البلوك تشين عن طريق محاولة إنفاق نفس الأموال مرتين، فإذا لم تطابق إحدى المعاملات المالية الملف المسجل فسيتم رفض هذا الملف واعتباره غير صالح.

لم يحل هذا الأمر مشكلة «ازدواج الإنفاق» فقط، ولكن أصبحت المعاملات المالية لا تتطلب وجود ثقة بين كلا الطرفين أو الوثوق في طرف ثالث من أجل إجراء المعاملة، فلا يمكن للشخص (أ) مثلاً أن يدعي إرساله للأموال إلى الشخص (ب) «وأنها قد ضاعت أثناء التحويل»، ولا يمكن للشخص (ب) أن يدعي أنه «لم يستقبل أي أموال»، وتكون كل المعاملات المالية مرئية للجميع؛ ومن ثَمَّ فإن كلا الطرفين سيكون قادرًا على رؤية ملف المعاملة المالي على البلوك تشين.

البلوك تشين والبيتكوين

أحد أكثر الجوانب المحيرة وغير المفهومة لتقنية البلوك تشين تظهر عندما نحاول فصلها عن البيتكوين، فكما ذكرنا سابقًا فإن البيتكوين ببساطة هو تطبيق واحد مبني على تقنية البلوك تشين، وهي كذلك أولى وأكبر وأكثر بلوك تشين معروفة في العالم، ويعتبر تطبيق البيتكوين لتقنية البلوك تشين أمرًا مفروغًا منه، بمعنى أنه عندما يتحدث الناس عن «البلوك تشين» فإنهم عادة ما يتحدثون تحديدًا عن نموذج البلوك تشين المستخدم في البيتكوين.

من المهم فهم أن نموذج البيتكوين ليس التطبيق الوحيد لتقنية البلوك تشين، ولكنه واحد من تطبيقات هذه التقنية الواعدة، وتوجد الكثير من العوامل التي تجعل تقنية البلوك تشين المستخدمة في البيتكوين تعمل بهذه الصورة التي نراها، ولكن الأمر يحتاج إلى فحص كل منها من أجل الوصول إلى فهم أكبر لتحديد أي جوانب تطبيق البلوك تشين خاص بالبيتكوين فقط، وأيها خاص بالبلوك تشين بشكل عام.

بلوك تشين البيتكوين

توجد العديد من الجوانب الأساسية التي تعمل معًا لخلق نظام بيئي للبلوك تشين ليكون حكرًا على البيتكوين، فقامت بعض العملات الرقمية الأخرى بتطبيق نماذج مشابهة، ولكن ما يهمنا هنا هو التركيز على البيتكوين وتوضيح كيفية عمل البلوك تشين الخاص بالبيتكوين، فنحن نعلم بالفعل بأن البلوك تشين هي نوع من دفتر الحسابات الموزع، وإذا ما تعمقنا أكثر في فكرة دفتر الحسابات الموزع فقد تظهر بعض الأسئلة:

- كيف يتم التحقق من المعاملات المالية؟
- ومن يقوم بتسجيلها؟
- وكيف يمكن التأكد من صحة هذه المعلومات؟

التشفير

لو تذكرت الفصل السابق الذي تحدثنا فيه عن تاريخ البيتكوين، فقد ذكرنا أن مفهوم البيتكوين قد تم إرساله في البداية إلى قائمة من عناوين البريد الإلكتروني الخاصة ببعض المهتمين بالعملات الرقمية.

• لماذا نستخدم التشفير؟

لقد تطور علم التشفير بسرعة جنبًا إلى جنب مع التكنولوجيا الرقمية كوسيلة لتأمين المعلومات، فلقد كان التشفير عادةً مجالًا غامضًا بدرجة ما وكان يستخدم على مدى واسع في المجالات العسكرية، وفي عصر الإمبراطورية الرومانية فإن «يوليوس قيصر» كان يستخدم التشفير لإرسال رسائل مشفرة إلى كبار قادته.

وفي عصر التكنولوجيا الرقمية الذي نعيشه الآن، فإن التشفير قد أصبح جزءًا أساسيًا من حياتنا اليومية؛ نظرًا لأن القراصنة ومنتطي الشخصية قد أصبحوا أكثر

انتشارًا من ذي قبل، فإن ممارسات التشفير الأساسية قد أصبحت مطلبًا أساسيًا كوسيلة حماية للحفاظ على البيانات الشخصية للأفراد، وسواء كنا على علم بها أم لا فإن معظمنا اليوم قد أصبح مُلمًا بتقنيات التشفير الأساسية، مثل استخدام كلمات المرور للوصول إلى حسابات البريد الإلكتروني، أو تمكين التسجيل الثنائي على هواتفنا الذكية كذلك. ويعتمد معظمنا على معاملات مالية مشفرة بصورة منتظمة، بداية من القيام بعمليات الشراء على الإنترنت حتى الوصول إلى الحسابات البنكية.

لن يكون من المفاجئ بعد ذلك أن تعتمد البيتكوين على خوارزميات مشفرة آمنة للتحقق من المعاملات المالية وإدارة البلوك تشين.



الفصل الثالث

SHA-256 Hashing Algorithm

تستخدم البيتكوين SHA-256 Hashing Algorithm، ألقا الطريقة الفعلية التي يتم من خلالها هذا الأمر فلن يتم تناولها في هذا الكتاب، ولكن من المفيد أن تعرف فكرة عامة أساسية عن الموضوع، فهناك طريقة وحيدة للتفكير في هذا الأمر وهي تخيل صندوق أسود، هذا الصندوق الأسود هو SHA-256 Hashing Algorithm، ولن نشغل بالنا بما يحدث في داخل هذا الصندوق وكل التفاصيل الصغيرة الخاصة بالدالة نفسها، ولكننا سنكمل حديثنا مع افتراض حدوث بعض الأمور الرياضية الغامضة بداخل هذا الصندوق.

الجانب الأهم بالنسبة لنا، هو أنه يمكنك أخذ أي نوع من البيانات -أيًا كان حجمها- ووضعها في هذا الصندوق، وفي النهاية فإن كل البيانات الرقمية حتى البيانات المعقدة مثل الأفلام التي قد تصل حجمها لعدة جيجابايت تكون عبارة عن تسلسل من الآحاد والأصفار أو «البتات»، وعندما نقوم بإدخال أي نوع من البيانات في الصندوق الأسود الخاص بتقنية SHA-256 Hashing Algorithm، فإن بتات البيانات سيتم معالجتها، ويمكننا

التفكير في هذه الأجزاء بـ «إعادة ترتيبها» بطريقة محددة داخل الصندوق، وعندما تتم معالجة البيانات في الصندوق الأسود، فإنها تنتج سلسلة من 256 بت من الرموز التي تبدو عشوائية وغير مفهومة، ويمكن اعتبار هذا التسلسل بمثابة «بصمة بيانات» فريدة تمثل تمامًا البيانات التي قمنا بإدخالها.

CryptoMENA

SHA
256

fcd4fc8a2613c7221ba7a257475a916ea
d8cc90ae6e63f47f4ec2dde1043145a

(البيانات المدخلة هنا هي كلمة «CryptoMENA» التي يتم إدخالها باستخدام (SHA-256 Hashing Algorithm)

الحقيقة هي أن ما يبدو «بدون معنى» ظاهريًا ليس كذلك في حقيقة الأمر.

إن SHA-256 Hashing Algorithm خاسمة، بمعنى أنه إذا قمت بوضع نفس البيانات في هذا «الصندوق الأسود» فسوف تحصل على نفس تسلسل النتائج أو «بصمة البيانات» في كل مرة، فإذا قمت بتطبيق هذه الخوارزمية على كلمة «hello» فسوف تحصل على تسلسل متطابق من 64 رمزًا كما ترى في الأعلى.

من المعايير الأخرى لهذه الدالة هي أنها وحيدة الاتجاه، يعني ذلك بأنه لا يمكنك أخذ تسلسل النتائج وتحويلها مرة أخرى إلى بيانات أصلية؛ لذا ففي هذا المثال لن يمكننا إعادة عكس العملية باستخدام «البيانات غير المفهومة» للحصول على كلمة «hello» الأصلية.

أحد الأمثلة على كيفية استخدام ذلك هو كيفية التحقق من الملفات مثل ملفات PDF، فإذا قمت بتوقيع عقد وأرسلته إلى أحد ما باستخدام البصمة الخاصة بخوارزمية SHA-256 Hashing Algorithm فسيتمكن اختبار Hashing Algorithm لمعرفة ما إذا قد تم تغيير

أي بت من البيانات. أمّا إذا تم إدخال المستند في SHA-256 Hashing Algorithm وحصلت على تسلسل نتائج مطابق فهذا يعني بأن الملف لم يتم تغييره.

وعلى الجانب الآخر، فإذا حدث أقل تغيير في البيانات؛ فإن بصمة البيانات التي ستظهر ستكون مختلفة بالكامل بغض النظر عما إذا كان هذا التغيير بحسن نيّة نتيجة خطأ مطبعي يمكن إصلاحه أو حالة التلاعب في البيانات. فإن طبيعة التغيير في البيانات الأصلية أمر غير مهم بالنسبة للخوارزمية؛ لأن نتيجة SHA-256 Hashing Algorithm ستكون مختلفة تمامًا ما لم تكن البيانات مطابقة بنسبة 100%، ففي المثال السابق إذا قمت بتغيير كلمة «cryptoMENA» إلى «CryptoMENA» أو «CRYPTOMENA» فسوف تحصل على تسلسل نتائج مختلف تمامًا.

والآن بعد أن أصبحت لدينا معرفة أساسية عن كيفية عمل SHA-256 Hashing Algorithm فقد تتساءل عن علاقة ذلك بتقنية بلوك تشين البيتكوين، ويمكن أن

يكون ذلك واحدًا من أكثر المفاهيم المعقدة والصعبة الفهم بخصوص ما يتم تحت نطاق بروتوكول البيتكوين، ومن أجل فهم دور SHA-256 Hashing Algorithm في نموذج «خوارزمية إثبات العمل» التي تؤدي وظيفة البيتكوين فسندرج إلى التعمق في معرفة كيفية مشاركة أجهزة تعدين البيتكوين في النظام البيئي للبلوك تشين.

دور المعدّنين

توجد الكثير من التفسيرات حول كيفية التحقق من المعاملات المالية للبيتكوين، ويمكننا القول بأن الأمر أشبه إلى فكرة: «يقوم المشتغلون بالتعدين بحل المشكلات الرياضية المعقدة لإضافة بلوك إلى سلسلة البلوك تشين في مقابل الحصول على مقابل»، هذا الأمر صحيح وهو توضيح دقيق للصورة بشكل كامل، وعندما يتعلق الأمر بفهم التركيب الأكبر لتقنية البلوك تشين أثناء تطبيقها على البيتكوين فقد وجدنا أن هذا التفسير بسيط للغاية، ومن أجل توصيل فكرتنا فنحن بحاجة إلى استكشاف آليات تعدين البيتكوين عن قرب.

يشتمل التعدين على حسابات معقدة مصممة لاكتشاف تركيبات معينة من أرقام عشوائية تسمى «الرقم الخاص (nonces)»، وتمتزج هذه الأرقام الخاصة بالمعلومات المتعلقة بمعاملات مالية محددة بالبيتكوين لتكوين تسلسل من SHA-256 Hashing Algorithm الذي ينطبق عليه رموز شديدة التحديد.

توجد البيانات المتعلقة بالبيبتكوين في العنوان الرئيس أو في أول «قطعة أو (chunk)» من أي بلوك في تقنية البلوك تشين التي يتم عرضها في شكل تسلسل SHA-256 Hashing Algorithm؛ لذلك فإن أول «قطعة» من التسلسل -والتي توجد في كل بلوك- تحتوي على معلومات عن المعاملات المالية الموجودة في هذا البلوك، مثل الوقت وكمية البيبتكوين والعنوان وتفاصيل أخرى، ويتكون باقي التسلسل عن طريق إيجاد رقم خاص، وعندما يضاف هذا الرقم إلى البيانات الخاصة بالمعاملة فسوف ينتج تسلسلاً من SHA-256 Hashing Algorithm يطابق المعايير المستهدفة المذكورة مسبقاً.

إذًا، فما المعايير التي تحدد ذلك؟ يجب إنشاء البلوك الخاصة بالبيبتكوين وفقاً لمجموعة من القواعد حتى يتم اعتبارها صحيحة من خلال النموذج المتوافق الذي يدير كل «nodes» على شبكة البيبتكوين، ويتم كتابة هذه المجموعة من القواعد المحددة للمعايير التي يجب مطابقتها لتوليد بلوك صالح في الكود الرئيس

لبرنامج البيتكوين، و«القواعد» هي مجموعة من الوظائف المكتوبة في شكل كود ++C الموجود في كل جهاز أو «node» والمرتبطة بشبكة البيتكوين.

يحتاج من يقوم بالتعدين إلى إنشاء بلوك وفقاً لهذه المجموعة من القواعد، ففي البداية يحتاج البلوك إلى أن يتضمن معلومات عن أحدث معاملات البيتكوين، ثم يجب على من يقوم بالتعدين إيجاد رقم خاص، وعندما يضاف هذا الرقم إلى بيانات المعاملة المالية فسوف ينتج تسلسلاً من SHA-256 Hashing Algorithm يطابق المعايير المحددة بواسطة نظام البيتكوين (فعلى سبيل المثال قد تكون هذه المعايير هي احتواء التسلسل على 15 صفراً في صف واحد).

لا توجد أي طريقة أخرى لإيجاد هذا الرقم الخاص بخلاف استخدام طريقة «القوة العمياء (Brute-force)، والتي تعني بشكل أساسي المحاولة والخطأ، وتقوم أجهزة التعدين بتجربة الكثير من الأرقام العشوائية بسرعة كبيرة حتى تجد أي منها يعمل، وعندما يقوم المعدّنون

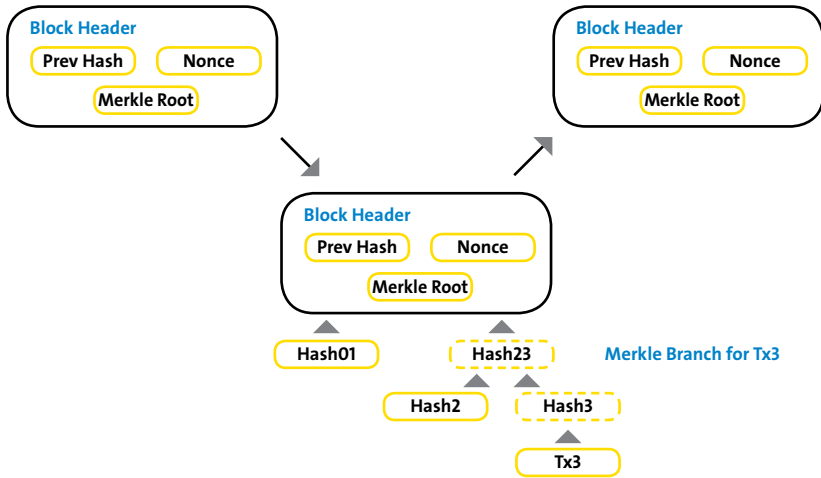
بعملية «حل بلوك» فإن هذا يعني بأنه قد وجد الرقم الخاص الذي ينتج SHA-256 Hashing Algorithm التي تطابق معايير بلوك صحيح، ثم يمكنهم تسجيل إجاباتهم على شبكة البيتكوين، وسوف تقوم «nodes» الأخرى بفحص المعاملة والتأكد من أنها صحيحة.

ولكي نعطيك فكرة عن مدى صعوبة إيجاد الرقم الخاص فإن شبكة البيتكوين تنتج أكثر من 500 كوادريليون Hashing Algorithm في الثانية، وهذه هي كل محاولات إيجاد رقم خاص لكي يحقق النتيجة المطلوبة، وحتى مع هذا الحجم الكبير من العمل فما زال الأمر يستغرق متوسط 10 دقائق لحل بلوك واحد أو لإيجاد رقم خاص صالح، وعندما يقوم المعدّنون بحل بلوك بنجاح فإنهم يَحْضُون على كمية صغيرة من البيتكوين.

«Merkel Root» هو مرجع لمفهوم رياضي يعرف بشجرة ميركل، وفي هذه الحالة فإن «Merkel Root» هو Hashing Algorithm لكل المعاملات المالية التي تشكل البلوك، وتخضع تفاصيل كل المعاملات المالية

الخاصة بكل شخص إلى Hashing Algorithm كذلك،
ولذلك فإن «Merkel Root» بالفعل عبارة عن Hashing
Algorithm خاص بكل Hashing Algorithms هذه.

Longest Proof-of-work Chain



Bitcoin Whitepaper

تعدين البيتكوين بنظام الدفع من أجل التشغيل

ربما سمعت من قبل أن هناك معدّنين للبتكوين، يحصلون عليه بطريقة مجانية ولا يكلفهم أموالاً.. هذا الأمر غير صحيح جملة وتفصيلاً حتى في الأيام الأولى لظهور البيتكوين؛ بل إن الأمر قد صار أكثر حدة هذه الأيام؛ لأن تعقيدات حل البلوك تشين تزيد مع الوقت وفقاً لحجم البيتكوين المتداول.

لقد أصبحت خصوصية تسلسل SHA-256 Hashing Algorithm أكثر تعقيداً بمرور الوقت (وهو ما يعرف باسم «الهدف الصعب»؛ مما جعل عملية توفير كمية الطاقة اللازمة لإيجاد رقم خاص أكثر صعوبة؛ فنحن نحتاج الآن إلى معدات خاصة حتى يمكننا تعدين البيتكوين بنجاح بأي طريقة مجدية، ولذلك فإن معظم المعدّنين يقومون بإضافة مواردهم في مجموعات تتشارك في العمل وفي النتائج.

يستخدم المعدّنون معداتهم لاختبار Hashing Algorithm بمعدل سريع جداً بشكل لا يصدق، وكما تعلم

فإن هذا النوع من الطاقة الحاسوبية يتطلب الكثير من الكهرباء وهي غير مجانية بالتأكيد، والسبب الذي يساهم في استمرار عملية تعدين البيتكوين يرجع في جزء منه إلى فكرة المشاركة، وتتحمل كل المجموعة تكلفة التعدين، وبدون هذه التضحية فلن يمكنهم الحصول أي ربح، والسبب الوحيد الذي يجعل الناس يقومون بتعدين البيتكوين هو اعتقادهم بأن المقابل الذي سيحصلون عليه من تعدين البيتكوين يستحق دفع هذه الفاتورة الباهظة من الكهرباء.

عندما يجد من يقوم بالتعدين رقمًا خاصًا فعليًا فإن نتائجه سيتم فحصها والتحقق منها عن طريق شبكة البيتكوين الأوسع؛ فإذا كانت البيانات صحيحة فسوف يقدمون خوارزمية إثبات العمل ومن ثمّ يمكنهم استقبال مكافآتهم، أمّا إذا وجدت باقي «nodes» على شبكة البيتكوين وجود بعض الأمور التي لا تطابق المعايير المحددة سواء بسبب اتباع القواعد بشكل غير صحيح أم بسبب عدم القدرة على تقديم رقم خاص يطابق المعايير الموضوعية، ففي هذه الحالة فسوف

يتم رفض البلوك وسيخسر من يقوم بالتعدين كل أمواله وموارده، فعلى سبيل المثال إذا قام شخص بمحاولة «الإنفاق المزدوج» فسيتم اكتشافه وسيتم رفض البلوك الخاص به.

ونظرًا لاستخدام البيتكوين لخوارزمية إثبات العمل فإنه من المستحيل افتراضيًا خداع أو قرصنة البلوك تشين، وفي البيتكوين فإن التعدين يكون بنظام الدفع من أجل التشغيل، ويشترط الدفع من أجل التشغيل العادل لعملية التعدين. وليس هذا فقط، بل إن من لا يقومون بالتعدين بنزاهة فإنهم سيخسرون أموالهم بسبب تكلفة الكهرباء اللازمة لتشغيل أجهزة التعدين.

استخدام البلوك تشين خارج نطاق البيتكوين

عندما ننظر إلى بلوك تشين البيتكوين فيمكننا أن نرى أنها تتكون من العديد من الأجزاء المختلفة التي تعمل معًا لإنشاء تركيب كلي للنظام البيئي، وقد ألقينا الضوء على ثلاثة من هذه المكونات وهي فكرة دفتر الحسابات الموزع، واستخدام SHA-256 Hashing Algorithm، ونموذج خوارزمية إثبات العمل.

أي من هذا خاص بالبيتكوين؟ وأيها داخل في مفهوم تقنية البلوك تشين نفسها؟ هذان سؤالان جيدان، ولكن الإجابة قد تعتمد على خبرة من يوجه السؤال؛ فيوجد بعض الجدل حول تحديد أين تنتهي البيتكوين وأين تبدأ البلوك تشين، أو ما معايير بلوك تشين البيتكوين الضرورية لإنشاء البلوك تشين الذي يعمل بطريقة عملية؟!

على مستوى المبتدئين، وعندما نزيل اللبس بين البيتكوين والمفهوم الأساسي للبلوك تشين، فسوف نصل في النهاية إلى فكرة دفتر الحسابات الموزع الذي

يحتوي على ملف بالمعاملات المالية، فإن معرفة نوع المعاملات وكيف يتم إدارتها والتحقق منها وتسجيلها هو أمر قد يُمكنُ لتطبيقات البلوك تشين المختلفة القيام به بطرق مختلفة.

وعندما نبدأ في إلقاء الضوء عن قرب على كيفية عمل تطبيقات البلوك تشين، ومعرفة كيف تضمن هذه التطبيقات الأمان؟ وهل هي مفتوحة ومتاحة لأي شخص أم لا؟ وهل تعمل بطريقة لا مركزية أم لا؟ وكيف تقوم بتشفير المعلومات؟ وهل تتم المعاملات المالية فيها دون تحديد الهوية؟ وما نوع المعاملات المالية التي يتم إدارتها؟ وهل تستخدم خوارزمية إثبات العمل؟ وهل يوجد نموذج متوافق آخر؟ فإن إجابات كل هذه الأسئلة ستظهر عندما نبدأ في إلقاء الضوء على تقنية البلوك تشين وتطبيقها على مجالات أخرى بخلاف البيتكوين.



الفصل الرابع العملات الرقمية المشفرة بخلاف البيتكوين



الإثيريوم (Ethereum)

إن مجال العملات المشفرة هو مجال متغير بشكل ملحوظ، فكل شيء يتغير يوميًا، وهناك المزيد من العملات التي يتم تطويرها في كل وقت، وما كان يُعدُّ ثورة في عالم العملات الرقمية يوقًا ما فقد يختفي لاحقًا، ولكن بعض العملات الرقمية قد نجحت في الوصول إلى ثبات نسبي؛ فتعتبر البيتكوين هي رائدة العملات المعتمدة على تقنية البلوك تشين، ولكن الإثيريوم قد لفتت الكثير من الانتباه منذ ظهورها في نهاية عام 2013.

لقد تم تطوير الإثيريوم بواسطة المبرمج «Vitalik Buterin»، وعلى عكس البيتكوين التي تستخدم كعملة رقمية فقط، فإن الإثيريوم هي منصة معتمدة على البلوك تشين لتطوير تطبيقات لا مركزية تعمل

باستخدام تقنية «العقود الذكية»، وبينما تعمل البيتكوين كنظام دفع إلكتروني بنظام الند للند، فإن بلوك تشين الإيثيريوم تعمل من خلال كود يشكل تطبيقات لا مركزية.

قد يكون من المفيد النظر إلى الإيثيريوم كفكرة مشابهة للهواتف الذكية، فالهاتف الذكي يستخدم نظام تشغيل عام مثل الأندرويد أو iOS، ويمكن لأي شخص أن يقوم بإنشاء تطبيقات تقوم بعدد من الأشياء المختلفة التي تعمل وفق نظام التشغيل، والإيثيريوم تشبه نظام التشغيل: فهي بروتوكول يمكن بناء تطبيقات عليه.

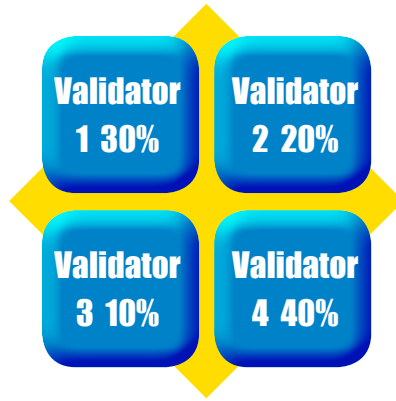
تعتبر العملات الرقمية أحد التطبيقات التي تعتمد على الإيثيريوم ويشار إلى هذه العملة باسم «الإيثيريوم»، بينما تعرف تقنيًا باسم إيثير، وقد يؤدي هذا الأمر إلى حدوث بعض الخلط بين العملة والمنصة نظرًا لأن كل منهما يحمل اسم «الإيثيريوم»، ولكن من المهم أن نتذكر بأن العملة هي مجرد تطبيق واحد لبلوك

تشين الإيثريوم، وفي مقابل الحفاظ على بلوك تشين الإيثريوم فإن المعدّنين لعملة «الإيثريوم» سيحصلون على مكافأة بعملة الإيثريوم.

يعمل تعدين الإيثريوم منذ بدايته على نموذج خوارزمية إثبات العمل (Proof of work) مثل البيتكوين، وبحلول عام 2017م أعلن الفريق المسئول عن الإيثريوم عن خطط للتحول إلى نموذج خوارزمية إثبات الملكية (Proof of stake).

إن فهم الفرق بين هذين النظامين للتحقق من المعاملات المالية بتقنية البلوك تشين هو أمر جوهري لفهم السياق الخاص بأحد أكثر الأمور الشائكة والملحة في المجال الأوسع لتقنية البلوك تشين في هذه الأيام؛ فعندما ننظر إلى «خوارزمية إثبات العمل» باعتبارها جزءًا لا يتجزأ من بروتوكول البيتكوين فسوف نقوم بتغطية كيف يضطر معدني البيتكوين إلى الاستثمار في معدات تعدين خاصة تتطلب الكثير من الطاقة الكهربائية لتشغيلها من أجل حل بلوك واحد.

تعمل خوارزمية إثبات الملكية (Proof of stake) بطريقة مختلفة قليلاً؛ ف نموذج خوارزمية إثبات الملكية أشبه قليلاً إلى فكرة المقامرة، فبدلاً من مصطلح «المشتغلون بالتعدين» فإن الإيثريوم يتحرك في اتجاه استخدام مصطلح «المنفذون»، ويساهم المنفذون بمبلغ محدد من أموالهم (عملة الإيثريوم) من أجل حل بلوك واحد.



في هذا المثال، فإن أربعة منفذين «يساهمون» بأموالهم لحل بلوك، كأن يكون للمنفذ رقم 4 أعلى سهم، ومن ثمّ أعلى احتمالية لحل البلوك والحصول على أكبر عائد.

تتشابه خوارزمية إثبات الملكية مع خوارزمية إثبات العمل في القيام بمعادلات غير مفهومة، والتي تقلل من التأثير الحقيقي للنظام البيئي لاستهلاك الطاقة الذي يحدث نتيجة التعدين، ويقوم المنفذون بالمساهمة بأموالهم من أجل حل البلوك مثل الدخول في مراهنة، ولكن ماذا يحدث عند محاولة «الغش»؟ في خوارزمية إثبات الملكية التي تُسمّى «Casper» نعرف ماذا سيحدث في حالة وجود شخص يريد الغش؟! إن الأموال الخاصة بمن يحاول التلاعب بأي شيء ستختفي ببساطة! وسوف يقوم النظام بحذفها من التداول؛ لذلك فإن دوافع المنفذين للمشاركة الجادة تكون عالية وتكون عواقب محاولة «تنفيذ» معاملة مالية زائفة مكلفة كذلك.

تعمل كل من خوارزمية إثبات الملكية وخوارزمية إثبات العمل على تحقيق نفس النتيجة في النهاية؛ فكل منهما يهدف إلى التحقق من البلوك وإضافته إلى البلوك تشين بطريقة تكون فيها الشبكة الأوسع متوافقة مع التحقق من هذا البلوك، ويصل كلا النموذجين إلى نفس النتيجة ولكن من خلال بروتوكول مختلف.

يجب عليك كمستثمر أو مشارك في مجال البلوك تشين أن تكون معتادًا على التعامل مع نماذج متوافقة ومختلفة بشكل جيد يسمح بتعميق فهمك بكيفية عمل المشاريع في الواقع، وسوف يعمل التحول في نموذج عمل الإيثيريوم من خوارزمية إثبات العمل المعتمد على التعدين إلى خوارزمية إثبات الملكية المعتمدة على المصادقة على فصل الإيثيريوم عن البيتكوين من حيث التركيب، ولكن يمكنك كذلك مراجعة بعض من الطرق الأخرى التي تختلف فيها كلتا التقنيتين.

لقد ذكرنا بالفعل أن الإيثيريوم التي تعتبر عملة في جزء منها هي في الأساس منصة لتطوير تطبيقات غير مركزية، وقد تكون فكرة التطبيقات اللامركزية فكرة غير واضحة إلى حد كبير؛ وذلك لأنها طريقة جديدة تمامًا لتنظيم المعلومات. ولكن لماذا نحتاج إلى منصة معتمدة على البلوك تشين لتشغيل التطبيقات؟ هذا هو السؤال الذي ما زال الكثير من المبرمجين يبحثون عن إجابة له، لكن إجابة واحدة مع ذلك تتماشى مع المفهوم الذي يشار إليه في عالم البرمجة بمصطلح «الوضع (state)».

يشير مصطلح الوضع ببساطة إلى حالة أي تطبيق أو برنامج في نقطة معينة من الوقت، فأحد الأشياء التي تجعل تقنية بلوك تشين الإثيريوم مختلفة عن بلوك تشين البيتكوين هي «المعاملات» التي تحدث في تقنية بلوك تشين الإثيريوم والتي يمكنها تنفيذ أي كود؛ لذلك فإنه من الممكن تشغيل هذه البرامج نتيجة للمعاملات التي تتم على منصة الإثيريوم، وفي كل مرة يتغير فيها أي شيء في التطبيق فإن وضع التطبيق سيتغير كذلك، وتحفظ تقنية بلوك تشين الإثيريوم بسجل لكل تغيير يحدث في وضع التطبيق، فعلى سبيل المثال يمكن دفع عقد ذكي عند تسليم العمل كلياً من خلال بلوك تشين الإثيريوم.

إذا لم تستوعب هذا الشرح جيداً فلا تقلق لأنك لست بحاجة إلى فهم الجوانب التقنية الخاصة بتغير وضع التطبيق، وكما يقال فإن الأمر يحتاج إلى أن تكون فليماً بهذه المفاهيم إذا كنت تخطط للدخول في مجال البلوك تشين كمستثمر، ولكي نعرف أكثر عما يمكن للإثيريوم القيام به فسوف نلقي نظرة على أحد التطبيقات اللامركزية التي تم تطويرها على منصة الإثيريوم.



الجوليم (Golem)

الجوليم هو مشروع معروف معتمد على الإيثريوم، وفكرته بسيطة جدًا، فالكثير من الناس لديهم أجهزة حاسب، والكثير منهم لا يستخدمها طول الوقت، وحتى في حالة استخدامها فإنهم لا يستخدمونها بكامل طاقتها فيما يتعلق بطاقة المعالجة، وفي نفس الوقت توجد الكثير من المجالات التي تحتاج إلى كميات هائلة من القوة الحاسوبية لتنفيذ مهام محددة، فعلى سبيل المثال إن إنتاج فيديو أمر يستهلك الكثير من الطاقة الحاسوبية ويحتاج لوقت طويل وقد يُبْطِئ من جهازك، كما تتطلب الكثير من الدراسات العلمية كذلك تحليلًا مكثفًا للبيانات، وأشكالًا أخرى من عمليات المعالجة المتقدمة.

فكرة الجوليم مصممة لتسمح للأشخاص بتأجير طاقة معالجة أجهزة الحاسب غير المستخدمة إلى أشخاص آخرين يحتاجون إليها في مشاريعهم، ومن خلال استخدام تركيب لامركزي فإن هذا يعني بأنه يمكن للأشخاص حول العالم المساهمة بكميات صغيرة من الطاقة الحاسوبية الخاصة بهم من أجل إكمال مهام تحتاج لطاقة حاسوبية مكثفة والتي قد تحتاج في المعتاد إلى جهاز حاسب عالي الطاقة لإنجازها.

ومن خلال استخدام نظام معتمد على تقنية البلوك تشين والذي يسمح بتنفيذ الكود أثناء تنفيذ المعاملات فإن الجوليم تسعى إلى توفير أجهزة حاسب فائقة وغير مركزية ومتاحة لأي شخص، ونظرًا لأنه يتم تسجيل التاريخ الكامل من وضع البرنامج على بلوك تشين الإيثيريوم؛ فإن المشاركين يمكنهم ضمان عدم استهلاك أي شخص لطاقة أكبر من الطاقة التي دفع ثمنها والعكس صحيح، ومن أجل ضمان المعايير الأخرى الخاصة بمعاملاتهم.

تملك منصة الجوليم كذلك عملتها الرقمية الخاصة المعتمدة على الإيثريوم، والتي يمكن للمشاركين من خلالها شراء وبيع مواردهم، وبالطبع يمكن لأي شخص الاستثمار فيها بغض النظر عما إذا كان مشتركًا في المنصة بشكل مباشر أم لا، وتعتبر الجوليم أحد أشهر وأنجح التطبيقات المبنية على منصة الإيثريوم حتى تاريخ كتابة هذا الكتاب.



الريبيل XRP

لقد تحدثنا بالفعل عن بعض الطرق التي تختلف فيها الإيثريوم عن البيتكوين، ولكن الشيء الوحيد الذي لم نذكره هو أن الإيثريوم على عكس البيتكوين، يتم إدارتها بواسطة فريق مركزي من أشخاص معروفين، ويحدد هذا الفريق كل ما يتعلق بالإيثريوم، مثل الانتقال من خوارزمية إثبات العمل إلى خوارزمية إثبات الملكية، ومن ثَمَّ فإنه يمارس مستوى معين من التحكم في المنصة بطريقة أكثر مركزية من البيتكوين، وعلى الرغم من ذلك فإن الإيثريوم ما زالت منصة بلوك تشين مفتوحة ومتاحة لأي شخص.

والريبيل هو مثال آخر على التفاوت الموجود في تقنية البلوك تشين؛ فالريبيل هو مصطلح مزدوج، فهو يشير إلى عملة الريبيل الرقمية، وإلى شركة التكنولوجيا

التي تعمل في مجال البلوك تشين، ويركز الريبل بدرجة أقل على المعاملات بنظام الند للند، ولكنه يركز بدرجة أكبر على الصناعة المالية نفسها بالشراكة مع البنوك والمؤسسات المالية لدمج تقنية البلوك تشين في بنيتها التحتية.

ما زالت الريبل مثيرة للجدل بين المتحمسين للعملات المشفرة، ولكنها تدعي حل بعض المشكلات الموجودة في البيتكوين، وأبرز المشكلات التي قامت بحلها هي مشكلة فترة الانتظار التي تحدث أثناء عملية التحقق؛ وذلك لأن معاملات الريبل تتم بصورة فورية، ومع ذلك فإن نموذج الريبل يختلف عن نموذج «خوارزمية إثبات العمل» الخاص بالبيتكوين، وبدلاً من ذلك فإن الريبل تعتمد على شبكة مركزية من الخوادم «الموثوقة» والتي تطرح بعض التساؤلات الكبيرة للمهتمين بتقنية البلوك تشين ممن يفضلون البنية غير المركزية.

يمثل مفهوم دفتر الحسابات الموزع أثناء تطبيقه من خلال تقنية البلوك تشين إعادة تصور أساسية للمنظمات المؤسسية للتحويل من النموذج الهرمي

إلى الشبكة الموزعة، وبالنسبة للكثير من المستثمرين فإن هذا الأمر هو مفتاح الثورة المحتملة لتقنية البلوك تشين، فبالرغم من أن تطبيقات المعلومات غير المركزية كثيرة ولكن أغلبها تقريبًا لم يتم تفعيله بشكل كامل.



الفصل الخامس تطبيقات البلوك تشين

تخزين البيانات الكبيرة والخصوصية والبيانات الشخصية

نظرًا لأننا نعيش الآن في عصر رقمي متطور باستمرار، فإن الكثير من التقنيات التي تم تطويرها قبل وجود الإنترنت قد تم تطبيقها وتطويرها لتناسب مع الطبيعة الجديدة للعالم المتصل عن طريق شبكة الإنترنت، فبدلاً من كتابة الخطابات فإننا نقوم الآن بإرسال رسائل البريد الإلكتروني على سبيل المثال، وفي ظاهر الأمر فإنه لا يبدو هناك أي اختلاف بين كلتا الطريقتين، ولكن في بعض الحالات الأخرى قد يوجد فرق بينهما.

وبغض النظر عن شعورك تجاه هذا الأمر فإنه لا يمكننا إنكار أن هناك المزيد والمزيد من الأشياء التي أصبحت موجودة في الإنترنت، ومن هنا فقد ظهر هذا المفهوم «إنترنت الأشياء (Internet of Things)» والذي يعرف اختصارًا (IoT)، فبعض الأجهزة مثل أجهزة مراقبة معدل ضربات القلب، والسيارات ذاتية القيادة، وحتى الشلاجات قد أثبتت جدارتها في السوق، وبالطبع فإن كلاً منا تقريبًا معتاد على حمل هاتف ذكي في

أغلب الوقت لفحص المعلومات المتعلقة بتقنية GPS، وتحديث تطبيقات وسائل التواصل الاجتماعي، وإدارة المعاملات المالية، ... وغيرها من الاستخدامات الكثيرة. وكل المجالات التي قد تخطر في بالك في حياتك فستجدها مرتبطة بالإنترنت بالفعل، أو ستجد أن لها احتمالية كبيرة للارتباط بالإنترنت في المستقبل القريب، وعلى الرغم من وجود الكثير من المميزات للثورة الناشئة في مجال «التكنولوجيا الذكية»، فهناك كذلك بعض المخاوف والتحديات الكبيرة.

وفي الوقت الذي قد تبدو فيه بعض الأشياء مثل شبكات التواصل الاجتماعي والآلات الذكية وأجهزة FitBits أفكارًا مختلفة كليًا، ولكنها مشتركة في بعض الأمور كذلك، فبشكل أساسي فإن كل منها ينتج بيانات: بيانات عنك بالأخص، فلو تذكرت عندما تحدثنا في جزء SHA-256 Hashing Algorithm، فقد ذكرنا بأن كل البيانات الرقمية يمكن اختصارها في النهاية إلى أرقام وأحاد، ومن هذا المنطلق، فإن معدل ضربات قلبنا وتاريخ بحثنا على جوجل ليس مختلفًا فيما يتعلق بنوده، فنحن ننتج بيانات باستمرار سواء أكانت أخبار

أليكسا المساعد الشخصي لأمازون لطلب المزيد من المناشف الورقية، أم كانت تختص بالبحث على جوجل عن صور لطفل ينظر إلى صورة أسد، أم كانت تتبَّعًا لجدول مواعيد عملك باستخدام تطبيق ما، أم كانت أيّ أداة يمكن حملها.

- أين تذهب هذه البيانات؟
- من يملك هذه البيانات؟
- ما البيانات التي يمكن معرفتها عنك أثناء عملية التحويل؟

ستقود هذه الأسئلة أي شخص إلى التفكير فيها بعناية، وعلى الرغم من أن التعمق في إجابة هذه المجموعة من الأسئلة هو أمر خارج نطاق هذا الكتاب، إلا أن الأمر يستحق أن نلقي نظرة عامة عليها، فباختصار توجد بعض الشركات الكبيرة متعددة الجنسيات التي تشتري بياناتك وتبيعها لشركات أخرى، ولكن ماذا تفعل هذه الشركات بهذه البيانات؟ سؤال جيد! بالطبع تقوم هذه الشركات بتوجيه الإعلانات بناء على تاريخ بياناتك وكلنا نعرف ذلك بالتأكيد، ولكن ماذا أيضًا؟ أحد الأمور التي

تجعل الإجابة على هذا السؤال صعبة هي أنه لا أحد يعرف بالفعل ماذا يحدث، كما أن مجال جمع البيانات هو مجال غير معرف وغير محدد بشكل دقيق.

لننظر إلى هذا المثال، فلتفترض بأنك وجدت ورقًا صغيرًا تحت إبطك في يوم من الأيام، فلا شك في أنك ستشعر بالتوتر وستهرع إلى جوجل وتقضي ساعات كثيرة في الانتقال بين المواقع المختلفة لقراءة مقالات عن السرطان. والآن لنفترض وبغض النظر عن الشركة التي تستقبل بياناتك أنها قد وضعت يدها على هذا البحث المكثف الذي قمت به، فربما قد يلاحظون أيضًا بأنك قد قمت بالبحث عن رقم الهاتف الخاص ببعض الأطباء في بلدك ممن يُجرون فحوصات السرطان، وفي هذا الوقت فقد بدأت في التفكير بخصوص سياسة التأمين الصحي أو عمل تأمين على حياتك على سبيل الاحتياط.

إكمالًا للموقف الافتراضي السابق، فإذا استطاع أي مقدم لخدمة التأمين على الحياة من خلال بعض وسطاء البيانات أن يعرف بأنك كنت تبحث مؤخرًا عن معلومات عن السرطان فما الذي يمكنه فعله بهذه المعلومات؟

حتى إذا كنت قد أخبرت شخصًا عن هذا الورم، وحتى إذا لم يتم فحصك وتشخيص حالتك بواسطة طبيب، فهل يمكن لشركة التأمين المحتملة هذه أن تستنتج شيئًا من بياناتك عندما تتفق معك على قيمة التأمين أو تحدد ما إذا كانت ستقدم لك تأمينًا على الحياة أم لا؟

هذا مثال واحد من بين مجموعة واسعة من الأمور الأخلاقية والقانونية التي تظهر عندما تبدأ بالفعل في التفكير بخصوص الآثار المترتبة على معرفة بياناتنا، وكيف يتم التنقيب عنها، ومن «يملكها»، ومن يمكنه الوصول إليها.

كلما زاد دمج التكنولوجيا في مجتمعنا وعلى كل مستويات حياتنا، وكلما انتشرت شبكات الاتصال، فإن حجم وتنوع بياناتنا سيصبح أكبر بالتأكيد. فأسئلة مثل ما الأفلام والموسيقى التي نسمعها وتاريخ تسوقنا ومعرفتنا السياسية وميولنا النفسية وارتباطنا بشبكات التواصل الاجتماعي والأجهزة التي نستخدمها والكثير.. الكثير، إنما هي معلومات يتم جمعها عادة نتيجة لإهمالنا مراجعة سياسة اتفاق الاستخدام عند بداية استخدام خدمة معينة.

نعم إنه أمر مخيف، ولكن... ما علاقة كل ذلك بتقنية البلوك تشين؟

سؤال جيد؛ إن العلاقة بين الخصوصية والتكنولوجيا هي مشكلة تمتد في الكثير من الصناعات والنقاشات المعاصرة، وبالنسبة للمهتمين بتقنية البلوك تشين والعملات المشفرة فإن الخصوصية هي إحدى المخاوف الكبيرة، فعندما يتعلق الأمر بمفهوم «الخصوصية»، فإن الكثير من المراقبين بما في ذلك وسائل الإعلام الكبيرة تضع هذا الافتراض: بأن «من يهتمون بالخصوصية هم فقط من لديهم شيء يخفونه»؛ وقد أدى ذلك إلى تقديم الكثير من التقارير عن العملات الرقمية المشفرة على وجه الخصوص، وتفترض هذه التقارير بأن المشكلة الأساسية لهذه التقنيات هي أنه يمكن استخدامها في الأنشطة الإجرامية.

ونظرًا لأن المزيد والمزيد من مجالات حياتنا قد أصبحت متصلة بالإنترنت فقد يبدو من الصعب تقبل فكرة أن فرض مزيد من الرقابة على بيانات الأفراد الشخصية ومعاملاتهم المالية وإدارتهم لأصولهم المالية قد

يشكل أو ينطوي على سلوك إجرامي، ويصر الكثير من المدافعين عن الخصوصية على أن الخصوصية هي أمر ضروري لتحقيق رفاهية الفرد وتحقيق ديمقراطية فعالة في المجتمع.

وبدلاً من الاعتماد على مؤسسات مركزية لتوفير خدمات في مقابل الحصول على بياناتنا، فإن النماذج المعتمدة على تقنية البلوك تشين قد بدأت في ترجيح فكرة تحويل المعلومات إلى شكل غير مركزي آمن ولا يحتاج إلى فكرة الثقة، (وتعني كلمة «عدم الحاجة إلى الثقة» هنا بأن المشاركين لن يكونوا بحاجة إلى وضع ثقتهم في مؤسسة مركزية لإدارة المعاملات المالية والاحتفاظ بالملفات وتوزيع الأموال وتخزين البيانات، إلخ).

إن تطبيقات البلوك تشين في مجالات مثل إدارة المعلومات الشخصية ومثل الملفات الصحية لها نتائج واعدة للغاية، وبدأت في كسب الكثير من انتباه المستثمرين ورواد الأعمال والشركات الكبيرة والمؤسسات الحكومية.

وبغض النظر عن شعورك تجاه موضوع الخصوصية، فمن الجدير بالذكر ومن منظور استثماري يجب معرفة أن العديد من العملات الرقمية المعروفة قد نشأت مؤكدة على فكرة الخصوصية كعامل هام فيها، وقد ساهمت القدرة على إجراء معاملات مالية مجهولة الهوية بالكامل وأمنة تمامًا في رفع أسهم الكثير من العملات المشفرة في مقدمة سوق العملات الرقمية، مثل عملات Monero و ZCash و Dash. وعلى الرغم من أنه لم يصل أي منها ولو بدرجة قليلة إلى مكانة البيتكوين أو الإيثريوم من ناحية الانتشار العالمي إلا أن العملات الثلاثة تقع من بين أعلى خمسين عملة رقمية من حيث القيمة السوقية.

يمكننا أن نستنتج من نجاح هذه العملات بأن عددًا كافيًا من الأشخاص يعتقدون وجود قيمة في إخفاء الهوية، وهذا هو ما جعل هذه العملات قادرة على المنافسة في هذا السوق الكبير من العملات الرقمية، وكذلك في مجال تقنية البلوك تشين بشكل عام.

تحقيق الربح من تقنيات البلوك تشين

من المهم تذكر أن تقنية البلوك تشين ما زالت تقنية جديدة جدًا، وأن تطبيقات دفتر الحسابات الموزع وأنظمة الند للند اللامركزية ما زالت غير مفعلة بالكامل حتى الآن. وكما هو الحال فبالرغم من أن كل مجال له حدود، كما في مجال الرقميات، فإنه توجد الكثير من الفرص كذلك، وبالطبع فإن طبيعة هذه الحدود تكمن في أن العملات الرقمية هي مجال غير مفهوم بالكامل، ولكن حيث توجد فرص فإنه يوجد كذلك خطر أكبر قد يتعرض له المستخدم حتى في التقنيات المعتادة والأكثر تنظيمًا.

ونظرًا لأن مجال البلوك تشين هو «مجال واعد»، فإن الكثير من أصحاب الأعمال ورواد الصناعة في كثير من المجالات قد بدءوا في الاستثمار واستكشاف البلوك تشين، وقد بدأت شركات التكنولوجيا الكبيرة مثل شركة IBM وشركة مايكروسوفت في استكشاف البلوك تشين بالإضافة إلى الكثير من البنوك وخاصة في أوروبا وآسيا.

كما بدأت الحكومات في الكثير من أنحاء العالم في تطبيق تقنيات البلوك تشين لإدارة الخدمات والملفات العامة، ففي «دولة إستونيا» على سبيل المثال، أصدرت الحكومة بطاقات هوية مشفرة وآمنة للمواطنين باستخدام تقنية البلوك تشين؛ مما يعطي لهم إمكانية الحصول على مختلف الخدمات العامة، كما تقوم حكومة «جورجيا» باستخدام تقنية البلوك تشين لإدارة سندات ملكية الأراضي والمعاملات العقارية، وقامت الأمم المتحدة مؤخرًا بإكمال برنامج تجريبي يستخدم بلوك تشين الإيثيريوم لإدارة توزيع المساعدات الغذائية إلى أكثر من عشرة آلاف لاجئ.

وعلى مدى الأعوام القليلة الماضية، فقد انتشرت الكثير من صناديق التمويل الاحتياطية التي تتعامل بالعملات الرقمية المشفرة وتطبيقات البلوك تشين في كل أنحاء العالم، ووجه الكثير من المضاربين في بورصة «وول ستريت» أنظارهم إلى مجال البلوك تشين، وفي عام 2016م، قامت شركة Overstock أحد أكبر شركات البيع بالتجزئة في الولايات المتحدة الأمريكية بإطلاق

منصة معتمدة على البلوك تشين لتجارة الأسهم، وقد استخدمت الكثير من الشركات الناشئة تقنية البلوك تشين لإدارة عمليات الدفع الصغيرة مقابل رسوم قليلة جدًا، وفي بعض الحالات فقد أمكن استخدام هذه التقنية في التحويلات الدولية والوصول إلى عمليات إرسال الأموال؛ مما يسمح للأفراد بإرسال واستقبال الأموال دون الحاجة إلى البنوك.

تحدث الكثير من التطورات الجديدة يوميًا في مجال البلوك تشين، فبالنسبة لمن يريدون التعمق أكثر والمشاركة والربح من هذه التقنيات الجديدة فإن أهم شيء يمكنهم القيام به هو البقاء على اطلاع، عن طريق قراءة المقالات والانضمام إلى التجمعات على الإنترنت، واستكشاف المشاريع المختلفة التي تكتسب زخمًا حول تقنية البلوك تشين، فكلما كنت أكثر اطلاعًا على مجال البلوك تشين كلما كان من السهل عليك اتخاذ قرارات مبنية على علم بخصوص المشاريع التي تستثمر فيها.

كتطبيق عملي يوجد اثنين من الاتجاهات العامة التي يمكنك المضي فيها قُدًا عند الاستثمار في تقنية البلوك تشين؛ وهما العملات الرقمية المشفرة، وأي مجال آخر من تطبيقات البلوك تشين، وهذه العملات بأي حال من الأحوال لا تتنافى مع تقنية البلوك تشين، وكما رأينا في مشاريع مثل الإيثريوم والريبيل فإنه يوجد عادة بعض اللبس بين المصطلحين أو عند دمج توكن رقمي في تطبيق بلوك تشين معين.

في مجال البلوك تشين، فإن الأسواق والبورصات الناشطة على الإنترنت تعمل وفق فكرة تداول مشابهة لبورصات الأسهم التقليدية، فيمكن للأشخاص تداول العملات النقدية المعتادة مع العملات الرقمية المشفرة أو تداول إحدى العملات الرقمية مع عملة أخرى، ومن ثَمَّ فإنهم يحاولون تحقيق الربح من خلال الاستثمار في العملات التي يعتقدون بأنها ستزيد في القيمة.

يتم التداول بمعظم البورصات بعملة البيتكوين بشكل

أساسي، ومن أجل شراء عملات مشفرة أخرى فلا بد أن يكون لديك بعض البيتكوين لكي تقوم باستبدالها، وعلى الرغم من ذلك فإن بعض العملات والبورصات تسمح بالتداول المباشر بين الأموال النقدية المعتادة والعملات المعروفة باسم «altcoins»، وهو مصطلح شائع الاستخدام للتعبير عن العملات الرقمية المشفرة بخلاف البيتكوين، فيمكنك شراء البيتكوين من خلال العديد من بورصات التداول على الإنترنت أو من خلال العدد المتزايد من ماكينات ATM البيتكوين المنتشرة في عدد من الأماكن حول العالم.

يمكنك اختيار إما التداول المباشر بين عملات رقمية مختلفة أو شراء البيتكوين أو غيرها من العملات الرقمية التي تعتقد بأنها ستكون واعدة، ومن ثمّ يمكنك الاحتفاظ بها على أمل زيادة قيمتها في المستقبل بمرور الوقت، وهناك طريقة واحدة للدخول فيما يُعدّ الآن أكثر مجال نشط لتطبيقات البلوك تشين، فإذا كنت محظوظًا فسيمكنك أن تصبح «مستثمرًا مبكرًا» عند دخولك في تقنية واعدة على وشك الانطلاق بالفعل.

لقد دخل الكثير من الناس في مجال العملات المشفرة من أجل هذا الأمل على وجه التحديد، وخاصة بعد سماع أخبار نجاح البيتكوين، وإذا كنت جديدًا في مجال العملات الرقمية المعتمدة على تقنية البلوك تشين فمن المهم أن تفهم أن هذا المجال هو مجال شديد التقلب، فليس من الغريب أن ترى ارتفاعات وانخفاضات كبيرة في القيمة على مدى ساعات قليلة، وفي الوقت الذي يكون من الممكن فيه كسب الكثير من الأموال فمن السهل كذلك أن تخسر كل أموالك.

إن الوعي بالمخاطر والقيام باستثمارات ذكية في العملات الرقمية المشفرة هو بلا شك أكثر طريقة مباشرة للربح من تقنية البلوك تشين، هذه هي الحقيقة بكل بساطة، وبالنسبة للأشخاص الذين لا يملكون الكثير من رأس المال للاستثمار فإن مفهوم التعدين قد يكون جذابًا للغاية بالنسبة لهم. ولقد ناقشنا بالفعل بعض التحديات المصاحبة لتعدين البيتكوين، فإنك سوف تحتاج إلى شراء معدات خاصة، وتحمل تكلفة الكهرباء، وكذلك ستحتاج إلى طاقة حاسوبية هائلة، إلخ،

فإذا كان رأس مالك قليلاً فإن الاستثمار في عملية تعدين البيتكوين لن يكون الخيار الأفضل بالنسبة لك.

ومع ذلك، فهناك الكثير من العملات الرقمية الأخرى التي يمكن تعدينها مع وجود شروط أقل للبدء فيها، ويمكن لأي شخص أن يتعلم كيفية تحويل جهاز الحاسب الآلي الاحتياطي إلى جهاز تعدين.

إن القدرة على كسب عملات مشفرة من خلال التعدين يمكنها أن تكون طريقة محتملة لتوفير دخل جارٍ من خلال التحقق من معاملات البلوك تشين.

لقد كانت تقنية البلوك تشين الناشئة في مجال العملات الرقمية والكثير من التطوير المبكر لتطبيقات البلوك تشين مرتبطًا بالأصول الرقمية والمعاملات المالية، وعند الحديث عن فكرة الربح من تقنية البلوك تشين فإن الدخول في تطبيق العملات الرقمية المشفرة هو طريق شائع لتحقيق هذا الربح، ولكنه ليس الطريق الوحيد للقيام بذلك، وبينما كانت تقنية البلوك تشين تدخل بطريقة متزايدة إلى مجالات جديدة،

فإن المستثمر الذكي يمكنه إيجاد الكثير من الفروع الرائعة التي يمكنها النمو بشكل جيد جدًا إلى مشاريع عملاقة لها تطبيقات على مستوى العالم وتغير من المستقبل بشكل واضح.

إن الاستثمار في الشركات والمطورين والتقنيات التي تستكشف إمكانيات استخدام البلوك تشين هو أمر يكتسب مزيدًا من الانتشار بين كل المستثمرين، بداية من وادي السيليكون (Silicon Valley) لرواد الأعمال حتى مسؤلوي بورصة وول ستريت.

لا أحد يعرف بالطبع على وجه التحديد ما تطبيق البلوك تشين الذي سيصبح بمثابة «جوجل القادم»، وسيواجه أي مستثمر محتمل؟ بلا شك تحدي تطوير أي من هذه الأفكار لمعرفة أي منها سيكون قاصرًا؟ وأي منها سيكون واعدًا في المستقبل؟ أي منها سيصبح منصات ثورية واعدة؟ وأي منها سيصبح مجرد تقليد رخيص؟

ونظرًا لأنه لا توجد عين سحرية يمكنها رؤية المستقبل، فسوف يمكنك تعزيز احتمالات اختيارك لفكرة رائعة عن

طريق البحث والاستفسار، وهذه هي بعض الأسئلة العامة التي يجب عليك أن تسألها عند اختيار المشاريع التي سيكون لها فرص جيدة للنجاح:

- ما المشكلة التي تحلها هذه التقنية؟
- (هل سيساهم استخدام البلوك تشين بالفعل في تغيير الوضع الحالي؟ هل هي أفضل الحلول؟)
- هل المشروع فعال بالفعل؟ هل هو نشط ويُستخدَم حاليًا أم هو مجرد فكرة غير منفذة على أرض الواقع حتى الآن؟ وإذا لم تكن موجودة بالفعل، فكيف يمكنك ضمان أن هذه الفكرة ستحقق وعودها؟
- كيف تم تكوين البلوك تشين؟ (على سبيل المثال، إذا كان المؤسس يتحكم في 90% من nodes على شبكة الاتصال، فماذا يدل ذلك بالنسبة لهذه الشركة؟)
- ما الخوارزمية التي يستخدمونها؟ هل هي خوارزمية إثبات العمل؟ أم خوارزمية إثبات الملكية؟ أم شيء آخر؟ لماذا اختاروا هذا النظام؟ وكيف يتم تطبيقه؟

- هل هذه الفكرة قابلة للتطوير؟ هل استطاع هذا النظام تحقيق متطلبات قاعدة المستخدمين؟
- كيف يطبق هذا التطبيق مفهوم السرية؟ وهل هذا كافي؟
- هل هذه المنصة آمنة؟ كيف يتم ضمان عملية التأمين؟ هل توجد «ثقة» في مؤسسة مركزية؟
- ما نوع التشفير المستخدم؟
- هل البلوك تشين مفتوحة ومرئية لأي شخص؟
- هل كود المشروع مفتوح المصدر؟
- (وإذا كانت الإجابة لا؛ إذن لماذا؟ وكيف يمكننا تحديد كيفية اتخاذ القرارات والتحقق من صحة المعاملات وما يحدث بالفعل عند استخدام هذه المنصة؟)
- من المسئول عن هذا المشروع؟ هل فريق تطوير المشروع مؤهل بدرجة كافية وله سمعة طيبة؟ وهل شارك هذا الفريق في مشاريع سابقة خاسرة؟ لماذا فشلت هذه المشاريع؟
- هل توجد مشاريع أخرى مشابهة؟ وما الذي يجعل هذا المشروع هو الأفضل؟
- هل تُؤمِنُ بنجاح هذا المشروع؟ هل أنت متحمس بشأنه؟

لا شك في أن هذه القائمة من الأسئلة متعبة، ولكن إذا كنت تفكر بجدية في استثمار أموالك في تقنية البلوك تشين فإن هذه الاعتبارات ستكون مهمة جدًا بالنسبة لك ونقطة جيدة للانطلاق، ومع الاهتمام المتزايد من قبل العديد من الصناعات الكبيرة بتقنية البلوك تشين فلن يكون من المفاجئ معرفة أن الكثير من رواد الأعمال قد قاموا باستثمار أموال كبيرة في تطوير تطبيقات لتقنية البلوك تشين، ولكن بالطبع ليس من المتوقع نجاح كل هذه التطبيقات، كما أن بعض التطبيقات قد تكون واعدة وناجحة أكثر من الأخرى، فبعض المشاريع قد تكون محاولات سليمة النية ولكنها لا تملك أفضل الحلول لمشكلة شائعة، وبعضها قد يكون محاولة احتيالية صريحة.

خذ وقتًا كافيًا حتى تعتاد على المصطلحات والمعاني المستخدمة في مجال البلوك تشين، وعندما تدعي شركة جديدة بأنها توفر منصة بلوك تشين «قابلة للتطوير بنسبة 100%»، فإن المستثمر الجيد سيسأل بالتأكيد عن كيف تمكنوا من تحقيق ذلك بدلًا من أخذ

كلمات الشركة كما هي على ظاهرها، ففي كثير من الأحيان، ستجد أن الشعارات الرنانة مثل «القابلية للتطوير بنسبة 100%» ستكون أقرب إلى «أهداف مستقبلية» أكثر من كونها واقعًا حاليًا.

لا يخفى عليك بأن التهويل التسويقي قد يلعب دورًا كبيرًا في «شعبية» أي شيء، وليست شركات العملات الرقمية المشفرة والشركات المعتمدة على تقنية البلوك تشين مستثناة من هذا الأمر، ويمكن للتسويق أن يكون له تأثيرٌ حقيقيٌّ على كيفية تقييم أي شركة في هذا المجال، فقد يحقق أي مشروع شهرة واسعة، ولكن ستكون فكرة جيدة أن تتعامل مع الاستثمارات المحتملة في هذا المجال بنوع من الحذر، وعلى العكس من ذلك فقد تكون أكثر الأفكار المبتكرة والواعدة في البلوك تشين عبارة عن شركات ناشئة صغيرة لها ميزانيات صغيرة ولا تملك مواقع كبيرة على الإنترنت ولا تحظى باهتمام كبير.

يمكنك عن طريق الإطلاع الدائم والبحث في مجموعة واسعة من المشاريع وتحديد المشكلات التي تعتقد

بأنها سٌحل بأفضل طريقة من خلال تقنية البلوك تشين وكذلك اكتساب خبرة بالتعرف على وجهات النظر البديلة تكوين فهم متعمق لمجال البلوك تشين، ونظرًا لأنه لا يوجد أي ضمانات حول وقت الاستثمار، فإن معرفة ما تبحث عنه سيساعدك كثيرًا على اتخاذ قرارات ذكية، وما زالت تقنية البلوك تشين في مراحلها المبكرة، واتخاذ قرارات ذكية الآن سيؤدي بالتأكيد إلى تحقيق أرباح كبيرة.

عقبات وتحديات تقنية البلوك تشين

يوجد طريقة وحيدة لفهم مفهوم البلوك تشين؛ وهي معرفة كيفية تشكيل معايير متغيرة مع الوقت، وكيفية البقاء آمناً والتصرف في كل الظروف، وحتى إذا استطعت القيام بكل ذلك فإن تحدي الحصول على أشخاص للاستثمار في التقنية الخاصة بك واستخدامها هو تحدي كبير كذلك. وبالنسبة للمهتمين بالدخول في مجال البلوك تشين فإن الأمر يحتاج إلى بعض الوقت لإلقاء نظرة على بعض الجوانب السلبية والمصاعب والعقبات المحتملة التي تواجهها تقنية البلوك تشين في الوقت الحالي.

السرعة

تعتبر السرعة أحد أكبر التحديات التي تواجه البيتكوين وتقنيات البلوك تشين الأخرى التي تستخدم خوارزمية إثبات العمل المعتمدة على البيتكوين؛ لأن تعدين بلوك واحد عملية مستهلكة للموارد، وتشتمل على الكثير من التجارب حتى يمكن إيجاد رقم خاص صحيح لحل البلوك؛ حيث إن تعدين بلوك واحد يستغرق حوالي 10 دقائق.

لا يؤدي ذلك إلى استهلاك كمية هائلة من الطاقة الكهربائية فحسب؛ ولكنه يعني كذلك بأن المعاملات المالية لن يتم التحقق منها بشكل فوري، ففي الواقع قد يستغرق الأمر بعض الوقت حتى يمكنك رؤية انتقال معاملاتك من «مُعَلَّقة» إلى «صحيحة»، ومن الناحية العملية فإن هذا الأمر يجعل من الصعب شراء شيء ما باستخدام البيتكوين في الكثير من الأحوال، فمعظم الناس لا يحبون الانتظار لساعة حتى يتم إنهاء عملية دفع الأموال، وكذلك فإن معظم التجار لا يحبون الانتظار لكي يحصلوا على أموالهم.

وعلى الرغم من هذه المشكلة، فإن عدد الجهات البائعة التي تنوي قبول الدفع عن طريق البيتكوين في تزايد مستمر بشكل يومي، ومع تطوير المزيد من تطبيقات تقنية البلوك تشين فإنه يتم اتخاذ طرق مختلفة للتحكم في سرعة المعاملة المالية وسرعة التحقق منها. فتوفر الريبل على سبيل المثال معاملات فورية، ولكن توجد بعض المخاوف من فكرة البروتوكول المركزي الذي تعتمد عليه الريبل، والذي يجعل الوصول لهذه السرعة أمرًا ممكنًا.

وأنت كمستثمر محتمل في تكنولوجيا جديدة فمن المهم أن تسأل عن كيفية التعامل مع هذا الأمر وفحص ما إذا كان يتم إهمال فكرة التأمين من أجل زيادة السرعة أم لا، وليس هذا هو الحال في كل الأوقات، ولكنه أمر يجب عليك التأكد منه عندما تتعرض لتطبيق بلوك تشين جديد.

التطوير

يعتبر التطوير أحد أكثر المشكلات الهامة التي تواجه تطبيقات البلوك تشين في الوقت الحالي، فإذا رأيت ما عليه البلوك تشين بالفعل فستجد أنها عبارة عن تسلسل طويل من أكثر من بلوك، ويمكنك تخيل أنه كلما زادت المعاملات وزادت إضافة المزيد من البلوك فإن التسلسل يصبح أطول فأطول.

أحد الأشياء التي تجعل البلوك تشين تعمل هو أنه يتم تخزين عدة نسخ وتحديثها عبر شبكة لا مركزية، ونظريًا عندما يصبح التسلسل أكبر فسوف يحتاج بالتأكيد إلى مساحة أكبر فأكثر، وإذا كان التسلسل كبيرًا جدًا فإنه سيحتاج إلى مساحة تخزين هائلة؛ لذلك فمن لا يملك مساحة كافية لتخزين كل التسلسل فلن يكون قادرًا على المشاركة في الشبكة؛ لذلك فإن الخوادم الكبيرة فقط -بمرور الوقت- ستكون كافية لتخزين تسلسل ضخم، مما يعيدنا مرة أخرى إلى النوع الشائع من النموذج المركزي الذي تم تصميم تقنية البلوك تشين من أجل تجنبه.

يعتبر التطوير مشكلة كبيرة تم ذكرها بطرق مختلفة وبواسطة الكثير من المبتكرين في مجال العملات الرقمية والبلوك تشين، وتعتبر «تكنولوجيا البرق (Lightning Network)» إحدى الطرق التي تم إدخالها كخيار محتمل واعد للمشكلات الحالية المتعلقة بالتطوير والتي تواجه تطبيقات البلوك تشين.

تعمل تكنولوجيا البرق عن طريق السماح بإجراء المعاملات الصغيرة بنظام الند للند بشكل فوري باستخدام العقود الذكية الخاصة بتقنية البلوك تشين، ولكن دون إضافة معاملات الفرد إلى البلوك تشين الرئيسية، وتدعم تكنولوجيا البرق كذلك «المبادلة الذرية (atomic swaps)» بين البلوك تشين المختلفة، فعلى سبيل المثال يمكن المبادلة من عملة مشفرة إلى عملة أخرى ما دامت هذه البلوك تشين تدعم نفس Hashing Algorithm. وتعتبر تكنولوجيا البرق عبارة عن جمع بين تقنية بلوك تشين البيتكوين وبين لغة البرمجة الداخلية الخاصة بها لإدارة العقود الذكية، وهي أحد أمثلة الخيارات المعتمدة على البلوك تشين

لحل مشكلة تطوير البلوك تشين، ويعتبر هذا الجمع مثالاً على كيفية اعتماد التكنولوجيا على نفسها لتطوير تطبيقات جديدة معتمدة على التركيب الموجود.

الحوسبة الكمية (Quantum computing)

قد تبدو الحوسبة الكمية نوعًا من الخيال العلمي، ولكنها لم تعد بعيدة عن أن تصبح حقيقة، ودون الدخول في الحديث عن «كيفية» الحوسبة الكمية، فما نحتاج إليه هنا بخصوص تقنية البلوك تشين هو «ماذا؟» ماذا تعني الحوسبة الكمية بالنسبة لنا بشكل عام؟ وما تطبيقات تقنية البلوك تشين فيها؟

باختصار، فإن ما تقدمه الحوسبة الكمية هو السرعة والطاقة الفائقة، واعتبارًا من الآن، فإذا نظرنا إلى مثال البيتكوين فسوف نعرف بأن كل بلوك موجود فيه قد تم «تعيينه» بواسطة شبكة غير مركزية من الأجهزة التي تعمل على التحقق من معاملات البيتكوين عن طريق حل معادلات رياضية معقدة من أجل تبادل كمية صغيرة من البيتكوين، وعند حل هذه المعادلات فإن المعاملة تعتبر صحيحة ويتم إضافة بلوك إلى التسلسل.

وستكون أجهزة الحاسب الكمية قادرة على حل هذه الحسابات الرياضية بمعدل أسرع بكثير من أي شيء

موجود الآن، وهذه هي المشكلة الأولى التي تحلها الحوسبة الكمية.

أما بخصوص المشكلة الثانية التي تظهر عندما نفكر في أكثر النماذج التي تتحكم في بروتوكول البيتكوين، ومن أجل تعديل البلوك تشين، فيجب على الشخص تعديل الملف في أكثر من 50% من النسخ المخزنة حول العالم، ونوع طاقة المعالجة اللازم لاختراق البلوك تشين بشكل فعال يستحيل توفيره في الوقت الحالي، لكن الحوسبة الكمية لديها إمكانية تغيير ذلك على الرغم من أنه حتى هذه اللحظة ما يزال هذا الخطر نظريًا فقط.



الفصل السادس اللمسة الإنسانية أو مشكلة نسبة 51%

إحدى الدعائم المركزية لتقنية البلوك تشين هي القدرة على إجراء المعاملات المالية من خلال تقنية لا تحتاج إلى الثقة في «وسيط»، فكما هو متعارف عليه بأننا نثق في النهاية في العمليات الرياضية التي تتم بواسطة أجهزة الحاسب الآلي أكثر من التي تتم عن طريق البشر، ونحن نحتاج إلى ضمان درجة من الأمان تكون بعيدة قدر الإمكان عن أي تلاعب بشري.

ومن المستحيل بطبيعة الحال إلغاء العامل البشري نهائيًا. وتكمن ميزة التطبيقات غير المركزية التي تعتمد على التحقق من خلال أجهزة الحاسب الآلي في أنها تعد فرصة كبيرة للتحويل من الشكل الهرمي لعملية التحقق إلى فكرة الشبكة الموزعة، ومع ذلك فعندما ننظر إلى تقنية بلوك تشين البيتكوين فيمكننا أن نرى بأن النموذج المستخدم يتطلب توافق الأغلبية حتى يتم التحقق من البلوك، وهي تمثل نسبة 51% من المعدنين.

ماذا يحدث إذن؟!

ومع زيادة نفقات التعدين بسبب زيادة طول البلوك تشين يستحب قيام المعدّنين بتجميع مجهودهم في مجموعات أكبر فأكبر؛ وليست هذه المشكلة من الناحية النظرية فقط، ولكن حتى وقت كتابة هذا الكتاب فإن 50% تقريبًا من كل بلوك البيتكوين تم تعدينها من خلال مجموعتين كبيرتين للتعدين على الأقل.

ولتنفيذ ما يسمى باسم «هجوم الـ 50%» فإنه يجب على عضو واحد فقط أن يشارك بنسبة 51% أو أكثر في التكلفة الكلية لشبكات تعدين البيتكوين، وسوف يتطلب ذلك كمية هائلة من الطاقة الحاسوبية، والتي ستحتاج إلى تحمل تكلفة عالية جدًا للطاقة الكهربائية، وفي الواقع فإن معظم الدول لا تملك الموارد الكافية لتنفيذ فكرة هجوم الـ 51%؛ لذلك فإن الأمر سيكون صعبًا بطريقة لا تصدق ولكنها غير مستحيلة، وإذا حدث ذلك فإن المهاجمين لن يتمكنوا من السيطرة الكاملة على الشبكة، وقد يتمكنون من وقف التحقق من المعاملات الجديدة، ولكن لا يمكنهم عكس هذه المعاملات التي تم تسجيلها بالفعل على البلوك تشين، ولا يمكنهم

كذلك سرقة البيتكوين من المحافظ الخاصة بالأشخاص، أو تعدين بيتكوين جديدة كذلك.

إن مشكلة نسبة الـ 51% هي مشكلة تحتاج كل التقنيات المركزية المبنية على نموذج مشابه في التعامل معها.

يقترح بعض المدافعين عن خوارزمية إثبات الملكية بأن هذا النموذج يوفر أمانًا أقوى ضد هجمة الـ 51%.

وتواجه كل الصناعات والتكنولوجيات الجديدة الناشئة تحديات، وتقنية البلوك تشين ليست باستثناء من ذلك الأمر.

وهناك جيل كامل من رواد الأعمال والمطورين والمحترفين الناشئين في مجال البلوك تشين، وبالنسبة لهؤلاء الذين يؤمنون بالإمكانية الثورية لهذه التقنية فإنها تعد فرصة عظيمة لهم.

مستقبل البلوك تشين

لقد قمنا بتغطية العديد من المفاهيم الأساسية التي تتعلق بتقنية البلوك تشين على مدار هذا الكتاب، وفي الوقت الذي يصبح فيه العالم أكثر اتصالاً من خلال شبكة التكنولوجيا المتصلة، ونظرًا لكمية البيانات التي ننتجها في كل يوم والتي تزيد في كل من الكمية والشكل، إلا أنه يوجد طلب وفرصة متزايدة للأشكال الجديدة من المنظمات في ظل هذه العصر الرقمي والمادي. إن استخدام البلوك تشين لدفتر الحسابات الموزع وإمكانية تشكيل تقنية لامركزية تكون آمنة ولا تحتاج إلى الثقة بدلاً من التقنية الهرمية كما تمثل هذه التقنية الجديدة بداية لخطوة ثورية نحو إعادة تصور الطريقة التي تعمل بها المؤسسات هذه الأيام.

وكما هو الحال في أي تكنولوجيا جديدة فتوجد تقنيات منافسة وتطبيقات مختلفة وعدد من التحديات الموجودة في مجال البلوك تشين، ولكن هل ستستمر تقنية بلوك تشين البيتكوين كالنموذج السائد للبلوك

تشين؟ وهل ستستمر البيتكوين كأكثر العملات الرقمية الشائعة؟ هذا هو ما ستخبرنا به الأيام القادمة. لا شك في وجود مساحة كبيرة للزيادة عندما يتعلق الأمر بإدراك كل إمكانيات تقنية البلوك تشين وما يتعلق بتوفير شفافية وشبكة لامركزية ومعاملات بنظام الند للند وإدارة الأصول المالية والمزيد من التطبيقات، لقد بدأت الكثير من الصناعات في مجالات الرعاية الصحية، والتمويل، ووسائل التواصل الاجتماعي، وحتى شركات البيع بالتجزئة، وخطوط الطيران، والمصانع، في استكشاف إمكانية دمج تطبيقات معتمدة على تقنية البلوك تشين، ولقد بدأت الحكومات والبنوك والمنظمات بالفعل في تطبيق أنظمة البلوك تشين لإدارة المعاملات المالية والوصول إلى الخدمات العامة وتوزيع المساعدات الإنسانية.

وسواء كنت متحمسًا لتطبيقات الشبكات اللامركزية التي غيرت الشكل الهرمي للمؤسسات على مستوى العالم، أم كنت مستثمرًا حريصًا على التفاعل مع التطورات الكبيرة القادمة، إلا أن البلوك تشين هي

تقنية واعدة للغاية. إن البلوك تشين دون أدنى شك هي الطريق إلى المستقبل، وعلى الرغم من الزيادة الهائلة في الاهتمام بتقنية البلوك تشين على مدى الأعوام القليلة الماضية، إلا أننا ما زلنا إلى حد كبير في المراحل المبكرة لهذا المجال. وحتى إذا كنت جديدًا بالكامل على تقنية البلوك تشين، فإنه في غضون خمسة أو عشرة أعوام يمكنك أن تكون «مستثمرًا مبكرًا» لأحد أكثر التقنيات الواعدة منذ اختراع الإنترنت.



الخلاصة

أود أن أشكركم على اقتناء هذا الكتاب وأحب أن أثنى على حرصكم على تعلم تقنية البلوك تشين التي ستغير العالم كله.

الخطوة الأولى: أتمنى أن يكون هذا الكتاب الموجز قد ساعدكم على تكوين فهم أساسي للعمليات الرقمية وتقنية البلوك تشين، وأثار داخلكم حافزًا للقيام ببعض البحث وبدء رحلتكم نحو النجاح.

الخطوة الثانية: هي يجب أن تظلوا نُشطاء على المنتديات والمصادر المذكورة في هذا الكتاب.

للمزيد من المعلومات يمكن زيارة

www.cryptomena.net

شكرًا



@alhasalah

www.alhasalah.com