



BITCOIN

حلقة بحث في مادة المعلوماتية للصف الثاني الثانوي

إعداد الطالب : أحمد هشام حمدان

بإشراف المدرس : أمجد طه

للعام الدراسي 2014 / 2015

الفهرس

الصفحة	الموضوع	
2	الفهرس	
3	فهرس الصور	
4	المقدمة	
4	إشكالية البحث	
5	التعريف و أهم التساؤلات	الباب الأول
5	التعريف بالبت كوين	الفصل الأول
10	أهم التساؤلات المطروحة	الفصل الثاني
18	التنقيب عن البت كوين	الباب الثاني
21	الأمان	الباب الثالث
22	الخاتمة	
23	قائمة المراجع و المصادر	

فهرس الصور

الرقم	الموضوع	الصفحة
1	الشكل الرمزي لعملة البيت كوين	5
2	كيفية عمل البيت كوين	7
3	عملية إرسال و استقبال البيت كوين	7
4	ربح الأموال مع البيت كوين	10
5	عملية توليد البيت كوين	13
6	مخطط تقلب سعر البيت كوين	14
7	آلية عمل المنقب	18
8	جهاز التنقيب	20

المقدمة

عن طريق وصل الإنسان إلى أماكن لم يكن يحلم بأن يصل إليها أو حتى يعلم بوجودها العلم و التكنولوجيا و نلاحظ اليوم أن التوجه العالمي للدول الغربية يتوحد كي تبقى حركة العلم في بلادهم في حالة تطور دائم و نحن اليوم نقف أمام أحد أهم الاختراعات في مجال البرمجة و التي تتعلق بحياتنا اليومية بشكل كبير إنها العملة الإلكترونية غير المركزية الأولى في العالم البت كوين .

إشكالية البحث

هل يمكن للبت كوين حالياً أن تحل محل العملة النظامية حتى نتخلى عنها نهائياً؟

هل يمكن استخدام البت كوين حالياً في سوريا على نطاق واسع ؟

الباب الأول

الفصل الأول

التعريف بالبت كوين

ما هو Bitcoin :

البت كوين هو شبكة جامعة توفر نظام جديد للدفع و نقود إلكترونية بشكل كامل. كما أنه أول شبكة دفع غير مركزية تعمل بنظام الند – للند يتم إدارتها بشكل كامل من قبل مستخدميها بدون أي سلطة مركزية أو وسطاء. من وجهة نظر المستخدم، فالبت كوين يمكن تشبيهها إلى حد كبير بالعملة النقدية الخاصة بالإنترنت. كما يمكن النظر للبت كوين أيضاً على أنها النظام الدفترى الثلاثي الأبعاد الأكثر بروزاً في الوجود.¹



رسم توضيحي 1

¹ www.BitCoin.org

من الذي قام بإنشاء البت كوين ؟

البت كوين هو أول تطبيق لمفهوم يطلق عليه اسم crypto – currency أو العملة المشفرة والذي تم الحديث عنه لأول مرة في عام 1998 من قبل Wei Dai في قائمة crypterpunks البريدية، كانت فكرة الكاتب تتمحور حول شكل جديد من المال يعتمد التشفير للتحكم في إنشائه و التعامل به بدلاً عن السلطة المركزية.

أول تطبيق و تأكيد على المبدأ تم نشره في 2009 على قائمة بريدية للتشفير بواسطة Satoshi Nakamoto لكنه قام بترك المشروع في 2010 دون توضيح المزيد حول نفسه. تطور المجتمع من حينها بشكل مضاعف و العديد من المطورين يعملون على البت كوين. لكن من المهم العلم أن Satoshi لا يتحكم بالبت كوين، وعلى نفس المنوال هوية مخترع البت كوين من المحتمل أن تبقى كهوية مخترع الورق!²

من يتحكم و يدير شبكة البت كوين ؟

لا أحد يملك شبكة البت كوين تماماً كما لا يوجد أحد يمتلك التكنولوجيا المحركة للبريد الإلكتروني. البت كوين يتم التحكم بها من قبل جميع مستخدمي البت كوين من جميع أنحاء العالم . بينما يقوم المطورون بتحسين البرنامج ، لا يمكنهم فرض تغيير في بروتوكول البت كوين لأن جميع المستخدمين لديهم مطلق الحرية لاختيار أي برنامج و أي إصدار يمكنهم استخدامه. من أجل أن يبقى المستخدمون على توافق مع بعضهم البعض، يحتاج جميع المستخدمين لاستخدام برامج تتماشى مع نفس القواعد. البت كوين يمكن أن تعمل بشكل جيد فقط عندما يكون هناك إجماع و تكامل بين جميع المستخدمين . ولهذا جميع المستخدمين و المطورين لديهم القدرة و الحافز على تبني و حماية هذا الإجماع.

كيف يعمل البت كوين ؟

من وجهة نظر المستخدم ، فالبت كوين لا شيء أكثر من كونه برنامج جوال أو برنامج كمبيوتر يقوم بتوفير محفظة بت كوين شخصية و يسمح للمستخدم بإرسال و استقبال عملات البت كوين عن طريقه. في الواقع ، تتشارك شبكة البت كوين جسر عام يسمى block chain أو سلسلة البلوكات. الجسر يحتوي على كل معاملة تم إرسالها يوماً ما، مما يسمح للكمبيوتر الخاص بأي مستخدم من التأكد من صلاحية كل معاملة.

صحة كل معاملة محمية بواسطة توقيع إلكتروني يتوافق مع عنوان المرسل، مما يسمح لجميع المستخدمين بالتحكم الكامل بإرسال عملات البت كوين من خلال محافظ البت كوين الخاصة بهم. بالإضافة لذلك يمكن لأي أحد إتمام المعاملات باستخدام قوة الحوسبة الخاصة بأجهزة متخصصة والحصول على جوائز بالبت كوين مقابل خدماتهم. وهذا ما يسمى Mining أو التنقيب.

هل البت كوين مستعملة حقاً من قبل الناس ؟

هنالك عدد متزايد من الأعمال و الأشخاص الذين يقومون باستخدام البت كوين. هذا يتضمن أعمال كثيرة و متنوعة كالمطاعم و العقارات و المؤسسات القانونية و خدمات إنترنت شهيرة بينما لا يزال البت كوين ظاهرة جديدة نسبياً فهو ينمو بسرعة. في نهاية أغسطس 2013 إجمالي قيمة المتوفر من عملات البت كوين للتداول تجاوز 1.5 مليار دولار مع ما قيمته ملايين من عملات البت كوين يتم تداوله يومياً.

كيف يحصل الفرد على عملات البت كوين ؟

- 1- كُثمن للمنتجات أو الخدمات.
 - 2- شراء البت كوين من خلال خدمات تبادل البت كوين.
 - 3- مبادلة البت كوين مع شخص قريب منك.
 - 4- ربح البت كوين من خلال التنقيب التنافسي.
- مع أنه من المستحيل أن تجد أشخاص راغبين في بيع البت كوين في مقابل الدفع ببطاقة الائتمان . فإن معظم خدمات تبادل البت كوين لا تسمح بإضافة الأموال باستخدام طرق الدفع هذه. و يرجع هذا إلى الحالات التي يمكن فيها لشخص ما أن يشتري البت كوين من خلال البايبال ، و بعد ذلك يقوم بعكس الجزء الخاص به من المعاملة. وتعرف هذه العملية باسم chargeback أو طلب استرجاع الأموال المدفوعة.

ما مدى صعوبة الدفع بالبت كوين ؟

الدفع بالبت كوين أسهل من الشراء بواسطة بطاقات الائتمان أو البطاقات المدنية و يمكن قبوله دون الحاجة لوجود حساب بنكي للتاجر. مدفوعات البت كوين تتم من خلال برنامج لمحفظة البت كوين ، إما من خلال الكمبيوتر الشخصي أو الهاتف الذكي عن طريق إدخال عنوان المستلم و المبلغ المدفوع و الضغط على إرسال و لجعل العملية أسهل عند إدخال عنوان المستلم يمكن للأجهزة الحديثة أن تعرف العنوان عن طريق ملامسة هاتفين معاً بواسطة تقنية NFC.

ما هي مزايا البت كوين ؟

- حرية الدفع : من الممكن إرسال و استقبال أي مبلغ من الأموال لحظياً من أو إلى أي مكان و في أي وقت، لا إجازات بنوك، لا حدود ، لا قيود لتخطيها .تسمح البت كوين لمستخدميها أن يتحكموا في أموالهم بشكل كامل.
- رسوم قليلة جداً : مدفوعات البت كوين يتم تنفيذها حالياً إما بدون رسوم على الإطلاق أو برسوم قليلة جداً.
- يمكن للمستخدمين تضمين رسوم نقل مع مدفوعاتهم للحصول على أولوية التنفيذ، مما ينتج عنه تأكيد أسرع للمعاملة من قبل الشبكة.
- على نحو إضافي،التجار لديهم وحدات للمساعدة في معالجة المعاملات و تحويل البت كوين إلى عملات رسمية و إيداع الأموال بشكل مباشر في حسابات البنوك الخاصة بهم بشكل يومي.

و لأن هذه الخدمات قائمة على البت كوين ، يمكنهم أن يقدموا خدماتهم بمصاريف أقل بكثير من الباي بال أو شبكات بطاقات الائتمان.

- **مخاطر أقل للتجار :** معاملات البت كوين آمنة غير قابل للعكس ولا تحتوي على معلومات المستهلك الخاصة أو الحساسة. وهذا يحمي التجار من الخسارة الناشئة عن الاحتيال أو المحاولات غير الأمنية لاسترجاع الأموال، ولا يوجد هناك حاجة لأي توافق مع قواعد PCI و يمكن للتجار التوسع إلى أسواق جديدة حيث دعم بطاقات الائتمان غير متوفر أو حيث ترتفع عمليات الاحتيال إلى حد غير متوقع. الناتج النهائي هو رسوم نقل قليلة، أسواق أكثر، و رسوم إدارية أقل.

- **الأمن و التحكم:** يمتلك مستخدم البت كوين تحكم كامل في معاملاتهم ، من المستحيل للتجار أن يفرضوا عنوة رسوم غير معلن عنها أو غير مرغوب بها كما يمكن أن يحدث مع وسائل الدفع الأخرى. مدفوعات البت كوين يمكن أن تتم بدون دمج المعلومات الشخصية بالمعاملة. وهذا يوفر حماية فائقة ضد سارقي الهويات.

كما يمكن لمستخدمي البت كوين أن يقوموا بحماية أموالهم من خلال النسخ الاحتياطي و التشفير.

ما هي عيوب البت كوين ؟

- **درجة القبول :** العديد من الأشخاص لا زالوا غير ملمين بفكرة البت كوين . كل يوم المزيد من الأعمال تقوم بقبول البت كوين لأنهم يريدون الحصول على مزايا قبولها لكن القائمة تبقى صغيرة ولا تزال في حاجة للنمو من أجل الاستفادة من مجهودات الشبكة.

- **القابلية للتطايير :** القيمة الكاملة للبت كوين في التداول و عدد الأعمال التي تستخدم البت كوين لا تزال صغيرة مقارنة بما يمكن أن تكون عليه.

و لهذا الأحداث الصغيرة نسبيا و التجارة أو أنشطة الأعمال يمكنها التأثير في السعر بشكل ملحوظ. نظريا هذه القابلية للتطايير ستقل مع تطور أسواق و تكنولوجيا البت كوين.

لم يرى العالم من قبل عملية ناشئة كهذه، و لهذا فمن الصعب حقا و المشوق أيضا تخيل ما ستؤول إليه الأمور.

- **التطوير المستمر :** برنامج البت كوين لا يزال تحت التجربة Beta مع العديد من المزايا غير الكاملة التي لا تزال قيد التطوير. العديد من الأدوات الجديدة و المزايا والخدمات يتم تطويرها لجعل البت كوين آمنة أكثر و قابلة للوصول إليها من الجميع .

العديد منها لا تزال غير جاهزة بعد للجميع .

الكثير من الأعمال التي تستخدم البت كوين لا تزال جديدة ولا تقدم تأمين.

بوجه عام البت كوين لا تزال قيد النضوج.

الفصل الثاني

أهم التساؤلات المطروحة

لماذا يثق الناس بالبت كوين ؟

الكثير من الثقة بالبت كوين يأتي من حقيقة أنها لا تتطلب أي ثقة على الإطلاق فالبت كوين مفتوحة المصدر ولا مركزية بشكل كامل. مما يعني أن لدى أي أحد القدرة على الوصول للكواد المصدري source code الكامل في أي وقت. وبناء عليه يمكن لأي مطور في العالم أن يتعرف كيفية عمل البت كوين بالتحديد. يمكن عمل جميع المدفوعات بدون الاعتماد على طرف ثالث و النظام بأكمله محمي بخوارزمية مشفرة و مراجعة بدقة متناهية من قبل طرفيها تماما كتلك المستخدمة في الأنظمة البنكية على الإنترنت. لا يمكن لأي فرد أو منظمة التحكم بالبت كوين، و الشبكة ستبقى آمنة حتى و إن لم يمكن الثقة بجميع مستخدميها.

كيف يمكنني أن أربح أموال مع بت كوين ؟

لا يجب عليك أن تتوقع أن تصبح مليونيرا من البت كوين أو من أي تكنولوجيا منبثقة عنها . البت كوين فضاء متنامي للإبداع و هناك فرص للأعمال تحتوي أيضا على مخاطر. لا يوجد أي ضمان أن البت كوين ستستمر بالنمو بالرغم من أنها تطورت بمعدل سريع جدا حتى الآن. استثمار الوقت و الموارد في أي شيء له علاقة بالبت كوين يتطلب روح الريادة و المغامرة. هناك طرق متعددة لجني المال مع البت كوين كالتنقيب أو المضاربة أو تشغيل عمل جديد بالاعتماد على البت كوين. جميع هذه الطرق تنافسية و لا يوجد أي ضمان للربح. يعود الأمر لكل شخص لعمل تقييم مناسب للمصاريف و المخاطر المرتبطة بكل مشروع .



رسم توضيحي 4

هل البت كوين افتراضية بشكل كامل ؟

البت كوين غير مادية تماماً virtual كبطاقات الائتمان و شبكات البنوك الإلكترونية التي يستخدمها الناس كل يوم .
يمكن استخدام البت كوين للدفع من خلال الإنترنت أو بالمتاجر العادية تماماً كأى نوع آخر من الأموال.
يمكن أيضاً مبادلة البت كوين بشكل مادي كعملات و لكن الدفع بواسطة الهاتف الجوال يبقى دوماً مريحاً أكثر .
أرصدة البت كوين مخزنة في شبكة كبيرة موزعة ولا يمكن التلاعب بها بشكل احتيالي من قبل أي أحد.
فمستخدمي البت كوين لهم تحكم كامل و حصري في أموالهم و عملات البت كوين الخاصة بهم لا يمكن أن تختفي فقط لأنها غير مادية .

هل البت كوين مجهولة الهوية ؟

البت كوين مصممة لكي تسمح لمستخدميها بإرسال و استقبال الأموال باستخدام حد مقبول من الخصوصية.
على أي حال البت كوين غير مجهولة ولا يمكنها أن توفر نفس درجة الخصوصية كالأموال السائلة.
لأن استخدام البت كوين يترك وراءه سجل عام شامل.
يوجد تقنيات متعددة لحماية خصوصية المستخدمين. وتقنيات أكثر لا تزال قيد التطوير.
ظهرت بعض التخوفات من استخدام المعاملات الخاصة لأغراض غير مشروعة باستخدام البت كوين.
على أي حال بدون نقاش فإن الحديث عن أن البت كوين سيتم إخضاعها لقواعد و قوانين مشابهة لتلك الموجودة في النظم المالية المختلفة لا يساوي شيئاً.
البت كوين لا يمكن أن تكون مجهولة أكثر من الأموال السائلة .
على أي حال فإن البت كوين مصممة أيضاً لكي تمنع طيف واسع من الجرائم المالية .³

ماذا يحدث عندما تفقد عملات البت كوين ؟

عندما يفقد عضو ما محفظة البت كوين الخاصة به فإن ما سيحدث هو التأثير عينه الناجم عن إخراج الأموال من التداول. حيث ستبقى عملات البت كوين المفقودة في سلسلة البلوكات تماماً كأى عملات بت كوين أخرى.
إن عملات البت كوين المفقودة ستبقى مجمدة إلى الأبد لعدم وجود أي طريقة لأي أحد كي يستطيع الوصول إلى هذه الأموال حتى ينفقها .

هل يمكن لشبكة البت كوين أن تتضاعف لكي تصبح شبكة دفع رئيسية ؟

يمكن أن تقوم شبكة البت كوين أن تقوم بمعالجة عدد أكبر بكثير من المعاملات في الثانية الواحدة عما تقوم بمعالجته اليوم . لكنها غير قادرة حالياً على التوسع بشكل كامل للحد المكافئ لما تقوم به شبكات بطاقات الائتمان.
التطوير في الطريق الآن من أجل التخلص من القيود الحالية .

منذ البداية وكل عنصر من شبكة البت كوين قيد النضوج و التطور، ومن المتوقع أن يبقى الأمر على هذا النحو لسنوات عدة قادمة.

بينما تنمو الحركة على شبكة البت كوين فربما يقوم عدد أكبر من مستخدمي البت كوين باستخدام برامج بت كوين أخف و نقاط تلاقي أكثر بالشبكة ربما تتحول إلى خدمات أكثر تخصصاً .

هل يمكن استعمال عملات البت كوين في نشاطات غير قانونية ؟

البت كوين هو مال والأموال يتم استخدامها دوماً من أجل كلاً من الأغراض المشروعة وغير المشروعة .

الأموال السائلة و بطاقات الائتمان و النظم البنكية تتجاوز البت كوين بكثير عندما يتعلق الأمر باستخدامها في تمويل الجرائم .

البت كوين مصمم لكي يكون خطوة هائلة دافعة للأمام في سبيل صنع أموال أكثر أماناً و يمكنها أيضاً أن تمثل حماية هامة ضد أشكال عديدة من الجرائم المالية . على سبيل المثال من المستحيل تزيف البت كوين.

لدى المستخدمين تحكم كامل في مدفوعاتهم ولا يمكن أن يتم مطالبتهم بمدفوعات غير مصدق عليها كما هو الحال مع الاحتيال من خلال بطاقات الائتمان.

معاملات البت كوين غير قابلة للعكس و محصنة ضد طلبات استرجاع الأموال الاحتياطية.

يجعل البت كوين من الممكن تأمين الأموال ضد السرقة و الخسارة باستخدام آليات قوية و مفيدة جداً كالنسخ الاحتياطي و التشفير و التوقيع المتعددة .

تم طرح بعد المخاوف بأن البت كوين قد يكون جاذب للمجرمين لأنه مم الممكن استخدامه لعمل مدفوعات سرية لا يمكن عكسها.

على أي حال فإن هذه الطرق موجودة و مستخدمة بكثرة .

استخدام البت كوين سيخضع بدون جدال لنفس القواعد المطبقة حالياً في الأنظمة المالية و البت كوين لن تمنع التحقيقات الجنائية من أخذ مجراها.

بشكل عام من التعارف عليه أن الاختراعات الهامة و الجديدة يتم استقبالها بشكل مثير للجدل قبل أن يتم فهم مزاياها بشكل جيد . الانترنت مثال جيد بين العديد من الأمثلة التي توضح هذا.

هل يمكن تقنين البت كوين ؟

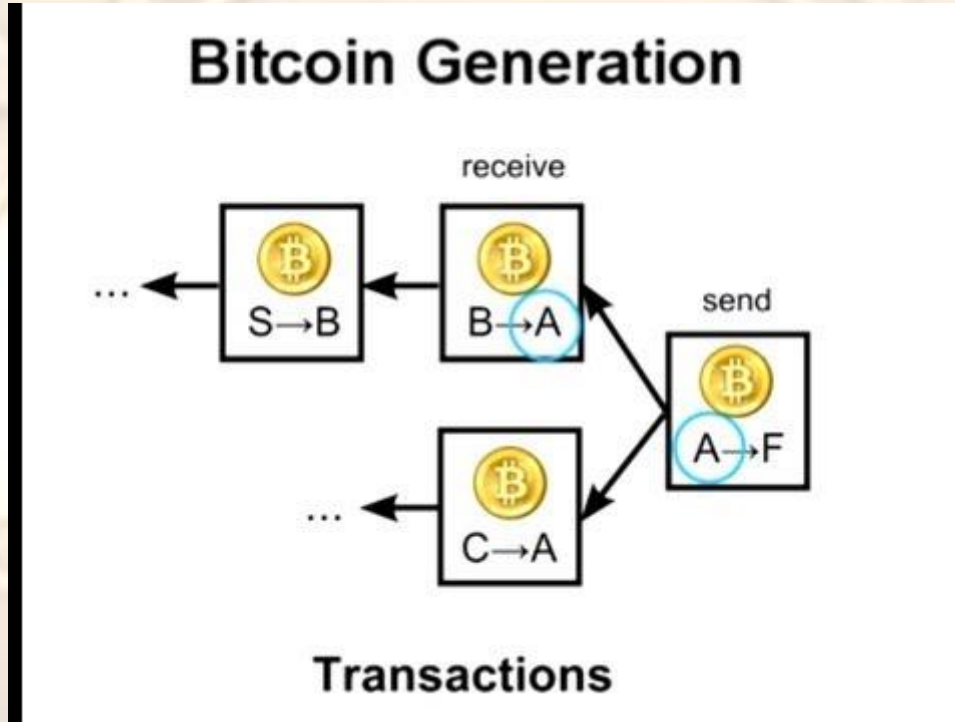
لا يمكن تعديل بروتوكول البت كوين نفسه بدون مشاركة جميع مستخدمي البت كوين تقريباً الذين يقومون بتحديد أي برنامج من البرامج سيقومون باستخدامه.

محاولة تخصيص أو مزايا لسلطة محلية ما ضمن قواعد شبكة البت كوين العالمية غير ممكن عملياً .

أي منظمة قادرة مالياً يمكنها اختيار الاستثمار في الأجهزة الخاصة بالتنقيب للتحكم في نصف قدرة شبكة البت كوين الإنتاجية وتصبح قادرة على حظر أو عكس المعاملات الأخيرة. على أي حال، لا يوجد أي ضمان على أن بإمكانهم الحفاظ على قدرة كهذه حيث سيتوجب عليهم استثمار مقدار مساو لما يقوم جميع المنقبين حول العالم باستثماره.⁴

كيف يتم إنشاء عملات البت كوين ؟

عملات البت كوين الجديدة يتم توليدها باستخدام عملية تنافسية ولا مركزية تسمى التنقيب mining هذه العملية تتضمن مكافأة الأشخاص من قبل الشبكة مقابل خدماتهم. منقبو البت كوين يقومون بمعالجة المعاملات وتأمين الشبكة باستخدام أجهزة متخصصة بينما يقوموا في المقابل بتجميع عملات البت كوين الجديدة.



رسم توضيحي 5

بروتوكول البت كوين مصمم بطريقة خاصة حيث يتم إنشاء عملات البت كوين الجديدة بمعدل ثابت. هذا يجعل التنقيب عن عملات البت كوين عمل تنافسي جداً. عندما يقوم منقبين جدد بالانضمام للشبكة، يصبح من الصعوبة بمكان تحقيق أي ربح ويتوجب على المنقبين حينها البحث عن طرق أكثر فعالية لتغطية مصاريف التشغيل الخاصة بهم. لا يوجد أي سلطة مركزية أو مطور لديه القدرة على التحكم بالنظام أو التلاعب به لزيادة أرباحه. يتم إنشاء عملات البت كوين بمعدل متناقص ومن الممكن التنبؤ به. عدد عملات البت كوين الجديدة التي يتم إنشاؤها كل عام يتناقص إلى النصف حتى يتم إنشاء جميع عملات البت كوين على نحو كامل وبإجمالي 21 مليون عملة بت كوين في الوجود كله. وعند هذه النقطة، فإن التنقيب عن البت كوين من المحتمل أن يتم دعمه على نحو استثنائي برسوم معاملات صغيرة عدة.

لماذا يحتوي البت كوين على قيمة ؟

البت كوين ذو قيمة لأنه مفيد كشكل من أشكال الأموال. لدى البت كوين نفس خصائص الأموال (الصمود، القابلية للحمل، التبادلية، الندرة، القابلية للقسمة وسهولة التعامل به) بناء على خصائص الرياضيات بدلاً من الاعتماد على الخصائص المادية (كما في الذهب والفضة) أو الوثوق في السلطات المصدرة (كما في العملات الورقية). باختصار، البت كوين مدعوم من قبل الرياضيات. بهذه المواصفات، كل ما هو مطلوب لشكل ما من أشكال الأموال لكي يصبح ذات قيمة هو الثقة به وتبنيه. وفي حالة البت كوين، يمكن قياس هذا بقاعدتها المتنامية من المستخدمين والتجار والشركات الناشئة. كما في جميع العملات الأخرى، يستمد البت كوين قيمته فقط وحصرها من الناس الراغبين في قبوله كطريقة دفع.

ما الذي يحدد سعر البت كوين ؟

يحدد سعر عملة البت كوين بقانون العرض والطلب. عندما يزداد الطلب على البت كوين يزداد السعر، وعندما يقل الطلب يقل السعر. هناك كمية محدودة فقط من عملات البت كوين متاحة للتداول وعملات البت كوين الجديدة يتم إنشاؤها بمعدل متناقص ويمكن التنبؤ به، مما يعني أن الطلب يجب أن يأتي لاحقاً على هذا المستوى من التضخم لكي يبقى السعر ثابت. ولأن سوق البت كوين لا يزال سوق صغير نسبياً مقارنة بما يمكن أن يصبح عليه في المستقبل، لا يتطلب الأمر كمية كبيرة من الأموال لتحريك سعر السوق للأعلى أو للأسفل، ولهذا لا يزال سعر البت كوين متطاير إلى حد بعيد.



رسم توضيحي 6

هل يمكن أن يصبح البت كوين بلا قيمة ؟

نعم فالتاريخ مليء بالعملات الفاشلة والتي لم تعد مستخدمة، كالمارك الألماني أثناء فترة جمهورية فايمار "Weimar Republic"، وحديثاً، الدولار الزيمبابوي. وبالرغم من أن فشل العملات السابق كان ناتج عن التضخم بشكل يستحيل حدوثه مع البت كوين، هناك دوماً احتمالية لانهاية تقني أو ظهور عملات منافسة أو مشاكل سياسية وهكذا. وكقاعدة أساسية، لا يوجد أي عملة يمكن اعتبارها آمنة تماماً ضد الانهيارات والأوقات

الصعبة. أثبت البت كوين إمكانية الوثوق به لسنوات منذ بدايته، وهناك احتمالية كبيرة أن يستمر البت كوين في النمو. على أي حال، لا أحد في موقع يمكنه من توقع مستقبل البت كوين أو كيف سيكون عليه الحال في المستقبل.

هل البت كوين أحد أشكال مخطط بونزي Ponzi Scheme ؟

مخطط بونزي أو كما يسمى بالإنجليزية "Ponzi Scheme" هو عملية استثمار احتيالية تقوم على دفع عوائد لمستثمريها من أموالهم، أو الأموال المدفوعة من مستثمرين لاحقين، بدلاً عن دفعها من الأرباح الناتجة عن إدارة الأعمال. مخطط بونزي مصمم لكي ينهار على حساب المستثمرين النهائيين عندما لا يكون هناك مشاركون جدد كافيين .

البت كوين هو برنامج مجاني بدون سلطة إصدار مركزية. وبناء على ذلك، لا يوجد أحد في موقع يمكنه من تقديم مزاعم احتيالية بخصوص عائدات الاستثمار. كما بالعملة الرئيسية الأخرى كالذهب أو الدولار الأمريكي أو اليورو أو اللين الياباني ...الخ، لا يوجد قوة شرائية مضمونة وسعر الصرف يتفاوت بحرية. وهذا يؤدي إلى التطاير حيث يمكن لمالكي البت كوين أن يربحوا أو يخسروا أموال على نحو غير متوقع. بعد التأمل، فالبت كوين أيضاً نظام دفع بخصائص مفيدة وتنافسية يتم استخدامها من قبل الآلاف من المستخدمين والأعمال.

ألن يشكل عدد العملات المحدود قيداً؟

يتفرد البت كوين في أن 21 مليون عملة بت كوين فقط يمكن إنشاءها على الإطلاق. على أي حال، لا يمكن أن يكون هذا عائقاً أبداً لأن كل عملة بت كوين يمكن تقسيمها حتى 8 خانات (0.000 01 000 BTC) ومن المحتمل أيضاً أن يتم تقسيمها إلى وحدات أصغر إذا تطلب الأمر هذا في المستقبل. وبما أن متوسط حجم المعاملة يتناقص، فالمعاملات يمكنها أن تتم في صورة وحدات منبثقة من البت كوين، كالميللي بت كوين "millibitcoins" أو (1 mBTC أو ما يساوي 0.001 BTC) .

ماذا لو اشترى أحدهم كل الموجود من عملات البت كوين ؟

فقط جزء صغير من كل عملات البت كوين التي تم إنشاءها حتى اليوم يمكن إيجاده للبيع في سوق التبادل. أسواق البت كوين تنافسية، ما يعني أن سعر البت كوين سوف يزداد أو يقل بناء على قانون العرض والطلب. على نحو إضافي، عملات البت كوين الجديدة سوف يستمر إنشاءها لعقود قادمة. ولهذا، حتى المشتريين الأكثر تصميماً لن يمكنهم شراء كل عملات البت كوين المتاحة بالوجود.

ماذا لو قام أحدهم بصنع عملة رقمية أفضل ؟

يمكن لهذا أن يحدث. حتى الآن، تبقى البت كوين العملة الافتراضية اللامركزية الأكثر شعبية، لكن لا يوجد أي ضمانات أنها ستبقى كذلك. هناك بالفعل العديد من العملات البديلة المستوحاة من البت كوين. ومع ذلك، فمن الصحيح اعتبار أن هناك العديد من التحسينات الهامة مطلوبة لأي عملة جديدة كي تتفوق على البت كوين في الأسواق الناشئة، على الرغم من أن هذا يبقى غير متوقع. يمكن أيضاً للبت كوين أن يتبنى التحسينات الخاصة بالعملات المنافسة ما دامت لا تقوم بتغيير الأجزاء الأساسية في البروتوكول .

لماذا يجب أن أنتظر عشر دقائق ؟

استقبال الأموال مع البت كوين لحظي تقريباً. على أي حال، هناك تأخير 10 دقائق في المتوسط قبل أن تبدأ الشبكة بتأكيد معاملتك عن طريق تضمينها في أحد البلوكات. وقبل أن تتمكن من إنفاق عملات البت كوين التي قمت باستلامها. التأكيد يعني أن هناك إجماع في الشبكة بأن عملات البت كوين التي قمت باستلامها لم يتم إرسالها لأحد آخر ويمكن اعتبارهم ملكية خاصة بك. بمجرد أن يتم تضمين معاملتك في أحد البلوكات، سوف يستمر تأكيدها من قبل كل بلوك تالي له، مما يعزز هذا الإجماع ويقلل من احتمالية عكس المعاملة. كل مستخدم حر في تقرير النقطة التي يعتبر عندها أن المعاملة قد تم تأكيدها، لكن 6 تأكيدات غالباً ما يتم اعتبارها آمنة بشكل مساو لانتظار 6 أشهر في معاملات بطاقات الائتمان.⁵

كم ستبلغ رسوم المعاملة ؟

معظم المعاملات يمكن معالجتها بدون رسوم، لكن يتم تشجيع المستخدمين لدفع رسوم صغيرة بشكل تطوعي لتأكيد أسرع لمعاملاتهم ولكي يتم تعويض المنقبين. عندما يتم طلب رسوم، فبشكل عام لا تتجاوز ما يساوي قيمته بنسات قليلة. وعندما يتطلب الأمر، فبرنامج البت كوين الخاص بك سوف يقوم عادة بمحاولة حساب رسوم مناسبة.

رسوم المعاملات يتم استخدامها كحماية ضد المستخدمين الذين يقومون بإغراق الشبكة بالمعاملات. والطريقة المحددة التي تعمل بها الرسوم لا زالت قيد التطوير وستتغير بمرور الوقت. لأن الرسوم لا ترتبط بكمية عملات البت كوين التي يتم إرسالها، فمن الممكن أن تبدو قليلة جداً (0.0005 بت كوين لمعاملة قيمتها 1,000 بت كوين) أو كبيرة على نحو غير عادل (0.004 بت كوين لمعاملة قيمتها 0.02 بت كوين). الرسوم يتم تحديدها ببعض الخصائص كالبيانات الموجودة بالمعاملة وتكرارية المعاملة. على سبيل المثال، إذا قمت باستلام أعداد كبيرة من المعاملات قيمة كل منها صغيرة جداً، فرسوم الإرسال ستكون أكبر. مدفوعات كهذه يمكن مقارنتها بدفع فاتورة مطعم باستخدام البنسات فقط. إنفاق كميات قليلة بسرعة من عملات البت كوين الخاصة بك قد يتطلب رسوم أيضاً. إذا كان نمط تعاملك يتبع نمط المعاملات المتعارف عليه، فيجب أن تبقى الرسوم قليلة جداً.⁶

ماذا يحدث إن تلقيت عملات البت كوين و كان الجهاز مطفأ ؟

يعمل البرنامج بشكل جيد في هذه النقطة. فالمعاملات المستلمة سوف تظهر في المرة القادمة التي تقوم فيها بفتح برنامج محفظة البت كوين الخاص بك. فعلياً، فعملات البت كوين لا يتم استقبالها بواسطة البرنامج الموجود على جهاز الكمبيوتر الخاص بك، لكن يتم إلحاقهم بجسر عام مُشارك بين جميع الأجهزة الموجودة على الشبكة. إذا تم إرسال عملات بت كوين لك بينما برنامج البت كوين الخاص بك مطفئ وقمت بتشغيله في وقت لاحق، فسيقوم بتحميل البلوكات الجديدة والتقاط أي معاملات لا يعلم البرنامج عنها أي شيء بعد، وعملات البت كوين ستظهر في آخر الأمر بعد انتهاء التحميل كما لو أنها استلمت للتو. محفظتك مطلوبة فقط عندما ترغب في إنفاق البت كوين.

⁵ www.Bitcoincharts.com

⁶ www.Howtobuybitcoins.info

ماذا تعني المزامنة و لماذا تأخذ وقتاً طويلاً ؟

زمن المزامنة الطويل مطلوب فقط مع البرامج المعتمدة على نقاط الشبكة الكاملة full node clients كبرنامج البيت كوين الرسمي BITCOIN CORE .

تقنياً، المزامنة هي عملية التحميل والتحقق من كل معاملات البيت كوين السابقة في الشبكة. لكي تقوم بعض برامج البيت كوين بحساب رصيد محفظة البيت كوين الممكن إنفاقه الخاص بك ولعمل معاملات جديدة، تحتاج هذه البرامج لمعرفة جميع المعاملات السابقة. هذه الخطوة قد تكون مُستهلكة للموارد بشكل كبير وتتطلب مساحة تخزين وحزمة نقل بيانات "bandwidth" كافية لكي تتناسب مع الحجم الكامل لسلسلة البلوكات. لكي تبقى عملات البيت كوين آمنة، يتوجب على عدد كاف من المستخدمين الإبقاء على استخدام البرامج المعتمدة لنقاط الشبكة الكاملة كبرنامج البيت كوين الرسمي لأن هذه البرامج تؤدي مهمة تبديل وتشريع المعاملات.

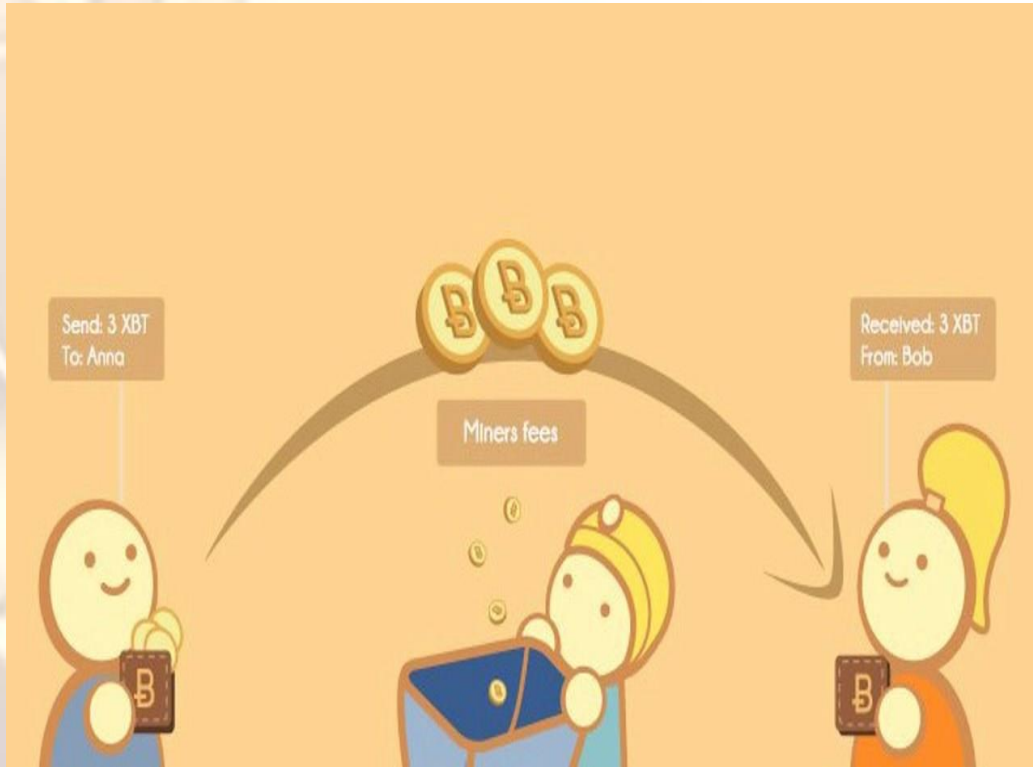
الباب الثاني

التنقيب عن البت كوين

ما هو التنقيب عن البت كوين ؟

التنقيب أو ما يسمى بالإنجليزية "mining" هو عملية استخدام قدرة الكمبيوتر لمعالجة المعاملات وتأمين الشبكة وإبقاء كل مستخدمي الشبكة متزامنين مع بعضهم البعض.

يمكن اعتبار التنقيب مركز العمليات المركزي للبت كوين باستثناء أنه قد تم تصميمه لكي يكون غير مركزي بالكامل مع وجود منقبين فاعلين بجميع الدول ولا يوجد أشخاص لديهم تحكم كامل بالشبكة. هذه العملية يتم الإشارة إليها بـ "التنقيب" تشبيهاً بالتنقيب عن الذهب لأنها أيضاً آلية مؤقتة يتم استخدامها لإنشاء عملات بت كوين جديدة. على أي حال، فعلى عكس التنقيب عن الذهب فالتنقيب عن عملات البت كوين يعطي مكافأة في مقابل الاستفادة من الخدمات المفيدة والمطلوبة للإبقاء على شبكة دفع آمنة. التنقيب سيظل مطلوباً حتى بعد أن يتم إصدار آخر عملة بت كوين.⁷



رسم توضيحي 7

كيف يعمل التنقيب عن البت كوين ؟

أي أحد يمكنه أن يصبح منقب عن البت كوين عن طريق تشغيل برنامج على أجهزة كمبيوتر متخصصة. برامج التنقيب تقوم بالنقاط سير المعاملات من خلال شبكة البت كوين وتقوم بأداء المهام المناسبة لمعالجة وتأكد هذه المعاملات. يقوم منقبو البت كوين بأداء هذا العمل لأنه يمكنهم من الحصول على رسوم المعاملات التي يقوم المستخدمون بدفعها من أجل تسريع معالجة معاملاتهم، وأيضاً للحصول على عملات البت كوين المولدة حديثاً تبعاً لمعادلة ثابتة.

لكي يتم تأكيد المعاملات الجديدة، يجب أن يتم تضمينهم في بلوك مع برهان رياضي على أنهم فاعلين. براهين كهذه من الصعب جداً أن يتم إنشاؤها لعدم وجود وسيلة لإنشائهم سوى محاولة مليارات الحسابات في الثانية. ويتطلب هذا أن يقوم المنقبين بعمل هذه الحسابات قبل أن يتم قبول البلوكات الخاصة بهم من قبل الشبكة وقبل أن يتم مكافأتهم. بينما يقوم المزيد من الأشخاص ببدء التنقيب، تزداد صعوبة إيجاد بلوكات صالحة بشكل أوتوماتيكي من قبل الشبكة للتأكد من أن متوسط الوقت المطلوب لإيجاد كل بلوك مساو لـ 10 دقائق. وكنتيجة لهذا، فالتنقيب هو عمل تنافسي جداً حيث لا منقب فردي يمكنه التحكم في ما يمكن تضمينه بسلسلة البلوكات.

برهان العمل مصمم أيضاً لكي يعتمد على البلوك السابق كي يتم فرض ترتيب البلوكات في السلسلة زمنياً. مما يجعل عكس المعاملات السابقة صعب بشكل مضاعف لأن هذا يتطلب إعادة حساب جميع براهين العمل الخاصة بكل البلوكات اللاحقة للبلوك المطلوب عكس معاملاته. عندما يتم إيجاد بلوكين معاً في نفس الوقت، فالمنقبين يعملون على المجموعة الأولى التي يتم استلامها والتحويل إلى السلسلة الأطول من البلوكات مباشرة بعد أن يتم إيجاد البلوك التالي. وهو ما يسمح للتنقيب أن يؤمن الشبكة ويحافظ على الإجماع بناء على قدرة المعالجة.

منقبو البت كوين غير قادرين على الغش عن طريق زيادة المكافآت الخاصة بهم ولا معالجة معاملات احتيالية يمكنها تخريب شبكة البت كوين لأن جميع نقاط شبكة البت كوين سترفض أي بلوك يحتوي على بيانات غير صحيحة طبقاً لقواعد بروتوكول البت كوين. وبناء على ذلك، فالشبكة تبقى آمنة حتى ولو لم يمكن الوثوق بجميع منقبو البت كوين.⁸

كيف يساعد التنقيب في تأمين شبكة البت كوين ؟

يخلق التنقيب نظام مكافئ لنظام اليانصيب التنافسي مما يجعل من الصعب لأي أحد أن يقوم بإضافة بلوكات جديدة تحتوي معاملات على التوالي في سلسلة البلوكات. يحمي هذا حيادية الشبكة عن طريق منع أي شخص من الحصول على القوة الكافية لحظر معاملات بعينها. ويمنع أيضاً أي شخص من تبديل أجزاء بعينها من سلسلة البلوكات لاستعادة ما قام بإنفاقه، مما يمكنه من الاحتيال على مستخدمين آخرين. التنقيب يجعل عكس المعاملات السابقة صعب على نحو مضاعف عن طريق طلب إعادة كتابة كل البلوكات التي تلي البلوك الذي يحتوي على المعاملة المراد عكسها وحتى تاريخه، وهو ما يستحيل عملياً!⁹

⁸ www.BitcoinFilm.org

⁹ www.BitcoinFilm.org

ما الذي أحتاج إليه لبدء التنقيب ؟

في أيام البت كوين الأولى، كان بإمكان أي شخص إيجاد عملات البت كوين الجديدة باستخدام المعالج الموجود في الكمبيوتر الشخصي. بينما يبدأ العديد والعديد من الأشخاص في التنقيب، تزداد صعوبة إيجاد بلوكات جديدة بدرجة كبيرة إلى الدرجة التي يصبح عندها الطريقة الوحيدة الفعالة للتنقيب اليوم من ناحية التكاليف هي باستخدام أجهزة كمبيوتر متخصصة.¹⁰



رسم توضيحي 8

الباب الثالث

الأمان

هل البت كوين آمن ؟

تكنولوجيا البت كوين (البروتوكول المستخدم والتشفير) لديها سجل أمان قوي، وشبكة البت كوين ربما تكون واحدة من أكبر مشاريع الحوسبة الموزعة في العالم. أكثر نقاط ضعف البت كوين انتشاراً هي خطأ المستخدم. الملفات الخاصة بمحفظة البت كوين والتي تقوم بتخزين المفاتيح السرية المطلوبة قد يتم مسحها عن طريق الخطأ أو فقدها أو سرقتها. هذا شبيه إلى حد كبير بالأموال المادية المحفوظة في هيئة رقمية. لحسن الحظ، المستخدمين يمكنهم تشغيل أصوات ممارسات الأمان لحماية أموالهم أو استخدام مزودي خدمة يقومون بتوفير درجات جيدة من الأمان والتأمين ضد السرقة أو الخسارة.

ألم يتم اختراق البت كوين في الماضي ؟

قواعد البروتوكول والتشفير المستخدمة في البت كوين لازالت فاعلة حتى بعد سنوات من بدايتها، وهو ما يعني أن المبدأ مصمم بشكل جيد. على أي حال، تم إيجاد وإصلاح الثغرات الأمنية على مدار الوقت في العديد من نسخ البرنامج. وكأي شكل آخر من أشكال البرامج، أمان البرنامج الخاص بالبت كوين يعتمد على السرعة التي يتم بها إيجاد وإصلاح المشاكل. كلما زاد اكتشاف مثل هذه المشاكل، كلما ازداد البت كوين نضجاً و أماناً.

غالباً ما يكون هنالك أفكار خاطئة حول السارقين والثغرات الأمنية التي حدثت في عدد من الأعمال وخدمات تبادل الأموال. بالرغم من أن هذه الأحداث مؤسفة في ذاتها، فإن أياً منها لم يتضمن اختراق البت كوين نفسه، ولم تنتقل أي ثغرات إلى تكنولوجيا أو شبكة البت كوين؛ تماماً كما أن سرقة أي بنك لا يعني وجود ثغرات في الدولار نفسه. على أي حال، من الدقيق القول أن مجموعة كاملة من الممارسات وحلول الأمان الجيدة مطلوبة لإعطاء المستخدمين حماية أفضل لأموالهم، ولتقليل الخطورة العامة للسرقة والخسارة. على مدار السنوات القليلة الماضية، مميزات أمان كهذه تم تطويرها كتشفير المحفظة والمحافظ الغير مرتبطة بالإنترنت والمعاملات متعددة التوقيعات.¹¹

هل البت كوين قابل للتحكم به من قبل الحوسبة الكمية ؟

نعم، غالبية الأنظمة تعتمد على التشفير بشكل عام، بما فيها أنظمة البنوك التقليدية. على أي حال، أجهزة الكمبيوتر الكمية غير موجودة حتى الآن ومن الممكن أن لا توجد لفترة قادمة. وفي حال ما أصبحت الحوسبة الكمية خطر وشيك على البت كوين، فيمكن تطوير البروتوكول لكي يستخدم خوارزميات ما بعد الحوسبة الكمية. بأخذ أهمية تطور كهذا بعين الاعتبار، من الآمن توقع أن أنه سيتم مراجعته بشكل مكثف من قبل المطورين وتبنيه من جميع مستخدمي البت كوين .

¹¹ www.Bitcoin.org

الخاتمة

والآن بعد أن تعرفنا على البت كوين من جميع الجوانب تقريباً و مقارناتها مع العملة النظامية أرى أنه في الواقع يمكن استخدام البت كوين في الكثير من المواقف الحياتية و الاعتماد عليها كبديل مكافئ للعملة النظامية لكن ليس لدرجة التخلي عن العملة النظامية بسبب وجود المعوقات لاستخدام البت كوين في البلدان النامية مثل سوريا حيث أن الكثير من المواطنين غير قادرين على تحمل كلفة متطلبات هذه التقنية مثل جهاز جوال متطور نسبياً أو جهاز حاسوب بالإضافة إلى إنترنت سريع و متوفر دائماً و لكن هذا لا يسمح لنا بالقول أن البت كوين غير فعالة فهي تملك الكثير من الميزات التي تجعلها عملة المستقبل .

قائمة المراجع و المصادر

www.WeUseCoins.com
www. BitcoinMinig.com
www. Bitcoin.org
www. Usebitcoins.info
Bitcoin Magazine
www. Bitcoincharts.com
www. BitcoinFilm.org
Bitcoin Knowledge Podcast
www. Howtobuybitcoins.info
An introduction to probability theory and its applications, W. Feller, 1957.