السمات العامة للبتكوين واقتصادياتها

رمزي بن عبد الله بن أحمد حسان

الجامعة الإسلامية - المدينة المنورة

لفتت البتكوين أنظار الباحثين الاقتصاديين إليها، بقوة انتشارها واشتهارها، الأمر الذي جعلنا نمعن النظر في سياساتها الاقتصادية، سلبياتها وإيجابياتها، حتى نفهم هذا التيار الجامح من التاثير في الاقتصاد النقدي الورقي.

قام الباحث بكتابة رسالته للماجستير في تخصص الاقتصاد الإسلامي في هذا الموضوع، في قسم الاقتصاد الإسلامي في الجامعة الإسلامية بالمدينة المنورة، فجزى الله مشايخنا عنا خير الجزاء.

وهذه الأسطر إنما هي استلال من الرسالة التي أرجو أن ترى النور قريباً إن شاء الله.

وستتناول هذه الاسطر اولاً: تعريف البتكوين، وثانياً: المفاهيم الرقمية والبرمجية للبتكوين، راجيا من الله النفع بها، لأرى ملحوظات السادة القراء وتصويباتهم على هذا العمل المتواضع.

تعرف البتكوين أنها: عملات رقمية لا تصدر عن أي حكومة أو بنك أوتنظيم، والاعتماد على بروتوكولات التشفير وشبكة موزعة من للمستخدمين[١]. أو: (هي شبكة لا مركزية من العملات الرقمية والتي تستخدم نظام النظير للنظير للتحقق من المعاملات ومعالجتها بدلا من الاعتماد على أطراف ثلاثة موثوق بها، مثل البنوك والبطاقات، كما أنها تستخدم نظام التشفير لمعالجة المعاملات والتحقق من شرعيتها[٢]. كما تعرف أنها: (عبارة عن مجموعة من المفاهيم والتقنيات التي تشكل أساس المال الرقمي وتستخدم وحدات العملة لتخزين ونقل القيمة بين المشاركين في شبكة بيتكوين وذلك بالتواصل بينهم باستخدام بروتوكول بتكوين المتوفر كبرنامج مفتوح المصدر على مجموعة واسعة من أجهزة الحوسبة بما في ذلك أجهزة الكمبيوتر المحمولة والهواتف الذكية مما يجعل التكنولوجيا يمكن الوصول إليها بسهولة[٣].

المفاهيم الرقمية والبرمجية

١ (quantitative analysis of the full bitcoin transaction ورقة علمية للباحثان دوريت رون وعدي شامير-قسم علوم الحاسوب بمعهد وايزمان للعلوم. ص1

٢ (introduction to bitcoin)سيم كيي بون واخرون-ص14

٣ (mastring bitcoin تاليف اندريس انتوبلوس-طبعت بواسطة –o reilly media-الولايات المتحدة-غرافنستين-الطبعة الأولى 2014م. ص1

إن مصطلح "شبكة بيتكوين" يشير إلى مجموعة من العقد تشغل بروتوكول "P2P"، والذي يعني الند أو النظير إلى النظير، دون إدارة مركزية لها، وهناك بروتوكولات أخرى مثل"Stratum"، والتي تستخدم للتعدين لسهولتها وقدرة أجهزة المحمول على التحكم فيها.

يتم توفير البروتوكولات من خلال خوادم توجيه البوابة الرقمية التي تصل إلى شبكة بيتكوين باستخدام بروتوكول "P2P"، الآتي توسيع تلك الشبكة إلى العقد لتشغيل بروتوكولات أخرى.

يشير مصطلح (شبكة بيتكوين الموسعة) للإشارة إلى الشبكة الشاملة التي تشمل بروتوكول P2P، وبروتوكولات التعدين -"pool mining protocols"-وبروتوكول -"the Stratum protocol"-، وأية بروتوكولات أخرى ذات صلة تربط مكونات نظام بيتكوين.

اكتشاف الشبكة:

عند رفع عقدة جديدة يجب اكتشاف عقدة بيتكوين أخرى على الشبكة من أجل المشاركة، لبدء هذه العملية يجب أن تكتشف عقدة جديدة واحدة موجودة على الأقل على الشبكة والاتصال بها، وهي غير ذات صلة بالموقع الجغرافي، لا يتم تعريف بنية شبكة بيتكوين جغرافيا. لذلك يمكن اختيار عقد البيتكوين الحالية عشوائيا للاتصال بنظيرٍ معروف، يعمل النظام عن طريق إرسال رسالة الإصدار، الذي يحتوي على معلومات تحديد أساسية، بما في ذلك:

- "PROTOCOL_VERSION": وهو ثابت يحدد إصدار بروتوكول "P2P" بيتكوين العميل (على سبيل المثال 70002).
- "NODE_NETWORK": قائمة الخدمات المحلية التي تدعمها العقدة حاليا فقط.
- "nTime":وقت التيار.
- "AddrYou": عنوان IP للعقدة البعيدة.
- "AddrMe":عنوان IP العقدة المحلية.
- "Subver":وهو إصدار فرعي يعرض نوع البرنامج الذي يتم تشغيله على هذه العقدة (على سبيل المثال: "/ساتوشي: 0.9.2.1/").
- "BestHeight":ارتفاع كتلة عقدة البلوكتشين.[1]

[1] Mastering Bitcoin مرجع سابق- ص144

- **الإنفاق المزدوج**: إذا حاول مستخدم احتيالي إرسال عملات البيتكوين الخاصة به لمستلمين اثنين في نفس الوقت، فهذا ما يطلق عليه الإنفاق المزدوج أو ما يسمى بالإنجليزية "double spending" وهنا يأتي دور التنقيب وسلسلة البلوكات حيث كلاهما موجود لخلق حالة من الإجماع في الشبكة حول أي المعاملتين سيتم تأكيدها واعتبارها صحيحة، وقد فسر الباحثان: د. حمود طارق ود. رقية وافية هذا الإنفاق المزدوج أنه وسيلة للتحايل تشبه إلى حد كبير ما يحدث في – إلغاء الفاتورة – في البطاقة الائتمانية مما يشكل خطراً كبيراً في حال عدم الثقة بين المتعاملين حيث يقوم المشتري فور شحن البضاعة بطلب إلغاء الصفقة ثم تصل البضاعة إلى المشتري ولم يقم بتحويل المال، إن هذا التفسير بعيد عن برمجيات البتكوين والتي يتطلب الاجماع الكامل على تأكيد شفرة واحدة فقط ولا يمكن بتاتا تواطؤ أجهزة الحواسيب في العالم على خطأ واحد(١).
- "bitcoin": دون حروف كبيرة، يتم استخدامها لتوصيف البتكوين كوحدة محاسبية. على سبيل المثال: "قمت اليوم بإرسال 10 "bitcoins" وغالباً ما يتم اختصارها أيضاً ل (BTC) أو (XBT)
- **البلوك**: البلوك أو المجموعة أو كما يسمى بالإنجليزية "block" هو سجل في سلسلة البلوكات يحتوي على العديد من المعاملات قيد التنفيذ يقوم بتأكيدها. في المتوسط، كل ١٠ دقائق تقريباً، بلوك جديد يحتوي مجموعة من المعاملات يتم إضافته إلى سلسلة البلوكات من خلال التنقيب.
- **التأكيد**: التأكيد أو ما يسمى بالإنجليزية "confirmation" يعني أن المعاملة قد تم معالجتها بواسطة شبكة البيتكوين وبشكل كبير لا يمكن عكسهاحيث إن جميع المعاملات يتم تأكيدها بعد تضمينها في وحدة "بلوك "ومن قبل كل بلوك تالٍ. إنَّ تأكيداً واحداً يمكن اعتباره آمناً للمعاملات ذات القيم الصغيرة، أما في المعاملات الأكبر كـ ١٠٠٠ دولار أمريكي أو أكثر، فمن المنطقي الانتظار حتى ٦ تأكيدات أو أكثر. كل تأكيد إضافي يقلل بشكل مضاعف من خطورة عكس المعاملة.
- **التشفير**: التشفير أو ما يسمى بالإنجليزية "cryptography" هو أحد فروع الرياضيات يتيح لنا إنشاء براهين رياضية ذات مستوى عالٍ من الأمان. ويمكننا القول بشكل أكثر دقة أن ال "cryptography" هو علم التشفير والتعمية معاً. في حالة البيتكوين يتم استخدام التشفير لجعل

١ البتكوين بين قياسية الارباح وتصاعد التحذيرات-د. حمود طارق واخرون-بحث منشور بمجلة الدراسات المالية والمصرفية لاكاديمية العلوم المالية والمصرفية –الاردن- (26/ع1)لسنة 2018م-ص28.

الأمر مستحيلاً لأي أحد يحاول إنفاق أي أموال من محفظة مستخدم آخر أو يقوم بمحاولة تخريب سلسلة البلوكات، يمكن استخدامه أيضاً لتشفير أي محفظة، حتى لا يمكن استخدامها من دون كلمة مرور.

- **التنقيب**: "mining" التنقيب عن عملات البيتكوين هو عبارة عن عملية جعل الكمبيوتر يقوم بعمل حسابات رياضية لصالح شبكة البيتكوين من أجل تأكيد المعاملات وزيادة الأمان. كمكافأة على خدماتهم تلك يستطيع معدِّنو البتكوين الحصول على رسوم المعاملات التي يقومون بتأكيدها بحواسيبهم الخاصة، بالإضافة إلى حصولهم على عملات البيتكوين المولدة حديثاً. التنقيب هو سوق تنافسي ومتخصص حيث يتم توزيع المكافآت تبعاً لكمية الحسابات التي تم عملها. لا يقوم كل مستخدمي البتكوين بالتنقيب، والتنقيب ليس طريقة سهلة لكسب الأموال[١].

ونظام المكافأت يعتمد على نظام العوائد المتناقصة –كما يصدر البنك المركزي النقودالجديدة– حيث تتناقص كل أربع سنوات أو كل (٢١٠٠٠٠) كتلة، وبدأت بالتناقص – وستستمر لمدة أربع سنوات متوالية – حيث كانت ب ٥٠ بتكوين لكل كتلة، وذلك في يانايير من عام ٢٠٠٩ م، ونزلت إلى النصف (٢٥ بيتكوين) لكل كتلة في نوفمبر من عام ٢٠١٢م، والنصف أيضاً أي (١٢.٥) في عام ٢٠١٦م – عند الكتلة ٤٢٠٠٠٠ –، وحتى مايقارب من عام ٢٠١٤م أو في بعض التقديرات أنها قبل ذلك بثلاثة أعوام، ستكون عمليات التعدين غير مجدية حيث يتوقع أن تصل البتكوين إلى الكتلة النقدية النهائية لها وهي ما يقارب من (٢١) مليون بتكوين[٢].

والشكل الآتي يوضح تزايد تعدين كتلة البتكوين رياضياً:

---

١ انظر أيضاً(Mastering Bitcoin)مرجع سابق-ص177

٢ (Incrementum-Crypto-Research-Report)-مرجع سابق-ص11/12*انظر أيضا: ?Bitcoin as Money ستيفاني لو وَ كريستينا وانق-منشور ضمن منشورات (current policy perspectives)الصادرة عن البنك الفيدرالي في بوسطن برقم 144-الصادر في 4سبتمبر2014م-ص3 *انظر أيضاً: (The social life of Bitcoin)-نايجل دود-بحث محكم بمجلة مدرسة لندن للاقتصاد وعلوم التقنية-(LSE)-2/2017م-ص10*(mastring bitcoin)-مرجع سابق-ص177-178. *انظر أيضاً: كتاب صادر عن مركز هردو لدعم التعبير الرقمي-القاهرة-2018م-ص6

```
# Original block reward for miners was 50 BTC
start_block_reward = 50
# 210000 is around every 4 years with a 10 minute block interval
reward_interval = 210000

def max_money():
    # 50 BTC = 50 0000 0000 Satoshis
    current_reward = 50 * 10**8
    total = 0
    while current_reward > 0:
        total += reward_interval * current_reward
        current_reward /= 2
    return total

print "Total BTC to ever be created:", max_money(), "Satoshis"
```

Running the script:

Example 8-2. Running the max_money.py script

```
$ python max_money.py
Total BTC to ever be created: 2099999997690000 Satoshis
```

شكل ١ يوضح تزايد البتكوين بيانياً – انظر (mastring bitcoin)مرجع سابق–ص ١٧٩ رسم توضيحي ١

ويوضح الشكل الآتي تعدين البتكوين بيانياً :

شكل ٢ يوضح تعدين البتكوين بيانيا – انظر (mastring bitcoin) ص ١٨٠

- **مجمعات التعدين – برك التعدين** (Mining Pools) : في ظل تلك البيئة التنافسية نجد المُعَدِّنين في نطاقهم الخاص يتعرضون لمخاطرة تعويض الكلفة الإنتاجية للتعدين من حيث كلفة الكهرباء وإهلاك

الأجهزة الحاسوبية ذات الكفاءة والقدرة العاليتين، فهي بهذا الشكل كلعبة الحظ بالنسبة لهم،؛ فهو لايعلم كم –بالضبط– ما سيحصل عليه، حتى إنَّ أسرع أنظمة التعدين–"ASIC mining system"– لايمكن أن تكون مضمونة الجدوى، لذلك ودفعاً لتلك المخاطر توجه الناس نحو الاستثمار أو التعدين الجماعي بنظام المجموعات التي يطلق عليها (بِرَك التعدين) لأجل التغلب على التكاليف وتفادي المغامرة الفاشلة، الآتي تقاسم الارباح بينهم كحصص الأسهم، ولفهم التكلفة والارباح المتوقعة سنقوم بضرب المثال الآتي: اشترى س معدات التعدين والتي تقوم بالتعدين بمعدل – ٦٠٠٠ – (GH/s – قيقاهاش في الثانية) والتي بلغت قيمتها (١٠٠٠٠) دولار أمريكي، الأجهزة أيضاً تستهلك كهرباء بمقدار (KW3) عند التشغيل، أي بمعدل ٧٢ (KW) ساعة/في اليوم، بتكلفة ٧–٨ دولار في المتوسط، وعلى قدر صعوبة التعدين الحالية فإن التعدين يقدر على فك كتلة كل ١٥٥ يوماً، أو كل ٥ أشهر، فإذا وجد عامل التعدين ذلك يستحق ٢٥ بتكوين، بموسط سعر صرف حوالي ٦٠٠ دولار، وسوف يؤدي بطبيعة الحال إلى صافي أرباح ١٥٠٠٠ دولار، سوف تفي بتغطية المصاريف خلال الفترة الزمنية مع أرباحٍ صافية بمقدار ٣٠٠٠ دولار، غير أنه من الجدير ذكره أنك قد لا تكسب في الأساس وتعاني من خسارة مالية لأسباب تقنية في أجهزة التعدين، وأيضا فإن أجهزة التعدين كل يوم في تطور وتقدم مستمر مما يجعل اللحاق بعصر السرعة أمراً مرهقاً مادياً. ولذلك يقرر الكثير من المعدنين الدخول ضمن تجمعات التعدين أو الشركات الكبرى بما يعادل صافي ربح ٥٠٠ دولار أو بالكثير ٧٥٠ دولار دولار، ولا ينطوي على مخاطر عالية مع قدرته على تغطية مصاريف الكهرباء والأجهزة. الآتي تقسم الأرباح كنسبة أسهم شركة المساهمة[١].

- **التوقيع**: التوقيع المشفر "signature" هو آلية رياضية تسمح لشخص ما بإثبات الملكية، وفي حالة البيتكوين، فإن محفظة البتكوين ومفاتيحها الخاصة يتم ربطهم معاً من خلال التشفير الرياضي عندما يقوم برنامج البيتكوين الخاص بك بتوقيع معاملة بالمفتاح الخاص المناسب، فإن الشبكة كلها يمكنها رؤية مطابقة التوقيع لعملات البتكوين التي تم إنفاقها. ومن المستحيل بأيَّ شكل كان تخمين الشفرات الخاصة بك[٢].

---

[١] Bitcoin as an example of virtual currency) (Modeling and Simulation of-مرجع سابق-ص14*انظر أيضاً: مايو 2016م-4/7. arxiv لويزيانا كوكو وميشيل ماركيسي-نشر the Economics of Mining in the Bitcoin Marke بتصرف*انظر أيضا: **Bitcoin: Economics, Technology, and Governance** "-راينربوهما واخرون-بحث علمي "-الصادرة عن الجمعية الاقتصادية الأمريكية-العدد 29 رقم 2-ربيع 2015م- *Journal of Economic Perspectives* بمجلة" ص222

[٢] Bitcoin: Technical Background and Data Analysis-أنطون باديف واخرون-مرجع سابق-ص8

- **العنوان**: عنوان البتكوين مشابه لعنوانك البريدي أو البريد الإلكتروني. وهو المعلومة الوحيدة التي يتوجب عليك إعطاؤها لشخص ما لكي يقوم بالدفع لك باستخدام البتكوين. ومع ذلك فهنالك فارق هام، وهو أن كل عنوان بتكوين يمكن استخدامه مرة واحدة فقط من أجل معاملة واحدة.
- **المحفظة**: محفظة البيتكوين أو ما تسمى بالإنجليزية "wallet" هي على نحو ما المكافئ للمحفظة المادية العادية ولكن في شبكة البتكوين، يعرف "راينر ونيكولا" المحفظة أنها: (ملفات تتضمن حسابات بتكوين والمفاتيح الخاصة اللازمة لإنفاق أو نقل القيمة المخزنة[١] إنَّ المحفظة تحتوي على مفتاحك الخاص والتي تسمح لك بإنفاق عملات البتكوين المرتبطة بها، إنَّ كل محفظة بتكوين يمكنك إدارتها والتحكم بها كالمحفظة المصرفية المعروفة[٢].
- **المفتاح الخاص**: المفتاح الخاص "private key" شفرة صغيرة سرية تؤكد ملكيتك وقدرة التحكم في إنفاق عملات البيتكوين من محفظة معينة من خلال التوقيع المشفر. المفتاح الخاص أو المفاتيح الخاصة المملوكة لك يتم تخزينها على جهاز الكمبيوتر الخاص بك إذا كنت تستخدم برنامج كمبيوتر كمحفظة، أو يتم تخزينه على سيرفر خاص إذا كنت تستخدم محفظة إنترنت. وفي حال إفصاح الشخص عن مفتاحه فكأنما سلم صلاحية التحكم لغيره.
- **الند-للند** "peer_to_peer" مصطلح يتم اختصاره "P2P" يشير إلى الأنظمة التي تعمل كمجتمع منظم، وتم بناء الشبكة بحيث يقوم كل مستخدم بنشر معاملات المستخدمين الآخرين على السجل العام. وبشكل يجعل الأمر لايتطلب وجود بنك كطرف ثالث.
- سلسلة البلوكات: سلسلة البلوكات أو كما تسمى بالإنجليزية "block chain" هي سجل عام لجميع معاملات البتكوين مرتبة زمنياً. سلسلة البلوكات يتم مشاركتها بين جميع مستخدمي البتكوين. يتم استخدام السلسلة من أجل التأكد من استمرارية معاملات البتكوين ولكي تمنع الإنفاق المزدوج[٣].

---

١ راينر بوهم وآخرون-بحث علمي منشور على (Bitcoin: Economics, Technology, and Governance Journal of Economic Perspectives) -Volume 29، Number 2 — Spring 2015 — Pages 213–238-ص220

٢ bitcoin system)-مرجع سابق-ص25

٣ منصات المعاملات البديلة والعملات الرقمية بين حرية التداول واشكاليات الرقابة-مرجع سابق-ص13-14

- **معدل الهاش**: معدل الهاش "hash rate" هو وحدة لقياس قدرة شبكة البيتكوين على المعالجة الرقمية لأغراض الأمان. فعلى سبيل المثال: عندما يصل معدل الهاش لشبكة البتكوين إلى ١٠ تيرا هاش/الثانية، فهذا يعني أن الشبكة يمكنها إجراء ١٠ تريليون عملية حسابية في الثانية الواحدة.
- BTC: هي الوحدة الشائعة لعملة البيتكوين. يمكن استخدامها بطريقة مشابهة للدولار الأمريكي بديلاً عن ฿ أو $[١].
- **الانكماش في البتكوين (Deflationary Money)**: هي (ظاهرة تقدير القيمة –ارتفاع الثمن– بسبب عدم التطابق في العرض والطلب)

يرى كثير من الاقتصاديين أن الانكماش هو كارثة ينبغي تجنبها بأي ثمن، لان فترة الانكماش السريع تجعل الناس تميل للاكتناز بدلاً من الإنفاق على أمل أن تنخفض الأسعار، وهذا هو الحال كما في (العقد المفقود Lost Decade) في اليابان. حيث كان الاقتصاد الياباني ينمو خلال ستينات القرن الماضي بنحو ١٠٪ سنوياً، وخلال السبعينات وأوائل الثمانينات نما الاقتصاد الياباني بنسب تراوحت ما بين ٤–٥٪، حتى صار الاقتصاد الياباني ثاني أكبر اقتصاد في العالم خلال الفترة بين ١٩٧٨–٢٠١٠م، حينما حل الاقتصاد الصيني محله كثاني أكبر اقتصاد في العالم، وأطل شبح الركود على بلد تعوَّد على النمو السريع والازدهار المستمر. فكانت النتائج :

- ارتفعت أسعار الأسهم وأثمان العقار إلى الحد اللا معقول، بحيث تحولت أسواق المال وأسواق العقار من أسواق استثمارية لتوسيع القاعدة الإنتاجية للاقتصاد الكلي إلى أسواق جشع ومضاربات، فانهارت "البورصة" اليابانية، وأدى انهيارها إلى جفاف قنوات التمويل والاستثمار. ففي نهاية العام ١٩٨٥م وصل مؤشر سوق المال الياباني الأهم "نيكاي Nikkei" إلى أقل من ١٣ ألفاً بقليل، وتابع ارتفاعه بسرعة حتى وصل خلال أربعة أعوام فقط إلى نحو ٤٠ ألفاً، أي تضاعف أكثر من ٣ مرات في فترة قصيرة.
- انفجرت "الفقاعة"، وبدأت رحلة الهبوط بسرعة. وخلال عامين ونصف العام من ١٢–١٩٨٩م إلى ٦–١٩٩٢م وصل "نيكاي" إلى نحو ٨ آلاف بعد أن كان قبل فترة وجيزة نسبياً وصل إلى نحو ٤٠ ألفاً[٢].

---

[١] bitcoin system)ورقة بحثية للباحث جان لانسكاي-نشرتها جامعة التمويل والإدارة بالتشيك(06/01-لسنة 2017)-ص20-
انظر موسوعة (https://bitcoin. org/ar/vocabulary#hash-rate)بتصرف.

[٢] Japan's Lost Decade:Origins, Consequences, and Prospects For Recovery)-غاري ار واخرون-بحث محكم منشور ضمن أبحاث ندوة(RESEARCH SEMINAR IN INTERNATIONAL ECONOMICS)-لجامعة ميشغان-2002م-(1-2-12)بتصرف

- بعد انفجار فقاعة اليابان الاقتصادية في أوائل التسعينيات، بدأ الناتج المحلي الإجمالي الحقيقي في الانخفاض بشكل حاد. استمر هذا الركود طويل الأجل لما يقرب من ٢٥ عاما[١].
- لدى بتكوين الآن فقط ١٦ مليون في العالم، وبعد الانتهاء من تعدين جميع البتكوين سيكون عددها ٢١ مليون بتكوين فقط، بمعنى سيكون الطلب في ازدياد والكمية محدودة فيزيد السعر، إن البتكوين التي تضيع على أصحابها تضيع إلى الأبد فلا يمكن استرجاعها أيضاً كخطرٍ يهدد بقاء البتكوين، بما يعني أن البتكوين ستكون في انخفاض مستمر بينما الطلب في ارتفاع مستمر[٢].

.

[١] (Japan's Lost Decade:Lessons for Other Economies)ناويوكي ياشينو واخرون-بحث محكم بمجلة ADBI-institute—التابعة لمعهدبنك التنمية الاسيوي-العدد(521/ابريل2015)ص3

[٢] (bitcoin economics)-من إعداد ونشر —bit mex-الصادر في 30 مايو 2018م-ص11-13 بتصرف*انظر أيضا: (bitcoin mastring)-مرجع سابق-180-181.