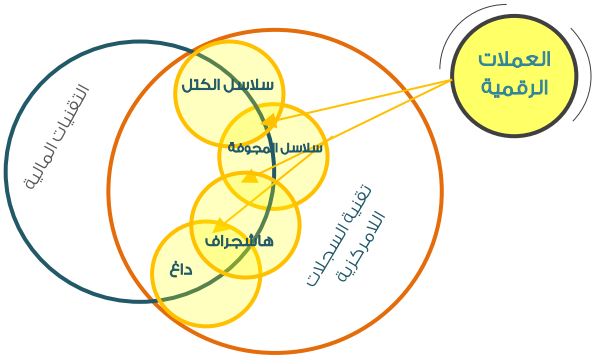
صندوق النقد العربي
ARAB MONETARY FUND

تقنيات العملات الرقمية

سلسلة كتيبات تعريفية
العدد (23)
موجهة إلى الفئة العمرية الشابة في الوطن العربي



إعداد

مهندس هشـــام رويـبـي

صندوق النقد العربي
2021

توجه جميع المراسلات إلى العنوان التالي:

الدائرة الاقتصادية

صندوق النقد العربي

ص.ب. 2818 – أبوظبي – دولة الإمارات العربية المتحدة

هاتف: 97126171552+

فاكس: 97126326454+

البريد الإلكتروني: Economic@amfad.org.ae

الموقــع الإلكتروني: https://www.amf.org.ae

هذا الكتيب يستهدف غير المختصين في الشأن الاقتصادي والمالي في الدول العربية ويخاطب بشكل عام الفئة العمرية الشابة بهدف تعزيز فهمهم بأساسيات تقنيات العملات المشفرة واستعمالاتها.

المتحتويات

1. تقديـــم

سعى الإنسان منذ الأزل إلى إيجاد طرق لتبادل السلع والخدمات والمنافع بطرق آمنة وفعالة، ونتج عن ذلك تطور مستمر في وسائل الدفع وتيسيرها بطرق عدة، سواءً بما يشمل إيجاد وسائط لتسهيل التداول، ومن ثم تصنيعها بشكل فريد يصعب تقليده بإستعمال المعادن الثمينة أو العملات النقدية والورقية أو ما يقابلها من وسائل دفع موازية مثل الشيكات والبطاقات الإئتمانية، إلى أن تم تطوير العملات الرقمية.

العملات الرقمية غير الصادرة عن البنوك المركزية والتي لا يوجد غطاء نقدي يقابلها في الواقع، تم تطويرها بالاستفادة من تقدم علوم الحوسبة والبرمجيات وقواعد البيانات والمعالجات وغيرها من التجهيزات التي أتاحت إمكانية التعدين الافتراضي لهذه العملات (على غرار العمليات المستخدمة لاستخراج المعادن من باطن الأرض)، وتوفير أساليب لحماية ملكية هذه العملات وكذلك تحويلها من شخص إلى آخر. ليس ذلك فحسب، بل وتوفير أساليب لضمان إستقلاليتها بحيث لا يوجد طرف أو جهة مركزية يُناط بها مهمة إصدار العملة الرقمية أو التحكم فيها (نظرياً على الأقل). وقد ينظر إلى هذا الجانب من الناحية السلبية، إلا أنه في المقابل له إيجابيات واضحة أتاحتها التقنيات الحديثة لأول مرة في التاريخ منذ بداية إصدار العملات التقليدية الرسمية.

تتسارع الدول حالياً إلى إعتماد العملات الرقمية الصادرة عن البنوك المركزية كعملات قانونية من المتوقع أن تحظى بقبول واسع النطاق، مما يشجع المزيد من الجهات الفردية والمؤسسات لإستعمالها وبالتالي إتجاه عدد متزايد من الدول لإعتمادها.

2. أهداف ونطاق الكُتيب

1.2 الأهداف

يهدف هذا الكُتيب إلى توفير مرجعية لأهم التقنيات الخاصة بإصدار العملات الرقمية وتقنيات الدفع المتعلقة بها، وتطوراتها المتوقعة خلال الفترات القادمة، لوضع الخطوات الأولى لكل من يرغب الإطلاع أو إكتساب المزيد من المعرفة الفنية في هذا المجال.

يستهدف الكُتيب الفئات الشابة ضمن مبادرات صندوق النقد العربي كمؤسسة إقليمية عربية تُعنى بتطوير القطاع المالي والنقدي في الدول العربية، لنشر الوعي بموضوع العملات الرقمية الذي يكتسب أهميةً كبيرةً في المرحلة الراهنة، وقد أصدر الصندوق كتيب آخر عن واقع العملات الرقمية ضمن هذه السلسلة.

كما يهدف إلى إعطاء صورة واضحة حول التقنيات المستخدمة في إصدار هذه العملات بما يُمكِن كذلك من إستشراف المخاطر الممكنة التي قد تنشأ عن إحتمالات تغير تقنية معينة أو إزدهارها على حساب تقنيات أخرى أو حتى إحتمال إندثارها.

2.2 النطاق

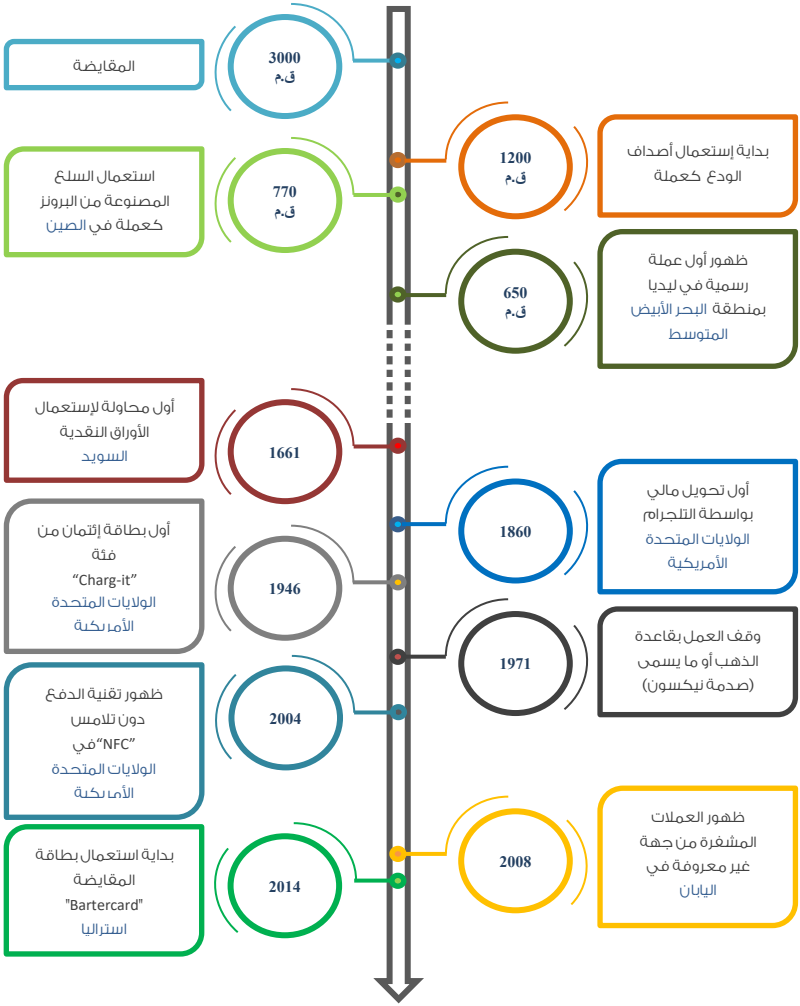
يشمل هذا الكُتيب كل التقنيات الخاصة بالعملات الرقمية وأنظمتها التقنية الحديثة المتوفرة إلى تاريخه، ويُستثنى من ذلك أنظمة الدفع الأخرى.

3. لمحة تاريخية عن تطور وسائل الدفع

بدأ الإنسان بإستعمال وسائط لتبادل المنافع مثل الملح والبذور منذ زمن بعيد، ويُعطي المخطط التالي لمحة تاريخية ملخصة لتطور وسائل الدفع بصفة عامة وحاجة البشرية إلى مثل هذه الوسائط لتسهيل معاملاتها وتبادلاتها التجارية منذ آلاف السنين، وصولاً إلى تطوير العملات الرقمية التي لا مقابل مطبوع أو مادي لها في الواقع، وذلك بفضل تقنيات الحاسب الآلي وبصفة خاصة تقنية السجلات اللامركزية كما هي مفصلة في هذا الكتيب.

الشكل رقم (1)

لمحة تاريخية عن تطور وسائل الدفع

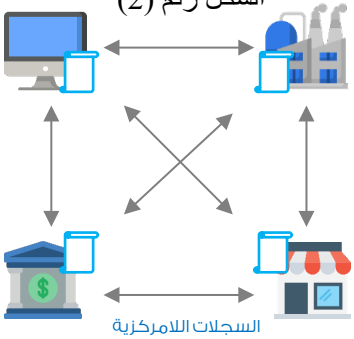


المصدر: مُعد الكُتيب بالاستناد إلى المصادر رقم 6 و 7 و8 و12 المُشار إليها في قائمة المراجع.

4. تقنية السجلات اللامركزية

(Distributed Ledger Technology) تعرف أيضا بالسجلات المشتركة ويرمز لها اختصاراً بـ (DLT)، وهي البنية التحتية التقنية والبروتوكولات التي تسمح بالوصول المتزامن لتحديث والتحقق من صحة السجلات في قاعدة البيانات بطريقة غير قابلة للتغيير من طرف واحد، وذلك عبر شبكة غير مركزية تضم كيانات أو مواقع متعددة.

الشكل رقم (2)

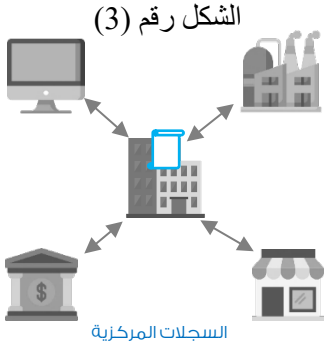


المصدر: مُعد الكُتيب بالإستناد إلى المصادر

ويستخدم في تقنية السجلات اللامركزية ما يسمى بالتشفير لتخزين البيانات والتوقيعات والمفاتيح المُشفرة بشكل آمن للسماح للمستخدمين المصرح لهم فقط بالوصول للبيانات.

تقوم التقنية أيضاً بإنشاء قاعدة بيانات غير قابلة للتغيير، مما يعني أنه بمجرد تخزين المعلومات، لا يمكن حذفها ويتم تسجيل أي تحديثات بشكل دائم مع الاحتفاظ بالأصل.

الشكل رقم (3)



المصدر: مُعد الكُتيب بالإستناد إلى المصادر

على عكس قواعد البيانات التقليدية، ليس لتقنية السجلات اللامركزية مكان مركزي لتخزين البيانات كما يدل عليه الإسم، بما يجعلها تتسم بكونها أكثر أماناً وشفافية وثقة بين الأطراف المستخدمة لها مقارنة مع قواعد البيانات التقليدية.

1.4 مصدر تقنية السجلات اللامركزية

تعود نشأة تقنية السجلات اللامركزية إلى شبكات "النظير إلى النظير (P2P)" وتسمى أيضا المشاركة المباشرة للبيانات المستعملة في قواعد البيانات الشبكية بصفة عامة، حيث تتواصل الأطراف المعنية دون الحاجة إلى جهة مركزية للتنسيق بينها، مما جعل تقنية السجلات اللامركزية ممكنة عبر هذا النوع من الشبكات، التي تستخدم كذلك خوارزميات إجماع (Consensus Algorithm) للتنسيق بين ما يسمى بالعقد (Nodes) لتعويض عدم وجود جهة مركزية تختص بإدارة البيانات.

2.4 مكونات تقنية السجلات اللامركزية

الشكل رقم (4)

المصدر: مُعد الكُتيب بالإستناد إلى المصادر

تتكون تقنية السجلات اللامركزية من عناصر وأدوات أربعة أساسية تمكنها من تحقيق أهدافها التي طورت من أجلها وهي مشتركة بين أغلب الأنواع التابعة لهذه التقنية بما يشمل التشفير والسجل المشترك وخوارزميات التوافق والعقدة وذلك على النحو التالي:

1.2.4 علم التشفير (Cryptography) : يرتبط علم التشفير بعملية تحويل النص العادي إلى نص غير مفهوم والعكس صحيح، فهي طريقة لتخزين البيانات ونقلها في شكل معين، بحيث لا يتمكن من قراءتها ومعالجتها إلا من وُجهت إليه.

كان التشفير سابقاً مرادفاً فعلياً للترميز، ولكن التشفير في الوقت الحاضر يعتمد بشكل أساسي على النظريات الرياضية وتطبيقات علوم البرمجة.

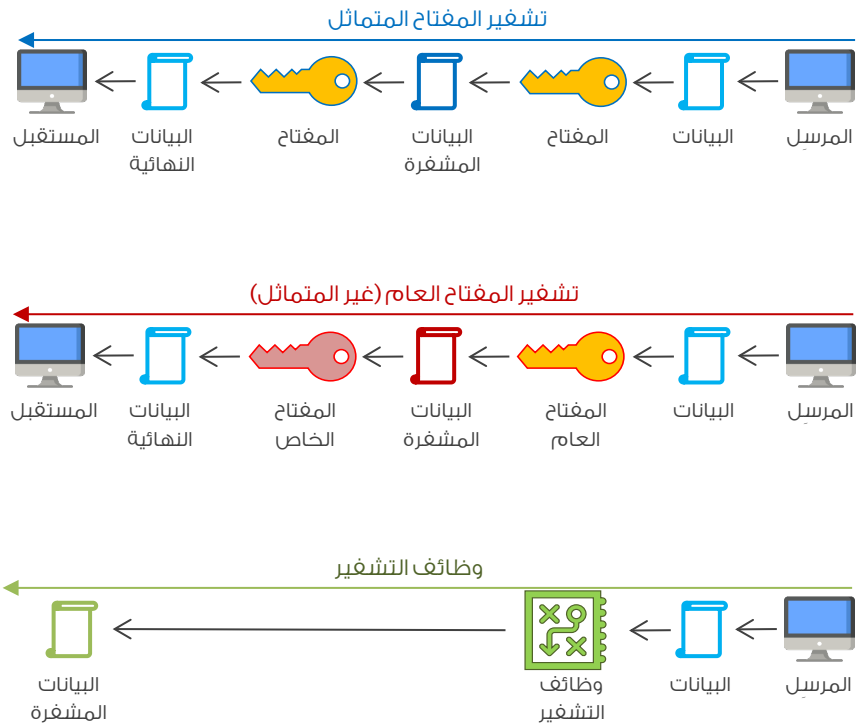
يرتكز علم التشفير الحديث على السرية بحيث لا يمكن لأي طرف أن يفهم المعلومات المتضمنة إلا الشخص المُرسل إليه ولا يمكن تغيير المعلومات والمسؤولية، أي أن المُرسل لا يمكنه إنكار نواياه في نقل المعلومة في مرحلة لاحقة. كما يمكن من خلال التشفير المصادقة على العمليات حيث يُمكن للمرسل والمستقبل تأكيد المعلومات المتضمنة. يُشار إلى أن التشفير يُستخدم في العديد من التطبيقات، مثل بطاقات المعاملات المصرفية، وكلمات مرور أجهزة الحاسب الآلي، ومعاملات التجارة الإلكترونية، وهناك ثلاثة أنواع من تقنيات التشفير بشكل عام وهي:

1.1.2.4 تشفير المفتاح المتماثل (Symmetric-key Cryptography):
حيث يشترك كل من المرسِل والمستقبل في مفتاح واحد، ويستخدم المرسِل هذا المفتاح لتشفير النص العادي وإرسال النص المشفر إلى جهاز الإستقبال. وفي الجانب الآخر، يطبق المتلقي نفس المفتاح لفك تشفير الرسالة وإستعادة النص الأصلي.

2.1.2.4 تشفير المفتاح العام (Public-key Cryptography): يعتبر تشفير غير متماثل ويستعمل فيه مفتاحين عام وخاص مرتبطين ببعضهما البعض، بحيث يتم إعطاء قيمة للناتج بطول ثابت انطلاقاً من النص العادي المراد تشفيره، مما ينتج عنه عدم إمكانية إسترداد محتويات النص العادي إلا بمعرفة ارتباط القيم الناتجة به، قد تتم إتاحة المفتاح العام، بينما يظل المفتاح الخاص المقترن به سراً لا يعرفه إلا المستخدم لهذا المفتاح، بحيث يتم إستخدام المفتاح العام للتشفير والخاص لفك التشفير.

3.1.2.4 وظائف التشفير (Hash Functions): يعتبرهذا المفهوم الأكثر ثورية في مجال التشفير، وهي دالة رياضية في شكل خوارزميات تقوم بتحويل معطيات ذات طول عشوائي إلى ناتج مشفر بطول ثابت، وبالتالي وبغض النظر عن المقدار الأصلي للبيانات أو حجم الملف، يظل الناتج دائماً بنفس الحجم، علاوة على ذلك لا يمكن الذهاب في الإتجاه المعاكس باستخدام المعطيات الأولية من الناتج المشفر، نظراً لأن وظائف التشفير "أحادية الاتجاه".

الشكل رقم (5)
أنواع تقنيات التشفير



المصدر: مُعد الكُتيب بالاستناد إلى المصادر رقم 1 و5 المُشار إليها في قائمة المراجع.

فيما يلي قائمة بأهم خوارزميات وظائف التشفير المستعملة في مجال العملات الرقمية وغيرها من المجالات:

جدول رقم (1)
أشهر خوارزميات التشفير المستخدمة

A5A v2	DEDAL	NeoScrypt	SoftCrypton
Aergo	ZHash	Nist5	SonoA
Allium	Equihash 192 7	Pascal RandomHash	Tensority
Argon2	Equihash 200 9	pGap	TimeTravel
Argon2d	Equihash 210 9	PHI1612	TimeTravel 10
Argon2i	Ethash	PHI2	Tribus
Balloon Hashing	Exosis	Polytimos	UBQhash
BCD	Fresh	Prime Constellation	VerusHash
BLAKE-256	Grøstl 512	Prime Six	X11
BLAKE2b	HEX	ProgPoW	X11 Binarium
BLAKE2s	HMQ1725	Quark	X11 Evo
BTHash	Keccak	Qubit	X11 Spread
C11	LBK3	Scrypt	X13
CryptoHello	LBRY	Scrypt²	X14
CryptoNight	Lyra2RE	Scrypt ChaCha	X15
CryptoNight	Lyra2REv2	Scrypt N	X16R
CryptoNightFast	Lyra2REv3	SHA 224	X16S
CryptoNightHeavy	Lyra2vc0ban	SHA 256	X21S
CryptoNightLite	Lyra2Z	SHA 256d	Xevan
CryptoNightLiteV1	Lyra2z330	SHA 256T	Yescrypt
CryptoNightV7	Lyra2Zoin	Shabal 256	YescryptR16
Cunninghamchains	MD5	Skein	YescryptR32
DaggerHashimoto	MTP	Skein SHA2	YesPoWer
Dcrypt	Multi algorithm	SkunkHash	

المصدر: مُعد الكُتيب بالاستناد إلى المصادر رقم 1 و5 المُشار إليها في قائمة المراجع.

2.2.4 العقدة (Node): تسمى أيضا نقطة التواصل، يُطلق على أي نظام أو جهاز متصل بشبكة عقدة، فعلى سبيل المثال، إذا قامت إحدى الشبكات بتوصيل خادم ملفات وأجهزة حاسب آلي وطابعات، فكل جهاز يحسب على أنه عقدة على الشبكة. يحتوي كل جهاز في الشبكة على عنوان شبكة، مثل عنوان (MAC) الذي يُعرّف كل جهاز أو نظام بشكل فريد بما يُساعد على تتبع مكان نقل البيانات من وإلى الشبكة.

يمكن أن تشير العقدة أيضًا إلى "ورقة (Leaf) " وهي عبارة عن مجلد أو ملف على القرص الصلب في جهاز الحاسب الآلي وتسمى عقدة أو النقطة العقدية.

3.2.4 السجل المشترك (Shared Ledger): يسمى أيضا بالسجل الموزع وهي قاعدة بيانات يتم مشاركتها بالتزامن والتراضي عبر مواقع أو مؤسسات أو مناطق جغرافية متعددة، ويمكن الوصول إليها من قبل عدة أطراف، ويسمح للتحويلات أن يكون لها شهود من العامة، ويمكن للمشارك في كل عقدة في الشبكة الوصول إلى البيانات المشتركة عبر تلك الشبكة، وامتلاك نسخة مطابقة منها، وتنعكس أي تغييرات أو إضافات يتم إجراؤها على السجلات، ويتم نسخها على أجهزة جميع المشاركين في غضون ثوانٍ أو دقائق.

4.2.4 خوارزميات التوافق (Consensus Algorithm): هو بروتوكول يعتمد على التصويت في إطار تقنية السجلات الموزعة للوصول إلى عملية صنع القرار لمجموعة ما، حيث يقوم أفراد المجموعة ببناء ودعم القرار الذي يعمل بشكل أفضل لبقية المجموعة، بما يُمثل شكلاً من أشكال القرار، حيث يحتاج الأفراد إلى الأغلبية لدعم القرار في إطار الشبكة.

بعبارات بسيطة، إنها مجرد طريقة لاتخاذ القرار داخل المجموعة، ويوضحها المثال التالي: لنتخيل مجموعة من الأشخاص يريدون اتخاذ قرار بشأن مشروع يفيدهم جميعاً. في هذه الحالة، يُمكن أن يكون لكل واحد منهم اقتراح فكرة، لكن الأغلبية ستؤيد الفكرة التي تساعدهم بشكل أكبر، فيما يتعين على الآخرين التعامل مع هذا القرار سواءً وافقوا عليه أم لا. ولنا أن نتخيل تطبيق نفس الشيء مع أعداد كبيرة من الأشخاص، وهو ما سيجعل الأمر أكثر صعوبة دون إستخدام مثل هذه التقنيات.

ولا تتفق خوارزميات التوافق فقط مع أصوات الأغلبية، ولكنها تتوافق أيضاً على القرار الذي يفيدهم جميعاً، لذا فهو دائماً مكسب للمجموعة.

جدول رقم (2)
قائمة الخوارزميات التوافقية المستعملة

▪ Proof of Work	▪ دليل العمل
▪ Proof of Stake	▪ إثبات الحصة
▪ Casper	▪ كاسبر
▪ Delegated Proof of Stake	▪ تفويض إثبات الحصة
▪ Practical Byzantine Fault Tolerance	▪ التسامح البيزنطي العملي
▪ Simplified Byzantine Fault Tolerance	▪ التسامح البيزنطي المبسط

▪ Delegated Byzantine Fault Tolerance	▪ التسامح البيزنطي المفوض
▪ Proof of Activity	▪ إثبات النشاط
▪ Proof of Importance	▪ إثبات الأهمية
▪ Proof of Capacity	▪ إثبات المساحة
▪ Proof of Burn	▪ إثبات الحرق
▪ Proof of Weight	▪ إثبات الوزن
▪ Open Representative Voting	▪ التصويت التمثيلي المفتوح
▪ Stellar Consensus Protocol	▪ بروتوكول توافق النجوم
▪ Proof Of Service	▪ دليل الخدمة
▪ Proof of Previous Transactions	▪ دليل التحويل السابق
▪ Leased Proof-Of-Stake	▪ إثبات ملكية مؤجر
▪ Proof of Elapsed Time	▪ إثبات الوقت المنقضي

المصدر: مُعد الكُتيب بالاستناد إلى المصدرين رقم 11 و16 المُشار إليهما في قائمة المراجع.

وفيما يلي تعريفات مختصرة لخوارزميات التوافق الأكثر إستعمالا:

1.4.2.4 دليل العمل (PoW): من أوائل خوارزميات التوافق المستخدمة في تطوير العملات الرقمية التي تم استخدامها في الأصل بهدف عدم السماح بالاستخدامات الضارة لأنظمة الحوسبة وذلك باستخدام كمية مهمة من الطاقة، وفي وقت لاحق في عام 2004 طور "Hal Finney" هذا المفهوم من أجل استخدامه في تطوير العملات الرقمية ، باستخدام خوارزمية التشفير (SHA256) لتطوير فكرة "دليل العمل القابل لإعادة الاستخدام".

بعد طرحها في عام 2009، أصبحت بيتكوين أول تطبيق معتمد على نطاق واسع لفكرة "PoW"، والذي شكّل أساساً لتطوير عديد من العملات الرقمية الأخرى التي يتم الحصول عليها مقابل عمليات تعرف بالتعدين.

2.4.2.4 إثبات الحصة (PoS): ينص مفهوم إثبات الحصة على أنه يمكن لأي شخص التعدين (Mining) أو التحقق من المعاملات المحظورة وفقاً لعدد العملات التي يمتلكها. هذا يعني أنه كلما زاد عدد العملات التي يمتلكها من يعمل في مجال تعدين العملات الرقمية كلما زادت قوة التعدين لديه، وتتطلب قدر أقل بكثير من الطاقة، مقارنة مع دليل العمل، ويتلقى العامل رسوم مقابل ذلك.

3.4.2.4 كاسبر (Casper): هي خوارزمية توافقية جديدة تجمع بين كل من خوارزمية إثبات الحصة ودليل العمل، تم تطويرها من طرف "إثيريوم"، العملة المشفرة الشهيرة، بما يمثل ثورة في عالم العملات الرقمية ، وتقنية جديدة تنافس بها عملة "إثيريوم" العملات الأخرى من ناحية الحجم ورسوم التحويل.

4.4.2.4 تفويض إثبات الحصة (DPoS) : هي خوارزمية توافق، تم تطويرها لتأمين سلاسل الكتل من خلال ضمان تمثيل المعاملات داخلها. تم تصميم تفويض إثبات الحصة كتطبيق بهدف تكريس مبدأ الديمقراطية بالاستفادة من المزايا التي تتيحها التقنية، وذلك باستخدام عملية التصويت والانتخاب لحماية سلاسل الكتل من المركزية.

5.4.2.4 إثبات ملكية مؤجر (LPoS): هي نسخة من آلية تفويض إثبات الحصة المستخدمة في منصة "Waves"، تسمح لحاملي الرموز "بتأجير" الرموز المميزة الخاصة بهم إلى بعض العقد القائمة وكسب نسبة مئوية من العائد كمكافأة، في منصة إثبات الحصة العادية، ويمكن لكل عقدة إضافة كتلة جديدة إلى سلاسل الكتل.

6.4.2.4 إثبات الوقت المنقضي (PoET): عبارة عن خوارزمية آلية إجماع تُستخدم غالباً على شبكات سلاسل الكتل المصرح بها لتحديد حقوق التعدين أو الفائزين بالكتلة على الشبكة، وتنشيء كل عقدة في شبكة السجلات اللامركزية وقت انتظار عشوائي تذهب فيه إلى وضع السكون.

7.4.2.4 التسامح البيزنطي العملي للخطأ (pBFT): هي خوارزمية توافق تم تطويرها في أواخر التسعينيات من قبل "باربرا ليسكوف" و"ميغيل كاسترو"، وتم تصميمها للعمل بكفاءة في أنظمة غير متزامنة (لا يوجد حد أعلى عند استلام الاستجابة للطلب)، وتم تحسينها للوصول إلى اختصار وقت التأخير.

8.4.2.4 التسامح البيزنطي المبَسِط للخطأ (SBFT): حيث يجب أن تقبل الكتلة (Block) من قبل عدد معين من العقد، مع الأخذ في الإعتبار عدد العقد المعيبة. يشرتط هذا النظام موافقة عدد محدد من العقد بما يفوق أو يساوي (2ف+1)، حيث (ف) هو عدد العقد التي اكتشفت فيها الخوارزمية عيب أو عدم موثوقية، فمثلا إن كان عدد العقد المعيبة 5 عقد، فإن شرط قبول الكتلة يتمثل في قبول ما لا يقل عن 11 عقدة.

9.4.2.4 المفوض البيزنطي للخطأ المتسامح (dBFT): وهي آلية إجماع بيزنطية متسامحة مع الأخطاء تتيح المشاركة على نطاق واسع في التوافق من خلال التصويت بالوكالة، يمكن لحامل رمز "NEO" اختيار المحاسب (bookkeeper) الذي يدعمه من خلال التصويت.

10.4.2.4 إثبات النشاط (PoA): يجمع بين مكونات إثبات العمل، وإثبات الحصة، ويبدأ التعدين أولاً بالطريقة التقليدية، حيث يتنافس القائمين على تعدين هذه العملات ليكونوا أول من يحل لغزاً معقداً ويطالبون بمكافئتهم، ويتمثل الفرق هنا في كون الكتل التي يتم تعدينها لا تحتوي على معاملات، إنما مجرد قوالب تحتوي على معلومات، إسم وعنوان مكافأة التعدين، وبمجرد أن يتم تعدين هذه الكتلة الفارغة تقريباً، يتحول النظام إلى بروتوكول إثبات الحصة.

11.4.2.4 إثبات الأهمية (DPoI): تدمج خوارزمية التوافق هذه مفاهيم تفويض إثبات الحصة مع ما تؤكده التفاعلات من نشاط اقتصادي بين الأفراد أو الجهات، ويتم تحقيق التوافق بمساعدة المندوبين، ويتم انتخاب المندوبين من قبل المشاركين في الشبكة على أساس أهمية كل ناخب.

12.4.2.4 إثبات المساحة (PoSpace): يُطلق عليه أيضًا إثبات السعة (PoC)، وهو وسيلة لإثبات أن المرء لديه مصلحة مشروعة في خدمة ما، من خلال تخصيص قدر مهم من الذاكرة أو مساحة القرص لحل مشكلة ما حسب التحدي الذي قدمه مزود الخدمة.

13.4.2.4 إثبات الحرق (PoB): تعمل هذه الخوارزمية التوافقية على الحد من التكاليف بضخ الأموال في أجهزة الحاسب الآلي باهظة الثمن، بحيث يتم "حرق" العملات المنتهية عن طريق إرسالها إلى عنوان لا يمكن استردادها فيه، من خلال كمية عملاتك الرقمية المحروقة، فإنك تكسب إمتيازاً مدى الحياة للتعدين على النظام بناءً على عملية إختيار عشوائية.

14.4.2.4 إثبات الوزن (PoWeight): وهو تصنيف واسع لخوارزميات التوافق يستند إلى نموذج توافق يسمى "Algorand". وفكرته هي أنه في نقاط البيع "POS"، تمثل النسبة المئوية للرموز المملوكة في الشبكة إحتمالية إكتشاف الكتلة القادمة، في هذا النظام يتم إستخدام بعض القيم التقريبية المرجحة نسبياً.

15.4.2.4 التصويت التمثيلي المفتوح (ORV): يمكن لكل حساب اختيار ممثل في أي وقت للتصويت نيابة عنه، حتى عندما يكون الحساب المفوِض نفسه غير متصل بالشبكة العالمية للمعلومات. يتم تكوين حسابات الممثل على العقد التي تظل متصلة بالشبكة وتصوت على صحة المعاملات التي تظهر على الشبكة، ووزن تصويتهم هو مجموع أرصدة الحسابات المفوضة إليهم. وإذا كان لديهم وزن تصويت كافٍ، يصبحون ممثلين رئيسين، ويتم إعادة إرسال الأصوات التي يرسلها هؤلاء الممثلون الرئيسيون لاحقاً من قبل العقد الأخرى.

16.4.2.4 بروتوكول (SCP): يوفر بروتوكول توافق النجوم وسيلة للتوصل إلى توافق في الآراء دون الاعتماد على نظام مغلق لتسجيل المعاملات المالية بدقة.

17.4.2.4 دليل الخدمة: تتحكم العقد الرئيسة في تسجيل الشهادات وإبطالها باستخدام خوارزمية إجماع مخصصة لإثبات الخدمة تضمن أن هذه العقد يمكن أن توافق على الترتيب الذي يجب أن تُلحق به الإدخالات بالكتل.

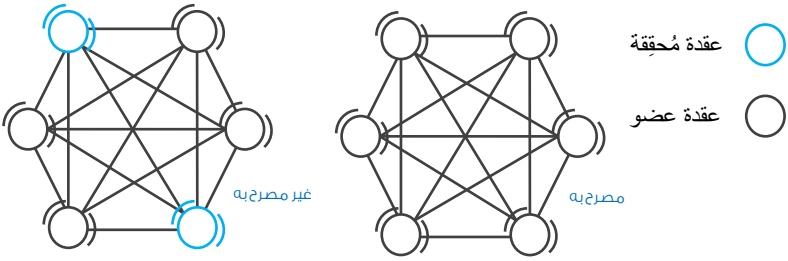
18.4.2.4 دليل التحويل السابق (PoPT): يستعمل لسجلات (JC Ledger) ويعتمد على ما يسمى سحابة مشتركة (Joint Cloud) ويمكنه تحسين موثوقية وملاءمة عمليات تبادل الموارد السحابية من خلال تمكين التعاون بين السحابات المتعددة، التحدي الأكبر لتنفيذ (JC Ledger) هو المفهوم التوافقي (Consensus)، حيث لا تنطبق خوارزميات الإجماع الحالية لسلاسل الكتل العامة مثل دليل العمل أو إثبات الحصة على السحابة المشتركة، لأنها تتطلب قوة حوسبة ضخمة.

3.4 أنواع السجلات المستعملة في تقنية السجلات اللامركزية

1.3.4 السجلات اللامركزية غير المصرح بها (Permissionless): يطلق عليها أيضاً السجلات اللامركزية "العامة" (Public)، وهي شبكات مفتوحة متاحة للجميع للمشاركة في عملية الخوارزمية التوافقية التي تستخدمها سلاسل الكتل للتحقق من صحة المعاملات والبيانات، وهي لامركزية بالكامل عبر أطراف غير معروفة.

2.3.4 السجلات اللامركزية المصرح بها (Permissioned): يطلق عليها أيضاً السجلات اللامركزية "الخاصة (Private)"، ويمكن اعتبارها نظام أمان إضافي لسلاسل الكتل، حيث تحتفظ بطبقة تتحكم في السماح بالوصول للقاعدة لاشخاص محددين من خلال تنفيذ إجراءات معينة فقط من قبل بعض المشاركين الذين يمكن التعرف عليهم. لهذا السبب، تختلف سلاسل الكتل هذه عن السجلات اللامركزية العامة.

الشكل رقم (6)
أنواع السجلات اللامركزية



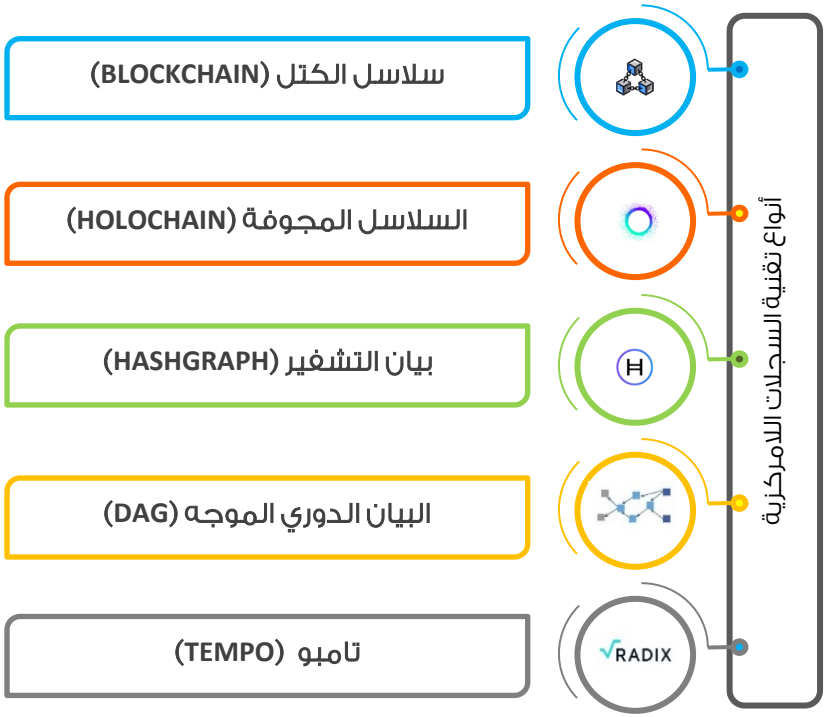
Source: Jürgen, B. and Udo, M. (2016). "Towards a framework for the evaluation and design of distributed ledger technologies in banking and payments", March.

3.3.4 السجلات اللامركزية الهجينة (Hybrid): وهي مزيج من السجلات العامة والخاصة، حيث يتم في إطارها استخدام السجلات اللامركزية العامة ولكن عبر استضافتها من خلال شبكة خاصة، وهو ما يعني أن هناك مشاركة مقيدة يتم التحكم فيها من خلال السجلات اللامركزية الخاصة نفسها.

4.4 تطبيقات وأنواع تقنية السجلات اللامركزية

تحتوي تقنية السجلات اللامركزية على العديد من التقنيات المتقاربة في المبدأ الخاص بعدم مركزية البيانات، ولكنها مختلفة، وبعضها تم تطويره استناداً إلى تقنيات أخرى سابقة كما هي مشروحة بالتفصيل في هذا البند.

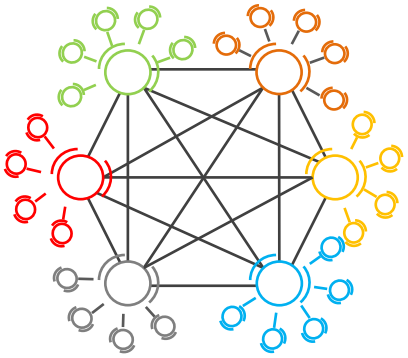
الشكل رقم (7)
أنواع تقنية السجلات اللامركزية



المصدر: مُعد الكُتيب بالاستناد إلى المصادر رقم 2 و 10 و 14 و15 المُشار إليها في قائمة المراجع.

1.4.4 سلاسل الكتل (Blockchain)

الشكل رقم (8)



المصدر: مُعد الكُتيب بالإستناد إلى المصادر

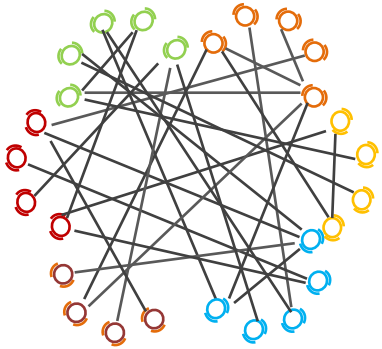
تسمى أيضا قواعد البيانات المتسلسلة، وهي نوع من تقنيات السجلات اللامركزية وجيل جديد من قواعد البيانات يتم فيها تنظيم البيانات بطريقة غير مركزية. تجمع سلاسل الكتل المعلومات معاً في مجموعات، تُعرف أيضاً بإسم الكتل (Blocks)، وتحتوي على مجموعات من البيانات. تتمتع الكتل بقدرات تخزين معينة وعند ملئها يتم ربطها بواسطة السلاسل في الكتلة المعبأة مسبقاً، لتشكيل سلسلة من البيانات تعرف باسم سلاسل الكتل. يتم تجميع المعلومات الجديدة التي تلي تكوين تلك الكتلة المضافة حديثاً في كتلة جديدة يتم إضافتها لاحقاً إلى سلسلة أخرى بمجرد ملئها وهكذا.

تختلف أنواع سلاسل الكتل بإختلاف السجلات المستخدمة فيها كما هي مفصلة في الفقرة (3.4) في هذا الكتيب، إضافة إلى النوع التحالفي الذي يُعد الأكثر شيوعاً، وفيه يكون العمل التوافقي من طرف مجموعة محددة مسبقاً وهي من النوع الأول المصرح به.

2.4.4 السلاسل المجوفة (Holochain)

توفر هذه التقنية إطاراً لتطبيقات التواصل والإرسال لإضافة البيانات بما في ذلك الأصول المصرفية إلى سلاسل الكتل، حيث يتم جمع السلاسل للدمج والتقسيم والتفاعل، ويتم تخزين هذه المعلومات بطريقة لامركزية. تحتوي البيانات على تشفير يرتبط بمقاييس بيوميترية عددية.

الشكل رقم (9)



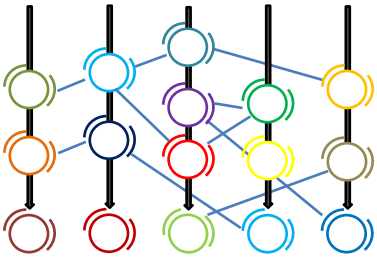
المصدر: مُعد الكُتيب بالإستناد إلى المصادر

على سبيل المثال، إذا حاول أي شخص إحداث تغيير ما في هذه البيانات، فإن التقنية تلاحظ الفرق بين البيانات والتشفير، ويتم رفض البيانات التي تغيرت، كما تضمن التوقيعات الرقمية عدم تشفير معلومات ملكية السلاسل المجوفة.

3.4.4 بيان التشفير (Hashgraph)

وهي تقنية سجلات لامركزية تقدم مزايا تقنية تعالج بعض عيوب سلاسل الكتل مثل عائق السرعة المنخفضة، ولاتتنافس تقنية السجلات اللامركزية هذه فقط مع سلاسل الكتل بل تتعداها لتنافس بعض مزودي الخدمة المشهورين.

الشكل رقم (10)

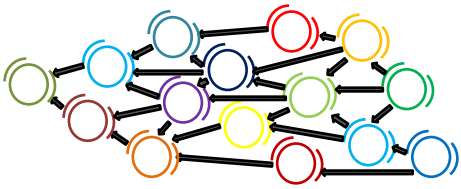


المصدر: مُعد الكُتيب بالإستناد إلى المصادر

تم إبتكار هذه التقنية من قبل "ليمون بيرد (Leemon Baird)" أحد مؤسسي شركة (Swirlds). تتمثل الميزة المهمة لتقنية بيان التشفير في كونها لا تحتاج إلى التحقق من صحة المعاملات، وبدلاً من تجميعها في كتل على غرار سلاسل الكتل، يتم معالجة المعاملات بشكل متزامن وتكون المعاملات موجهة في إتجاه واحد.

4.4.4 البيان الدوري الموجه (Directed Acyclic Graph)

الشكل رقم (11)



المصدر: مُعد الكُتيب بالإستناد إلى المصادر

هو نوع مختلف من بنية البيانات التي تفرض نفسها كقاعدة بيانات تربط مجموعات مختلفة من المعلومات، وهي تتألف من مجالات وخطوط تربطها لتوجهها في نفس الاتجاه، وهي دورية كما يدل عليه إسمها أي أنه لا يمكنك العودة إلى نقطة البداية إذا بدأت وإتبعت البيان في لحظة معينة.

البيان الدوري الموجه هو بنية بيانات رسومية بترتيب طوبولوجي يمتد فيه التسلسل فقط من السابق إلى اللاحق، وغالباً ما تستخدم هذه التقنية لمعالجة البيانات وجدولتها وإيجاد أفضل طريقة للتنقل ومعالجة التحديات. كما أنها تستخدم للتطبيقات التي تتطلب آلاف المعاملات في الثانية ولديها قابلية للتوسع.

5.4.4 تامبو (Tempo)

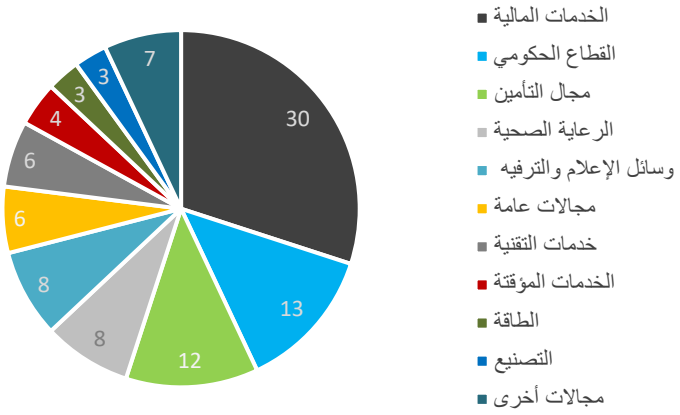
تم تصميم تقنية السجلات اللامركزية "تامبو" والتي تسمى أيضا (Radix) بما يخدم العملة المشفرة "Rad (XRD)" بهدف خفض مستويات تقلب هذه العملة بما يُمكن المستثمرين والشركات والمطورين من استخدام هذه العملة الرقمية مع تقلبات أقل لمستويات أسعارها.

من ميزات هذه التقنية أنها لا تحتاج إلى أجهزة حاسب آلي باهظة الثمن أو معدات تعدين أو رأس مال كبير للمشاركة من أجل تشغيل العقد والمشاركة في خوارزمية توافق الآراء ومعالجة المعاملات الخاصة بها.

5.4 استخدامات تقنية السجلات اللامركزية

تُستخدم تقنية السجلات اللامركزية في عدة مجالات ، قد تكون العملات الرقمية في المقدمة ، لكنها ليست الوحيدة. كما تستخدم هذه التقنية في قطاع العقارات ، والإعلام ، وإدارة التوريد ، وكشف الاحتيال ، والنقل ، والصحة ، والطاقة ، شكل (12). ومن المتوقع أن يتسع استخدام هذه التقنية من الأنواع المذكورة في هذا الكتيب أو أي أنواع قد تتطور في المستقبل لتشمل العديد من القطاعات والمجالات الأخرى ، أو حتى مجالات جديدة، لما تتمتع به من مزايا عديدة.

الشكل رقم (12)
استخدامات تقنية السجلات اللامركزية بحسب أهميتها النسبية (%)



Source: Mandelbrod, M. (2012). "Layered Hashing Algorithm for Real-time Systems", Feb.

5. العقود الذكية (Smart Contracts)

بينما كان يُنظر مسبقاً إلى تقنيات السجلات اللامركزية في المقام الأول على أنها تقنية داعمة بالأساس للعملات الرقمية، إلا أنها تطورت لاحقا إلى ما هو أبعد من ذلك بكثير. في هذا الإطار، تعتبر العقود الذكية من بين أهم الثمار المستفادة من التقنيات المذكورة في هذا الكتيب وعلى رأسها تقنية السجلات اللامركزية بمحتوياتها من تشفير وسجلات وعُقد وخوارزميات.

العقود الذكية هي عُقود ذاتية التنفيذ يتم فيها كتابة شروط الاتفاقية بين المشتري والبائع مباشرةً ضمن سطور البرمجيات (Code)، والاتفاقيات الواردة فيها، تتواجد عبر شبكة السجلات اللامركزية وبشكل غير مركزي كما يدل عليه إسمها

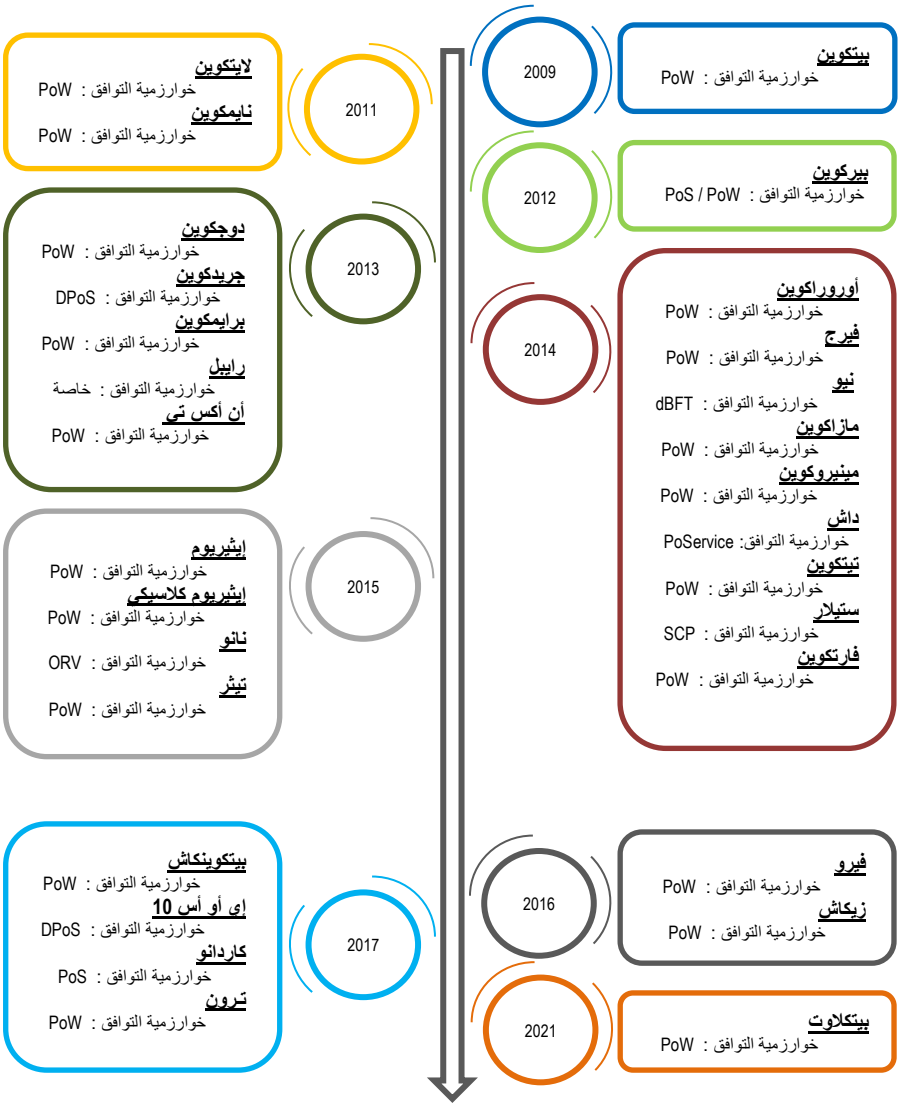
وكما تم شرحها في هذا الكتيب، حيث تتحكم الخوارزمية في التنفيذ، والمعاملات قابلة للتتبع ولا رجعة فيها. تسمح العقود الذكية بتنفيذ المعاملات والاتفاقيات الموثوقة بين أطراف متباينة ومجهولة الهوية دون الحاجة إلى سلطة مركزية أو نظام قانوني أو آلية إنفاذ خارجية.

6. العملات المشفرة (Cryptocurrencies)

العملة المشفرة هي عملة افتراضية بالكامل ولا تمثلها أي وسيلة مادية في أرض الواقع ويتم تأمينها بواسطة التشفير، مما يجعل عمليتي التزوير أو الإنفاق المزدوج من المستحيل تقريباً. تعمل العملات المشفرة على شبكات لامركزية تعتمد على تقنية السجلات اللامركزية (كما هي مفصلة في هذا الكتيب). ومن السمات المميزة للعملات المشفرة أنها لا تصدر غالباً من قبل أي سلطة مركزية، مما يجعلها من الناحية النظرية محصنة ضد سيطرة جهة مركزية عليها.

فيما عدا العملة المشفرة الشهيرة "بتكوين (Bitcoin)"، تسمى باقي العملات بالعملات البديلة أو " ألتكوينز(Altcoins)"، كما توجد فئة ثالثة من العملات المشفرة وهي العملات "المستقرة (Stablecoins)"، حيث يتم ربط سعرها بعملة مشفرة أخرى أكثر استقراراً، أو بأصول أخرى، أو سلع يتم تداولها في البورصة، مثل المعادن الثمينة، ويوجد حالياً العديد من العملات المشفرة، موضح أهمها في الشكل التالي بحسب ترتيب تاريخ ظهورها.

الشكل رقم (13)
العملات المشفرة حسب تاريخ الصدور



Source: Josias N. (2021). "Blockchain & Cryptocurrency Regulation", Global Legal Group, Feb.

7. الخاتمـــة

تتوجه كل الكيانات والجهات حالياً وبشكل واضح إلى المجال الرقمي وأتمتة الأنظمة والتعاملات والاستغناء عن التعاملات الورقية بما يسمى "المعاملات صفرية الأوراق"، ومع التطور الهائل في مجالات البنوك الإلكترونية وأنظمة الدفع الإلكتروني، فلا شك في أن مجال النقد والعملات يتوجه كذلك في نفس الاتجاه. ونحن بالفعل لا نستعمل في يومنا هذا العملات الورقية والمعدنية إلا نادراً، فأغلب الفواتير والمشتريات بشتى أنواعها تتم بواسطة البطاقات بأنواعها أو عن طرق إدخال بياناتها في جهاز حاسب أو بواسطة الهاتف النقال.

يرى بعض الداعمين للمزيد من الدفع باتجاه العملات الرقمية أن أبرز فوائدها تتمثل في الحد من مخاطر التضخم، وتقييد السلطة المطلقة للبنوك المركزية حول العالم في إصدار العملات، بما يتماشى مع التطورات على صعيد مستويات الناتج من السلع والخدمات، بما يحدث الضغوطات التضخمية. فهذه العملات ومن أبرزها "البيتكوين" لها حجم معروض نقدي محدد منذ بداية تصميم وإصدار النظام بما يسمح بالحفاظ على قيمة العملة عبر الزمن بل وارتفاعها بما يسمح بمكافحة الضغوطات التضخمية.

كذلك قد تكون العملات المشفرة من نوع "العملات المستقرة" حلاً وسطاً قد تجده الجهات الرسمية مناسباً للتبني، مع تطور تقنيات الدفع الحديثة وحاجة البنوك المركزية إلى تقييد استعمال النقد خاصة في أعقاب جائحة كوفيد-19. بات واضحاً كذلك توجه عدد من الحكومات نحو إعتماد العملات الرقمية الصادرة

عن البنوك المركزية كعملة قانونية يسمح تداولها على نطاق واسع، ومع الكم الهائل من العملات المشفرة التي تصدر قد تتوجه كل حكومة أو تحالف اقتصادي إلى إصدار عملة مشفرة خاصة بها.

علاوة على ما سبق، ومع تطور التقنيات التي تعتمد عليها العملات المشفرة، ويأتي على رأسها تقنية السجلات اللامركزية التي باتت تشهد إزدهاراً كبيراً وفي مجالات أكثر بكثير من العملات المشفرة كما سبق الإشارة، من المتوقع في المستقبل التوسع في إستخدام هذه التقنيات في العديد من المجالات، بما يستدعي المزيد من التركيز والاهتمام من قبل صناع القرار على دراسة هذه التطورات التقنية واللحاق بالركب العالمي في الاستفادة من الفرص التي تتيحها من جهة، والتحوط للمخاطر التي قد تنتج عنها من جهة أخرى.

8. المصادر

1/ Al-odat, z. , ali, m., abbas, A. & khan, s. (2020), “Secure Hash Algorithms and the Corresponding FPGA Optimization techniques”, ACM Computing Surveys , Sep.

2/ Bott, J. & Milkau, U., (2016), “Towards a framework for the evaluation and design of distributed ledger technologies in banking and payments”, Journal of payments strategy & systems, Nov.

3/ Fu, X., Wang H., Shi P,. (2021),"Proof of Previous Transactions (PoPT): An Efficient Approach to Consensus for JCLedger”, IEEE Transactions on Systems, Man, and Cybernetics Systems, Apr.

4/ Garrick, H. and Michel, R. (2017), “GLOBAL BLOCKCHAIN BENCHMARKING STUDY”, Golf Australia , Feb

5/ Gennaro, R., Gertner, Y., Katz, J. and Trevisan, L. (2005). “Bounds on the Efficiency of Generic Cryptographic Constructions”, SIAM Journal on Computing, Feb.

6/ Glyn, D. (2003), “ History of Money”, Economic Affairs. Dec

7/ Jamie, R. (2017),"Satoshi Nakamoto's Brilliant White Paper Turns 9-Years Old”, Bitcoin.com, Oct.

8/ Jenks, J. (1966) “Chapters on the History of money”, Financial Analysts Journal, Sep.

9/ Josias N. (2021). “BLOCKCHAIN & CRYPTOCURRENCY REGULATION”, Global Legal Group, Feb.

10/ Kauflin, J. (2019), “Hedera Hashgraph Thinks It Can One-Up Bitcoin And Ethereum With Faster Transactions”, Forbes.com , March.

11/ Laphou, L., Zecheng, A., Songlin h., Songtao g., yuanyuan y. and bin x, (2020). “Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling”. The Hong Kong Polytechnic University, Feb.

12/ Liuliang, Y. and Hong, Y. (2004), "Chinese Coins: Money in History and Society.”, Long River Press, Nov

13/ Mandelbrod, M. (2012), “ Layered Hashing Algorithm for Real-time Systems.” Theory of Computing Systems. Feb

14/ Maull, R., Godsiff, P., Mulligan, C., Brown, A., and Kewell, B. (2017). “Distributed ledger technology: Applications and implications”, Strategic Change , Sep.

15/ Md Arafatur, R., Balamurugan, B., Neeraj, K. and Gayathri N. (2020) “Blockchain, Big Data and Machine Learning: Trends and Applications edited”, Feb.

16/ Rui, Z., Rui X. & Ling L. (2019), ”Security and Privacy on Blockchain.” ACM Computing Surveys, Jan.

17/ Sakai, K. Qiong, H. Zongyang, Z. (2017) “identity-based non-interactive key exchange revisited and more and Yu Chen”, International Journal of Information Security, Feb.

18/ Shermin, V. (2019), ”Token Economy How Blockchains and Smart Contracts Revolutionize the Economy”, Shermin Voshmgir; Edition ed, Jun.

19/ Team of ARFWG, (2020), “Financial Technology Glossary”, Arab Regional Fintech Working Group, Nov.

20/ Timoney, M, (2002), “Bartering Set to Enhance the Credit Function”, Credit Control, Dec.

صدر من سلسة كتيبات صندوق النقد العربي الموجهة إلى الفئة العمرية الشابة في الوطن العربي الأعداد التالية:

م	المؤلف	عنوان الكتاب	السنة
1	حنان الطيب	الشمول المالي	2020
2	رانيا سليمان	أساسيات التمويل	2020
3	نرمين مجدي	الذكاء الاصطناعي وتعلم الآلة	2020
4	نفيسة الخير	التقنيات المالية الحديثة	2020
5	رشا العشي	تعزيز الثقافة المالية للمرأة وتمكينها اقتصادياً ومالياً	2020
6	نورا رزق	المؤسسات المالية غير المصرفية	2021
7	ولاء سعد أبوزيد	المحفظة الرقميّة	2021
8	زينة مزيان	توعية فئة الشباب بأهمية الادخار "مُوجّه إلى الفئة العمرية الشابة في الوطن العربي	2021
9	غسان أبوموريس	مخاطر غسل الأموال	2021
10	أيمن صالح	واقع العملات الرقمية	2021
11	رانيا سليمان	Have You Ever Thought of Being an Economist?	2021
12	عصام إسماعيل	مخاطر التركز الائتماني في المؤسسات المالية والمصرفية	2021
13	سامر بابكر	اقتصاد المعرفة	2021
14	أحمد حمد حمدناالله	واجبات ومسؤوليات شركات المعلومات الائتمانية	2021
15	مها سمهدان وتمارا سلمو	انعكاسات الذكاء الاصطناعي على مجال التدقيق	2021
16	محمود عبد السلام	تقنية البيانات الضخمة	2021
17	محمد ادريس	السياسة النقدية	2021
18	رانيا طه	"التضخم: أسبابه، آثاره، وسبل معالجته "	2021
19	نرمين مجدي	مفاهيم اقتصادية أساسية: الناتج المحلي الإجمالي	2021
20	جمال قاسم ومحمود عبد السلام	التجارة الإلكترونية	2021
21	د. عبد الكريم قندوز	الأسواق المالية	2021
22	أفنان خليل	نُظم الضمانات المنقولة	2021
23	مهندس هشام رويبي	تقنيات العملات الرقمية	2021

للحصول على مطبوعات صندوق النقد العربي

يرجى الاتصال بالعنوان التالي:

صندوق النقد العربي

شبكة المعرفة

ص.ب. 2818

أبوظبي - الإمارات العربية المتحدة

هاتف رقم: 6215000 (9712+)

فاكس رقم: 6326454 (9712+)

البريد الإلكتروني: Publications@amfad.org.ae

متوفرة إلكترونياً بموقع الصندوق على الشبكة العالمية للمعلومات من خلال الرابط التالي:

https://www.amf.org.ae