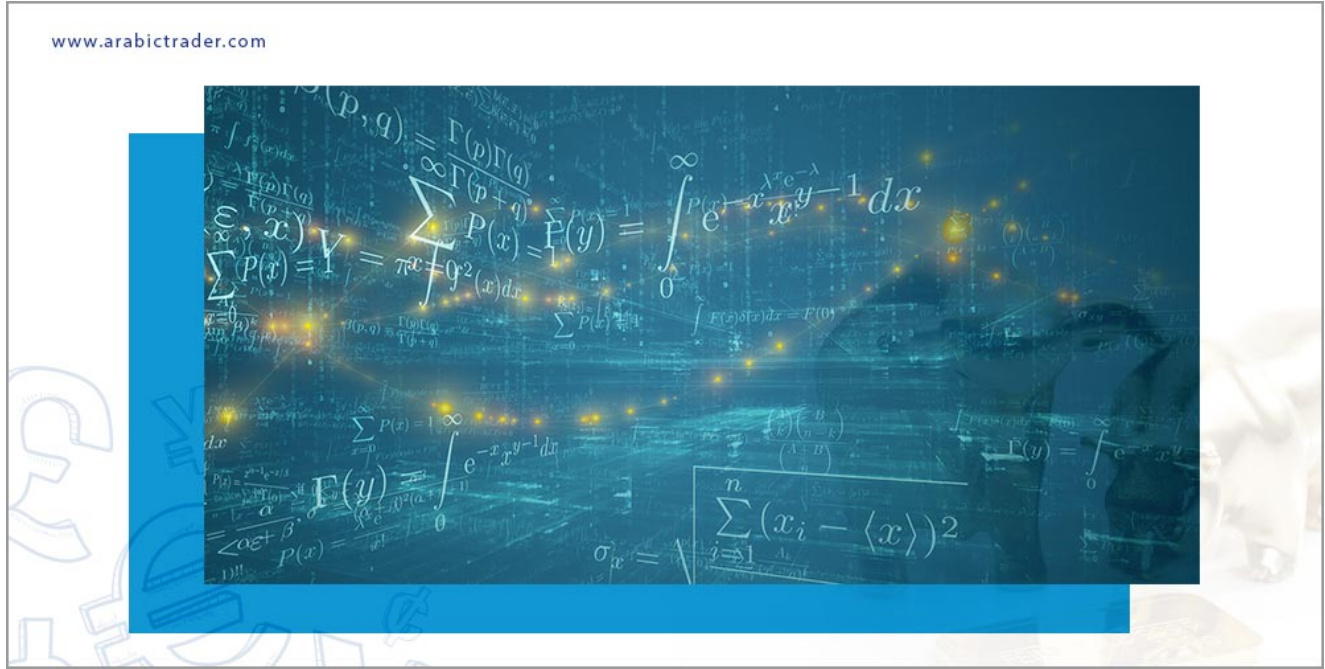
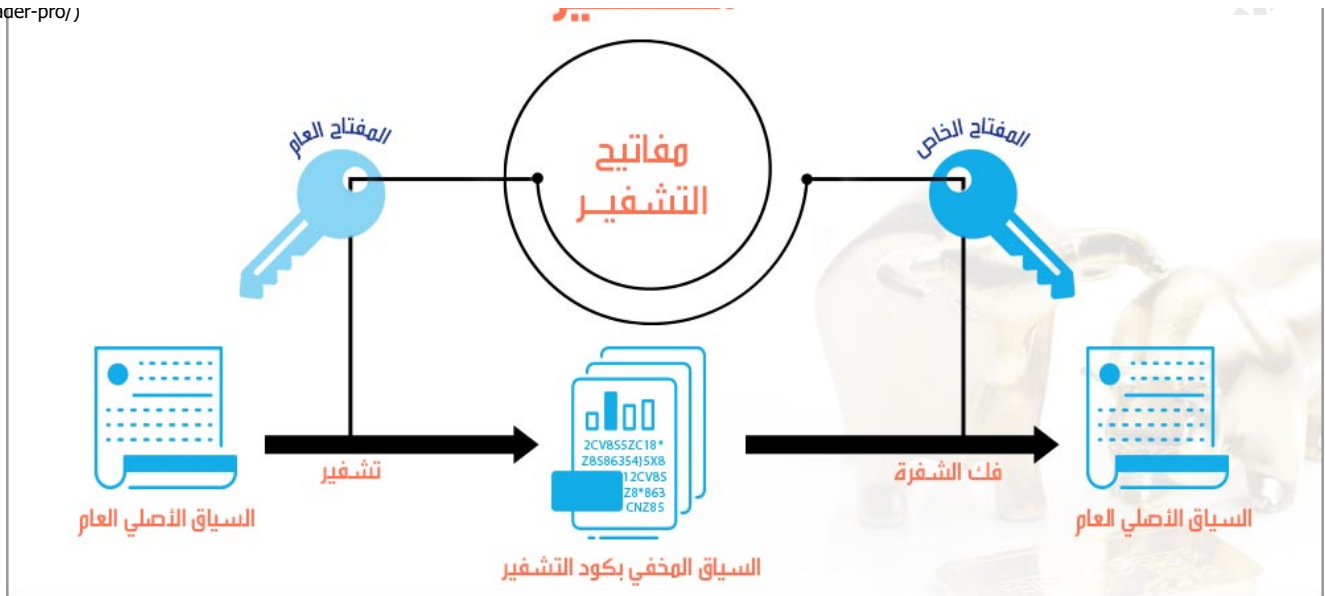


مفهوم علم التشفير Cryptography

قبل التعرف على العملات الرقمية أو العملات المشفرة، تعالوا نتعرف على علم التشفير أو التعمية Cryptography والذي يعزى له طريقة خلق واستخدام تلك العملات.



عملية التشفير Cryptography هي في الأصل وسيلة لحماية المعلومات والبيانات من خلال استخدام الرموز بحيث لا يمكن قراءتها أو معرفة محتواها المخفي إلا من تستهدفهم المعلومات ويكون لديهم مفتاح الشفرة التي تمكنهم من معالجة تلك الرموز للتعرف على المعلومات الأصلية. ويمكن ترجمة كلمة تشفير أو Cryptography بتقسيمها إلى crypt وتعني مخفي و graphy وتعني كتابة أي أن المقصود بالمصطلح أنها محتوى مكتوب بطريقة تخفي فحواه.



أي إخفاء البيانات من سياقها المعتاد والمتداول إلى سياق آخر غير معلوم للعامّة بشكل يحفظ سرية محتواها، وهي ليست عملية مستحدثة، فمبدأ التشفير استخدم في العديد من المجالات الدبلوماسية والعسكرية قديماً وله استخدامات عديدة مصرفية ومعلوماتية في وقتنا المعاصر، حتى وصلنا إلى العملات الرقمية التي تعتمد في بنائها على نفس الفكرة

الفرق بين فك الشفرة Decryption و تحليل الشفرة Cryptanalysis

مقابل التشفير Encryption، يأتي فك الشفرة Decryption، وهي إعادة السياق المشفر إلى صورة المحتوى الأولي في سياقها المعتاد والمقروء من العامة قبل عملية التشفير، ويتم ذلك باستخدام مفتاح التشفير.

ومع تطور علوم الرياضيات والحاسب الآلي والاتصالات أصبحت عملية التشفير وفك التشفير تستند إلى خوارزميات حسابية معقدة يصعب حلها، وحتى لو كانت علمية كسر الشفرة أو حل هذه الخوارزميات - دون فكها بالطريقة التي أُعدت بها من البداية - متاحة نظرياً، فإنه يكون من غير الممكن القيام بها عن طريق الوسائل المعلوماتية المعروفة والموجودة حالياً، وهذا هو سبب ثبوت افتراض أمنها وسريتها إلى الآن.

وهذا ما عرف باسم تحليل الشفرة أو Cryptanalysis ويعني دراسة فك خوارزميات التشفير وتطبيقاتها للحصول على محتوى المعلومات أو الأصول المشفرة ومصدرها دون الوصول إلى المفتاح المطلوب للقيام بذلك.

أي أننا يمكننا اختصار الفرق بين فك الشفرة Decryption و تحليل الشفرة Cryptanalysis إلى أن فك الشفرة يعني إعادة سياق الرموز المشفر إلى حالته الأولى باستخدام مفتاح الشفرة والمعد من البداية لإعادة ترجمة هذه الرموز إلى ما كانت عليه، في حين أن تحليل الشفرة فهي محاولة فك تلك الرموز عن طريق التجربة والخطأ عدد مهول من المرات للوصول إلى حل خوارزمية التشفير لترجمة الرموز المشفرة ومعرفة السياق الأصلي دون معرفة المفتاح



كيف بدأت فكرة التعاملات النقدية الإلكترونية

إنطلاقاً من فكرة التشفير وفك الشفرة، وأيضاً تحليل الشفرة ولدت فكرة إنشاء العملات الرقمية Cryptocurrency أي العملة الافتراضية الرقمية التي تم تشفيرها للتعاملات الآمنة والسرية، حيث يتم إنشائها وتخزينها إلكترونياً دون وجود سلطة إشرافي أو بنك مركزي يتحكم فيها، ولا يوجد لها كيان فيزيائي ملموس مثل العملات الاعتيادية الأخرى أو ما يطلق عليه النقد الإلزامي الصادر عن البنوك المركزية مثل الريال السعودي SAR أو اليورو EUR أو الدولار الأمريكي USD.

فكرة التعامل الرقمية أو الإلكترونية البديلة للتعامل النقدي المعتاد بدأت في أواخر الثمانينيات تقريبا في هولندا في سلسلة محطات للتزويد بالوقود أو محطات البنزين على الطريق السريع كانت تحدث فيها سرقات كثيرة، وحاولت الإدارة إيجاد حل لهذه المشكلة، فقامت الإدارة بالاستعانة بمجموعة من المبرمجين والمطورين لربط النقود ببطاقات خاصة يستطيع من خلالها حاملها من السائقين الراغبين في التعامل مع هذه المحطات الحصول على الوقود منها دون الحاجة للتعامل بالنقود الورقية في تلك المحطات، وبذلك لا يوجد أو على الأقل ستقل بشكل كبير النقود من المحطات تقريبا لحالات السرقة، تطورت بعدها فكرة ميلاد بطاقات النقود الذكية، التي كانت تعكس فكرة النقود المحفوظة بشكل إلكتروني مشفر في البطاقة، في حين يكون في محطة الوقود جهاز لفك تلك الشفرة، وهو نقطة المبيعات أو ما يعرف اليوم بفكرة POS أو point-of-sale. وتعتبر هذه أول صورة للنقود الإلكترونية التي تطورت لتصل إلى ما وصلت عليه الآن.

بداية فكرة العملات الرقمية أو العملات المشفرة

استلهمه الـ!فكرة التعاملات الإلكترونية وتقريبا في نفس الوقت أو قبله بقليل، كانت هناك فكرة تجول في رأس برمجي أمريكي يدعى ديفيد شوم David Chaum فحواها يدور حول الخصوصية المالية ومحاولة محاكاة (ar/home) المعنوية أو الورقية إلى نقود رمزية يكون لها نفس القدرة على التعامل في المدفوعات والانتقال من يد إلى يد

بأمان وبخصوصية، فقام بابتكار صيغة خوارزمية يمكن من خلالها تمرير الأموال بين المرسل والمتلقي بشكل خفي غير متتبع عبر عملة رمزية أسماها وقتها Chaum أسس بعدها Chaum DigiCash كبنية أساسية لتنفيذ تلك العملية والتي استمرت لسنوات إلى أن وقع في عدة أخطاء تسبب في إفلاس DigiCash عام 1998 والتي على الرغم من ذلك كان قد وضع من خلالها أساساً قويا لفكرة الصيغ الخوارزمية للمعاملات النقدية الرمزية أو العملات الرقمية.

استكمالاً للفكرة ذاتها، برمجي أخر يدعى Wei Dai يبدأ في طرح فكرة نظام نقدي متكامل خفي غير متتبع يحقق به فكرة الخصوصية والأمان أطلق عليه أسم B-money حيث يتم التعامل من خلال أسماء مستعارة رمزية لتحليل العملات داخل شبكة غير مركزية، وقد قام بالفعل بعرض الورقة التقديمية whitepaper لمشروعه إلا أن الفكرة لم تلق الترحيب والرواج المطلوب، فلم يقدر لها النجاح، والجدير بالذكر أن الورقة التقديمية التي عرضها ساتوشي ناكامورا لفكرة البيتكوين Bitcoin - والذي سنتحدث عنه تفصيلاً في مقال لاحق- كانت تحتوي على بعض العناصر التي كانت مذكورة في الورقة التقديمية whitepaper لمشروع B-money مما يعني أنها كانت البداية الحقيقية للسباق نحو تطور العملات الرقمية.

نشأة العملات الرقمية

بعدما أصبح الطريق ممهداً أمام إنشاء العملات الرقمية، ومع التطور التكنولوجي والمعلوماتي ولدت بروتوكولات التشفير المعقدة المبنية على مبادئ الرياضيات وهندسة الكمبيوتر المتقدمة التي تجعل من المستحيل نظرياً تقريباً كسرها والتي اعتمد عليها مبرمجي العملات الرقمية من خلال أنظمة توكيد معقدة للغاية تقوم بتشفير عمليات نقل البيانات لتأمين وحدات التبادل الخاصة بها، إضافة إلى قدرتها على إخفاء هوية المتعاملين فيها مما يجعل التعاملات والتحويلات وتدفقات الأموال مجهولة المصدر بما يحقق مبدأ الخصوصية الذي كان المسعى الرئيسي منذ البداية.

وبذلك يمكننا القول أن العملة الرقمية هي برنامج حاسوب Software، لكنه برنامج لا مركزي، أي أنه لا يتم تنصيبه أو بناءه على جهاز واحد بعينه إنما هو موزع مما يعني أنه يتم استضافته على العديد من أجهزة الكمبيوتر للعديد من الأفراد في جميع أنحاء العالم بدلاً من الاستضافة على خادم server واحد من قبل فرد بعينه أو شركة محددة.

ويتم التحكم في عرض العملات الرقمية وقيمتها من خلال أنشطة مستخدميها من خلال أكواد بروتوكولات التشفير شديدة التعقيد، كل دالة وظيفية أو معاملة بداية من كيفية تسجيل المعاملات إلى كيفية تخزين البيانات تختزل في كود برمجي خاص عادةً ما يتم تخزينه في نوع من قواعد البيانات المعروفة باسم سلسلة الكتل - بلوك تشين blockchain والتي تعتبر بمثابة سجل شامل موزع محمي ومخفي لكافة بيانات ومعاملات العملة الرقمية، ومن خلال معالجة تلك الخوارزميات بشكل عام يتم منح العملة الرقمية للمستخدم الذي

يضيفه، معاملات إلى شبكة سلسلة الكتل أو بلوك تشين blockchain (ar/home/)

(ar/trade/https://www.arabictrader.com/ar/learn/forex-school/304/%D9%85%D9%81%D9%87%D9%88%D9%85-

%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%B3%D9%84%D8%B3%D9%84%D8%A9-

%D8%A7%D9%81%D9%82%D8%A8%D9%81-%D8%B3%D9%84%D8%B3%D9%84%D8%A9-

blockchain) وتعرف عملية إضافة المعاملات إلى blockchain التعدين (Mining).

بقى أن نعرف أن من أهم ما يميز معظم العملات الرقمية، وليس كلها، هي أن لها أعداد محدودة من الوحدات. أي أنه تم إنتاج معظم العملات الرقمية على فكرة أن لها سقف سوقي، أي أن عملية تشفير بروتوكولات الإنشاء من البداية خلقت عدد محدد من العملات ومع كل عملية فك تشفير - أو تعدين بإضافة معاملة - يقلل عدد المخزون تدريجيًا، وهذا شبيه بفكرة المعادن النفيسة، فمثلا كلما تم استخراج كمية من الذهب قل الاحتياطي المخزون في باطن الأرض. فيصبح من الصعب على المعدنين Miners إنتاج وحدات العملة الرقمية، حتى يتم الوصول إلى الحد الأعلى ويتوقف سك العملة تمامًا.

ولفهم هذا بشكل أبسط، البيتكوين Bitcoin أحد أشهر العملات الرقمية، وأعلىها قيمة حاليا، كعملة رقمية تم تشفيره من البداية على أن يحتوي الكود على 21 مليون قطعة فقط، وبمجرد الإنتهاء من تعدينهم جميعا أو استخراجهم، لن يكون هناك بتكوينات Bitcoins جديدة، أي لن يتم طباعة أموال جديدة كما يحدث في العملات الاعتيادية الأخرى، وهذا يعني أنك لو تمتلك 1 بيتكوين فهذا يعني أنك تمتلك 1/21000000 من إجمالي ثروة العالم من البنكوين.

مزايا العملات الرقمية

فيما يلي نسرد أهم مميزات التعامل بالعملات الرقمية والتي ظهرت مع انتشارها في الفترة الأخيرة

1. محمية من فقدان قيمتها، أو التضخم

التضخم هو آفة اقتصادات العالم، والعديد من العملات الاعتيادية واجهت وتواجه خطر التضخم، لكن فكرة أن العملات الرقمية يتم إنتاجها على أساس تحديد سقف سوقي لها، وكمية محدودة منها، يزيد مع ارتفاع الطلب عليها من قيمتها بما يتواكب مع السوق، ويحميها من التضخم على المدى الطويل

2. التحكم الذاتي والصيانة المستدامة

إدارة وصيانة أي عملة تعتبر من العوامل الرئيسية في تطورها واستدامتها. في العملات الرقمية يتم تخزين المعاملات بواسطة المعدنين Miners في شبكة سلسلة الكتل blockchain على حواسيبهم، ويحصلون في المقابل على العملة نفسها كمكافأة على ذلك. لذلك فإنهم يحتفظون بسجلات المعاملات دقيقة ومحدثة باستمرار، مما يحافظ على سلامة العملة الرقمية وسجلتها لامركزية.

3. الأمان والخصوصية

يمكن القول استنادا لما ذكرناه في مقالنا هنا منذ البداية أنهما كانا الدافع الأساسي لبناء العملات الرقمية من الأساس، لذلك فإن سجلات شبكة بلوك تشين (ar/home/)

(ar/trader/)

(https://www.arabictrader.com/ar/learn/forex-school/304/%D9%85%D9%81%D9%87%D9%88%D9%85-

%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%B3%D9%84%D8%B3%D9%84%D8%A9-

%D8%A7%D9%84%D9%83%D8%AA%D9%84-%D8%A8%D9%84%D9%88%D9%83-

%D8%AA%D8%B4%D9%8A%D9%86-blockchain) تستند في بنائها إلى خوارزميات تشفير مختلفة يصعب فكها أو تحليلها. مما يجعل العملة الرقمية أكثر أمانا من المعاملات الإلكترونية العادية إضافة إلى استخدام أسماء مستعارة أو أرقام حسابات غير مرتبطة بأي مستخدم أو حساب أو بيانات مخزنة يمكن ربطها بملف تعريف، بما يحقق مبدأ الخصوصية.

4. إمكانية صرف العملات بسهولة

من المزايا المهمة جدا، وهي التي أعطت العملات الرقمية قيمة حقيقية وسط التعاملات المادية حيث يمكن استبدالها بالعملات الاعتيادية كقيمة صرف مقابلة، مما يعني أن لكل منها سعر صرف متغير مع العملات العالمية الرئيسية - مثل الدولار الأمريكي USD أو الجنيه الإسترليني GBP أو اليورو EUR أو الين الياباني JPY - الأمر الذي ساعد في انتشارها وفي القبول عليها وطلبها كونها بديل للمعاملات النقدية الاعتيادية، ومكافئة لها في القيمة.

5. اللامركزية

على عكس العملات الاعتيادية أو عملات النقد الإلزامي التي تسيطر عليها الحكومات متمثلة في البنوك المركزية، فإن العملات الرقمية لامركزية بطبيعتها ولا يمكن التحكم فيها أو زيادة عددها أو وقف التعامل بها أو إتاحتها إلا من قبل من يستخدموها ويملكون منها الكمية الأكبر، أو من خلال منظمة إنشائها أو تطويرها قبل طرحها في السوق، الأمر الذي يساعدها على الحفاظ عليها من الاحتكار وحمايتها من تحديد التدفق أو القيمة لضمان استقرارها وخصوصيتها وشفافيتها وأمنها

6. قلة تكلفة التحويلات، وسرعتها

أحد أهم استخدامات العملات الرقمية الرئيسية هو تحويل الأموال، وتكلفة أو رسوم التحويلات من أهم العوامل التي يتم وضعها في الاعتبار للحكم على جودة نظام أو عملية التحويل، في تبادلات العملات الرقمية يتم تقليل رسوم المعاملات التي يدفعها المستخدم إلى مبلغ ضئيل أو ربما تصل إلى صفر وتتم بشكل مباشر بين حسابات المستخدمين وبسرعة. لذلك لسنا في الحاجة إلى أطراف ثالثة، مثل VISA أو SWIFT، للتحقق من المعاملة. وهذا يلغي الحاجة إلى دفع أي رسوم معاملات إضافية، أو انتظار وقت طويل.

عيوب العملات الرقمية

كما لها من مميزات فإن التعامل من خلال العملات الرقمية له بعض من العيوب لا بد من وضعها في الاعتبار قبل التعامل بها أو الاستثمار فيها، وهي كالتالي:

1. بي...هل استخدامها في المعاملات غير القانونية

(ar/höme/)

(ar/trader-pro/)

الأمان والخصوصية المطلقة التي كانتا أهم ما يميزها تصعب على الحكومات تعقب أي مستخدم من خلال عنوان محفظته أو معرفة بياناته وربما نذكر أنه تم استخدام البيتكوين Bitcoin كوسيلة لتبادل الأموال والتمويل في الكثير من الصفقات غير القانونية، كما يستخدم البعض العملات الرقمية لغسيل الأموال التي حصلوا عليها بطريقة غير مشروعة من خلال مسيطر نظرف، لذلك مصدها.

2. فقدان البيانات قد يعني خسائر مالية ضخمة

أراد مطوروا العملات الرقمية إنشاء كود مصدر ب خوارزميات تشفير لا يمكن تعقبها وبروتوكولات مصادقة غير قابلة للاختراق، بهدف جعل حفظ الأموال عبر العملات الرقمية أكثر أماناً وسرية عن النقد التقليدي، ولكن الوجه الآخر لهذا القدر من الخصوصية أنه إذا فقد أي مستخدم المفتاح الخاص بالولوج إلى محفظته الرقمية أو حسابه، فلا يمكن استعادته. ستبقى المحفظة مقفلة على ما فيها من عملات مما يجعلها في حكم المفقودة

3. بعض العملات الرقمية لا يمكن صرفها بالعملات الاعتيادية

الأمر الذي يفقدها ميزة الصرف حيث لا يمكن تداول بعض العملات الرقمية إلا مقابل عملة واحدة أو عملات معينة. مما يؤدي يؤدي ذلك إلى إجبار المستخدم على تحويل هذه العملات الرقمية إلى إحدى العملات الرئيسية، مثل البيتكوين Bitcoin أو الإيثيريوم Ethereum أولاً ثم من خلال بورصات خاصة، ثم إلى العملة التي يريدها. هذا ينطبق فقط على عدد قليل من العملات الرقمية، لذلك قد يتم إضافة رسوم أو عمولات على المعاملات الإضافية في العملية، مما يكلف أموالاً غير ضرورية.

4. الآثار السلبية للتعدين على البيئة

عملية تعدين العملات الرقمية Mining عملية معقدة وتتطلب حواسيب حديثة ومتطورة مما يجعلها كثيفة الاستهلاك للطاقة. حيث لا يمكن عمل ذلك على أجهزة الكمبيوتر العادية. معدنين عملة البيتكوين Bitcoin Miners مثلاً الموجودون في دول مثل الصين التي تستخدم الفحم لإنتاج الكهرباء يؤدي عملهم إلى زيادة البصمة الكربونية للصين بشكل هائل.

5. بورصات تداول العملات الرقمية عرضة للاختراق

على الرغم من أمان وخصوصية العملات الرقمية إلا أن بورصات تداولها ليست آمنة بذاك القدر. تقوم معظم البورصات بتخزين بيانات المحفظة الخاصة بالمستخدمين لتشغيل معرف المستخدم الخاص بهم بشكل صحيح. ويمكن للمتسللين من المخترقين المحترفين التسلل إلى هذه البيانات والوصول إليها وأيضاً سرقة العملات الرقمية المخزنة بها، وقد تم اختراق بعض البورصات، مثل Bitfinex أو Mt Gox، في السنوات الماضية وسرقت وحدات من البيتكوين Bitcoin بألاف بما يعادل ملايين الدولارات الأمريكية. معظم البورصات آمنة للغاية حالياً، ولكن هناك دائماً احتمال حدوث اختراق آخر.

6. لا توجد سياسة استرداد أو إلغاء

التعامل المالي بالعملات الرقمية شأنه شأن التعاملات المالية الأخرى، فإذا كان هناك نزاع بين الأطراف المعنية، أو إذا أرسل شخص ما أموالاً عن طريق الخطأ إلى عنوان محفظة خطأ، فلا يمكن للمرسل (ar/trade) العملات الرقمية المرسلة. وقد يمكن استخدام هذا من قبل العديد من المحتالين لسلب الأموال. نظراً لعدم وجود مبالغ مستردة أو رجوع في العملية، يمكن بسهولة إنشاء معاملة لم يتسلم منتجها أو خدماتها مطلقاً.

سجل الآن
ar/learn/forex-/
g/webinar/41/2023-
(03-14)

التداول في الأسهم والعملات باستخدام موجات إليوت التصحيحية (ar/learn/forex-/
(training/webinar/50/2023-03-16)

أ. محمد
صلاح

أ. محمد صلاح
الخميس 16 مارس 08:30 م

مجانا عبر الانترنت

سجل الآن
ar/learn/forex-/
g/webinar/50/2023-
(03-16)

استراتيجية تداول السلوك السعري (ar/learn/forex-training/webinar/42/2023-03-20/)

أ. رانيا
وجدى

أ. رانيا وجدى
الاثنين 20 مارس 08:30 م

مجانا عبر الانترنت

سجل الآن
ar/learn/forex-/
g/webinar/42/2023-
(03-20)

شاهد المزيد من الندوات والمحاضرات (ar/learn/forex-training/%D9%86%D8%AF%D9%88%D8%A7%D8%AA-/
(%D8%AF%D9%88%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%AA%D8%AF%D8%A7%D9%88%D9%84

(ar/trader-pro/)

ICMarkets-footer.png

[https://pubads.g.doubleclick.net/gampad/clk?](https://pubads.g.doubleclick.net/gampad/clk?(id=5391345024&iu=/21885385154)
(id=5391345024&iu=/21885385154)

vantage-footer.png

[https://pubads.g.doubleclick.net/gampad/clk?](https://pubads.g.doubleclick.net/gampad/clk?(id=5867412936&iu=/21885385154)
(id=5867412936&iu=/21885385154)

exness-logo.png

عروض شركات الفوركس (ar/brokers/forex-brokers/)
(ar/home/)

alpari-footer.png

[https://pubads.g.doubleclick.net/gampad/clk?](https://pubads.g.doubleclick.net/gampad/clk?(id=6234385813&iu=/21885385154)
(id=6234385813&iu=/21885385154)

zenfinex-footer.png

[https://pubads.g.doubleclick.net/gampad/clk?](https://pubads.g.doubleclick.net/gampad/clk?(id=6148254373&iu=/21885385154)
(id=6148254373&iu=/21885385154)

forex-footer.png

https://pubads.g.doubleclick.net/gampad/clk? (id=6212038986&iu=/21885385154/AT-C1P	https://pubads.g.doubleclick.net/gampad/clk? (id=6057049650&iu=/21885385154
xm-footer-logo.png https://pubads.g.doubleclick.net/gampad/clk? (id=5849092940&iu=/21885385154	houseofhorse-footer.png https://pubads.g.doubleclick.net/gampad/clk? (id=5297104262&iu=/21885385154
oneroyal-footer.png https://pubads.g.doubleclick.net/gampad/clk? (id=5969393950&iu=/21885385154	easymarkets-footer.png https://pubads.g.doubleclick.net/gampad/clk? (id=6213796924&iu=/21885385154/AT-C1P

X

القائمة البريدية

إشتراك ✓

إشتراك بالقوائم البريدية

(https://www.linkedin.com/company/ibrahim-ahmed-trading)

عن المتداول العربي (ar/about-us/) جديد المتداول العربي (ar/press-release/) ألبوم الصور (ar/photo-album/)

التوظيف (ar/career/) إتصل بنا (ar/contactus/) أعلن معنا (ar/advertise-with-us) Advertise

تحذير المخاطرة: المتاجرة باستخدام الروافع المالية في أسواق المال ينطوي عليها مخاطر عالية جدًا لا تتناسب مع جميع أنواع المستثمرين. يجب عليك أن تستوعب حجم المخاطرة التي قد تتعرض لها أموالك. جميع ما يطرح في الموقع من آراء وتحليلات وتوصيات ومحتويات هو من باب المعلومات العامة ولا يجب أن يتخذ كأداة لاتخاذ أي قرارات استثمارية بالبيع أو الشراء. الرجاء الاطلاع على تحذير المخاطرة التفصيلي بالضغط هنا (ar/risk_disclosure/).

© 2023 جميع الحقوق محفوظة لموقع المتداول العربي

تحذير المخاطرة واخلء المسؤولية (ar/risk_disclosure/) شروط الاستخدام (ar/privacy-policy-service-terms/)