

ملخص الرسالة

سلسلة الكتل هي تقنية ثورية جديدة تم تطويرها بشكل أساسي للتخلص من أي سلطة مركزية على الشبكة العنكبوتية منذ نشأتها اكتسبت توسعًا سريعًا وتم بواسطتها تطوير تطبيقات لا مركزية جديدة و عملات رقمية. بسبب أمانها الذي يجعل المعاملات غير قابلة للتغيير وأكثر ثقة في بيئة تحافظ على سرية الهوية والتي تجمع بين ثلاث تقنيات رئيسية. المفهوم الأول البنية التحتية للمفتاح العام والتوقيعات الرقمية لإثبات ملكية المعاملات داخل شبكة عامة. تقنية النظر للنظر للاتصال المباشر بين المشاركين دون طرف ثالث. وأخيرًا بروتوكول توافقي يتم فيه التأكد من التوصل إلى اتفاق بين معظم المشاركين في الشبكة. ولكن مع ذلك ، لا يزال لديها العديد من نقاط الضعف والقضايا التي يجب دراستها ومعالجتها. أحد تحديات سلسلة الكتل التي تسبب الكثير من المشكلات الأمنية هو التأخير في الانتشار بين شبكة سلسلة الكتل. في هذه الرسالة ، سيتم اقتراح طريقة جديدة لتعزيز انتشار التأخير وتقليل التحقق من المعاملات على وجه التحديد باستخدام نظام تشفير و توقيع رقمي مختلف.