ما هي التجزئة (الهاش) ؟

التعريف

تشير كلمة التجزئة (أو Hashing) الى عملية انشاء مخرجات ذي حجم ثابت عن طريق مدخلات ذي حجم متغير. يتم ذلك من خلال استخدام الصيغ الرياضية المعروفة باسم دالات التجزئة (يتم تطبيقها كـخوارزميات تجزئة).
على الرغم من أن ليست جميع دالات التجزئة تستخدم التشفير إلا أن ما يسمى بدالات/وظائف تجزئة التشفير هي جوهر العملات الرقمية.

الأستخدامات

-تستخدم اثناء عملية تسجيل الدخول لمطابقة البيانات المدخلة مع البيانات المخزنة في قاعدة البيانات

-التحقق من سلامة الملفات
التحقق من سلامة الملفات والبيانات من أي تعديل أو تغيير

اشهر خوارزميات (SHA)

تحصل على العديد من التحديثات بشكل مستمر للحفاظ على مستوى الأمان وتنشئ الهاش بأطوال مختلفة حسب نوع الهاش, والخوارزمية الاشهر حاليا هي SHA2

plain text (النص):123
SHA256.:a665a45920422f9d417e4867ef
dc4fb8a04a1f3fff1fa07e998e86f7f7a27ae
3

اشهر خوارزميات (MD5)

تنشئ Hashes بطول 128-بت (32 خانة)، لها اصدارات قديمة مثل MD4،MD2 ولكن تم العثور على بعض المشاكل الأمنية فيها

plain text (النص): 123
MD5.:202cb962ac59075b964b07152d23
4b70

الهاش

تركز على سلامة البيانات.

سرعة في الحساب والتحويل وصعوبة في استخراج المعلومات الأصلية.

أي تغيير بسيط في المدخل يغير شكل الهاش تماماً.

من الصعب جدا عكس الخوارزمية لاستخراج المعلومات الأصلية

التشفير

تركز على الحفاظ على سرية البيانات

تتطلب مفتاح خاص لفك الشفرة

تستخدم في حماية البيانات من الوصول الغير مصرح

يمكن استخراج المعلومات المشفرة عن طريق عكس الخوارزميات

الخلاصه

يمكن أن تكون خوارزميات التجزئة متعددة الاستخدامات عند دمجها مع التشفير مما يوفر الأمان والمصادقة بعدة طرق مختلفة. على هذا النحو تعد دالات التجزئة التشفيرية مهمة للغاية بالنسبة لجميع شبكات العملات الرقمية تقريبًا. لذلك فإن فهم خصائصها وآليات عملها مفيد بالتأكيد لأي شخص مهتم بتقنية البلوكشين.

إعداد وتصميم : سلمى المقبل