X16R

ASIC-beständig durch Design

Tron Schwarz und Joel Gewicht

Die Geschichte des Hashings für Kryptowährungen begann mit SHA256 für Bitcoin, dann Scrypt für Litecoin, Ethash für Ethereum, X11 für Dash, gefolgt von X13, X15 und X17. Die X16R ist der nächste Schritt in dieser Entwicklung, um einen besseren Mining-Algorithmus zu finden.

Der Grund für die Algorithmusänderungen ist, die Auswirkungen von speziell entwickelter Hardware auf das Bergbau-Ökosystem der Münze zu minimieren. Bitcoin sollte ursprünglich von Computern überall abgebaut werden. Da der Wert von Bitcoin zunahm, wurde es vorteilhaft, parallel auf Hardware zu minen, die für die parallele Verarbeitung ausgelegt war, so dass das Mining auf Graphics Processing Units (GPUs) umgestellt wurde. Mit zunehmendem wirtschaftlichen Wert des Mining wurde es wirtschaftlich sinnvoll, programmierbare Hardware in Form von Field-programmable Gate Arrays (FPGAs) einzusetzen, die einen Vorteil gegenüber CPUs und GPUs hatten. Der nächste Schritt war die Herstellung von kundenspezifischen Chips, die speziell für den Bergbau entwickelt wurden.
Diese anwendungsspezifischen integrierten Schaltungen (ASICs) konnten die konkurrierenden Technologien dominieren und machten es unpraktisch, andere Wege zu gehen. Die letzte und wahrscheinlich letzte Iteration des Bitcoin-Mining ist der Übergang zu schnellerer und energieeffizienterer ASIC-Hardware.

Der unglückliche Nebeneffekt dieses Übergangs zur ASIC-Hardware ist die Zentralisierung des Mining. Obwohl jeder diese ASICs bestellen kann, hat die Nähe zur Produktionsstätte einen Vorteil, da die Lieferzeit reduziert wird. Darüber hinaus ist der Zugang zu billigem Strom eine Priorität, da der verbrauchte Strom die variablen Kosten des Bergbaubetriebs ist. Dies hat zu einer gewissen Zentralisierung des Bergbaus in China geführt, da die Nähe zur ASIC-Entwicklung und die Verfügbarkeit von preiswertem Strom in einigen Provinzen gegeben ist.

Eine Lösung zur Minimierung der Auswirkungen von ASIC-Minern ist die Verwendung eines speicherintensiven Hashing-Algorithmus. Dies ist der Ansatz von Scrypt, verwendet von Litecoin, und Equihash, verwendet von ZCash. Diese beiden Algorithmen haben die Auswirkungen von ASICs reduziert. Obwohl es einige ASIC Miner für Scrypt gibt, ist der relative Vorteil gegenüber GPUs vernachlässigbar. Es gibt derzeit keine ASIC Miner für Equihash.

Ein weiterer Ansatz ist die Verwendung einer Sequenz von Hashing-Algorithmen, bei denen die Ausgabe von einem zum nächsten wird. Dash, ehemals DarkCoin, ging diesen Weg mit seinem X11-Algorithmus. X11 verwendet elf verkettete Hashing-Algorithmen1, um den Übergang zum ASIC-Mining zu verhindern.

Dieser Ansatz funktionierte eine Weile, aber mehrere Hersteller produzieren nun ASIC Miner für X11. Das Konzept hinter X11 kann auf zusätzliche Algorithmen erweitert werden. Aus diesem Grund verwenden einige Münzen X13, einige X15 und sogar X17,

die siebzehn Hashing-Algorithmen verketten.

---

[1] https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/

Die feste Reihenfolge der Hashing-Algorithmen eignet sich für den Aufbau von ASICs. Während die Verkettung mehrerer Algorithmen zusammen die Schwierigkeit bei der Konstruktion eines ASICs erhöht, verwenden die X13, X15 und X17 alle die gleiche Reihenfolge von Hashing-Algorithmen wie die X11. Dies wird wahrscheinlich zu einer schnelleren Herstellung von ASICs für diese Algorithmen führen, da die Hersteller ihr bestehendes Design nur noch erweitern müssen, um die zusätzlichen Hashing-Algorithmen aufzunehmen.

Der X16R-Algorithmus beabsichtigt, dieses Problem zu lösen, indem er die Reihenfolge der Hashing-Algorithmen ständig unterbricht. Die Hashing-Algorithmen sind die gleichen bewährten Algorithmen, die in X15 + SHA512 verwendet werden, aber die Reihenfolge wird basierend auf dem Hash des vorherigen Blocks geändert.

Diese Neuordnung macht es nicht unmöglich, ein ASIC zu bauen, aber es erfordert, dass sich das ASIC an zusätzliche Eingaben anpasst, was durch eine CPU oder GPU einfacher zu erreichen ist. Die Neuordnung verhindert auch eine einfache Erweiterung der aktuellen X11-ASICs oder zukünftigen X15-ASICs.

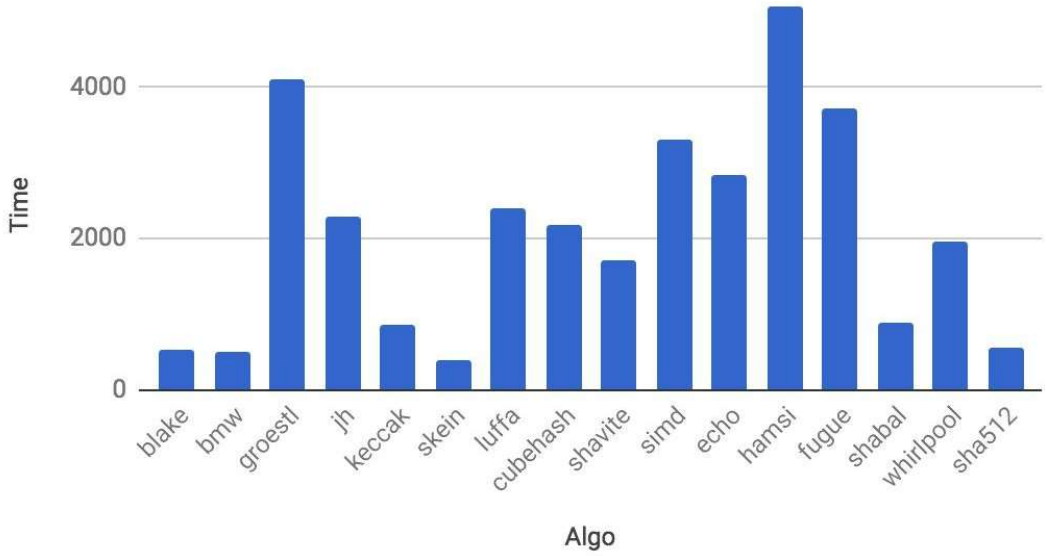
Der X16R-Hash-Algorithmus besteht aus 16 Hash-Algorithmen, die in Kettenform arbeiten, wobei die Reihenfolge von den letzten 8 Bytes (16 Nibbles) des Hash des vorherigen Blocks abhängt. Die Algorithmen sind wie folgt:

0=blake
1=bmw
2=groestl
3=jh
4=keccak
5=skein
6=luffa
7=cubehash
8=shavite
9=simd
A=echo
B=hamsi
C=fugue
D=shabal
E=whirlpool
F=sha512

Beispiel:
Vorheriger Block-Hash:
000000000000000007e8a29f052ac2870045ae3970270f9***7da00919b8e86287***

Die letzten 8 Bytes: **0x7da00919b8e86287**

Jede Hex-Ziffer (Nibble) bestimmt, welcher Algorithmus als nächstes verwendet werden soll.
cubehash -> shabal -> echo -> blake -> blake -> simd -> bmw -> simd -> hamsi -> shavite -> whirlpool -> shavite -> luffa -> groestl -> shavite -> cubehash



Einige der Hash-Algorithmen dauern länger als andere. Dieses Zeitgefälle neigt dazu, über die 16 Algorithmen zu berechnen, während jeder Block abgebaut wird.

Die Testplattform für diesen Mining-Algorithmus ist Raven (RVN). Raven wurde am 3. Januar 2018, dem 9. Jahrestag der Einführung von Bitcoin, gestartet. Raven ändert den Ausgabeplan, die Blockzeit und den Mining-Algorithmus.

Raven ist die Referenzimplementierung für X16R, die die Anzahl der Algorithmen, die verwendeten spezifischen Hashing-Algorithmen, die Reihenfolge der Algorithmen sowie die Reihenfolge der und der verwendeten Bytes aus dem vorherigen Blockhash definiert.

Die Konzepte der X16R könnten um Scrypt, Equihash und andere ASIC-resistente Algorithmen erweitert werden, um es auch weiterhin jedem mit einem ungenutzten Computer zu ermöglichen, mit handelsüblicher Hardware am Mining teilzunehmen. Die Reihenfolge der Algorithmen kann für jede Münze leicht geändert werden, um Hardwarehersteller davon abzuhalten, ASICs für eine ganze Münzklasse wie bei X11 zu bauen.