بیتکۆین: سیستمێکی خەرجکردنی هاوتابەهاوتای ئێلێکترۆنیکی

نووسەر: ساتۆشی ناکامۆتۆ

satoshin@gmx.com

www.bitcoin.org

Übersetzt von Deutsch zum soranischer Kurdisch durch: Ayub Rahmani

پاچڤە لە ئاڵمانییەوە بۆ کوردیسۆرانی لە لایەن: ئەیوب ڕەحمانی

Donation, only BTC: 3MM9P4teD765gFwKceAetQvf4HPUiE7V1a

یارمەتی, تەنیا بۆ بیتکۆینە، سپاس: 3MM9P4teD765gFwKceAetQvf4HPUiE7V1a

کورتەیەک: سیستمێکی خەرجکردنی ئێلێکترۆنیکی بەتەواوی هاوتابەهاوتا (Peer-to-Peer) ئەتوانێت ئەم ئیمکانەمان بۆ دابین بکات کە خەرجکردنی ئانلاین یا ئینتێرنێتیی لە کەسێکەوە ڕاستەوخۆ بۆ کەسێکی دیکە بنێردرێت، بە بێ ئەوەی ڕێکخراوێکی سێهەمی دارایی ناوپشک وەکو بانک لەنێواندا بێت. واژۆ یا مۆرە دیجیتاڵییەکان بەشێک لە چارەسەرییەکەن، ئەمە وادەکات کە وەک جاران ناوەندێکی سێهەمی جێگای بڕوا زەرور نەبێت، ئەمەش ئەبێتە هۆی ئەوەی کە هەزینە یا خەرجی زیاتر بە ناوپشک نەدرێت و ئەمەش لە قازانجی خەڵکە. ئێمە بە مەبەستێ نەهێشتنی خەرجی زیاتر بە تەرەفی سێهەم یا ناوپشک ئەم ڕێگاچارە پێشنیاز دەکەین، لەوەی کە ئێمە کەڵک لە سیستمی هاوتابەهاوتا وەردەگرین. تۆڕی گشتیی (Network) مۆری زەمەنی لە دانەبەدانەی حەواڵە و ڕەدووبەدەڵەکان (Transactions) دەدات، لەوەی کە ئەم حەواڵانە بەشێوەی زنجیرێکی بەردەوام کە واژۆی هاشیان (Hash) لێدەدات لە شێوەی سەلماندنی کارکرد (Proof-0f-Work) و بەمشێوە حیساباتێک پێکدێنێت کە پاش تەواوبوون بە هیچ کلۆجێک و هیچکەس ناتوانێت دەسکارییان بکات، مەگەر ئەوەی کە سەلماندنی کارکرد لە خاڵی سفرەوە دەسپێبکرێتەوە. هەرچی ئەم زنجیرە هاشانە درێژتر ببنەوە، نەک هەر بوونی یەکتر ئەسەلمێنن، بەڵکوو بەڵگەشن بۆ ئەوەی کە ئەمانە حەوزێکی ئێجگار مەزنن لە کارکردی سی پی یووە کۆمپیوتریەکان (CPU). هەتا ئەوکاتەی کە زۆرترین بەشی کارکردی سی پی یووەکان لە ڕێگای ماینەرەکانەوە کۆنترۆڵ بکرێن، کە ڕێگە نادەن تۆڕی گشتی هێرشی هەکریی بکرێتە سەر، بەمجۆرە درێژترین زنجیرەی ئێلێکترۆنیکیش پێکدێنن و خێراتریش پەرچەکرداریان دەبێت لە ئاست هەکرەکاندا. خۆی تۆڕی گشتیی پێویستی بە چوارچێوەیەکی کەم و سنووردارە. هەواڵە ئێلێکترۆنیکییەکان لەسەر بنەمای چاکترین هەوڵ یا هیممەت (Best-Effort-Basis) ڕەوانە دەکرێن، وە ماینەرەکان ئەتوانن تۆڕی گشتیی بەدڵی خۆیان بەجێبێڵن و هەمدیسانیش بێنەوە جێگای خۆیان، لەبەر ئەوەی کە درێژترین زنجیری سەلماندنی کارکرد، وەکوو بەڵگە نیشانمان دەدەن کە لەوکاتەدا کە ئەم ماینێرانە لەجێی خۆیاندا نەمابوون، چ ڕوویداوە، واتە هیچ کردارێک لەم زنجیرەدا ون و بزر نابێت و نافەوتێت.

١ پێناسە (Introduction)

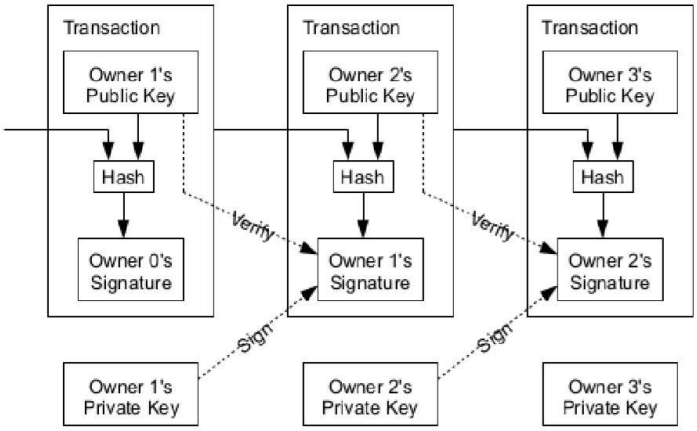
بۆماندەرکەوت کە مەعامەلە لەڕێگای ئینتێرنێتەوە ئیتر بە قایمی لەسەر ئەم بنەمایە ئەڕواتە پێش کە شەبەکە دارایییەکان (و: بانک، دەڵاڵ و هتاد) وەکوو تەرەفێکی سێهەمی ناوپشکی جێگای بڕوا عەمەل دەکەن، بۆ ئەوەی بتوانرێت مەعامەلە یا حەواڵە ئێلێکترۆنیکییەکان بەڕێوە ببردرێن. لەکاتێکدا کە ئەم سیستمە بۆ زۆربەی حەواڵە ئێلێکترۆنیکییەکان زۆر بە باشی کار دەکەن، بەڵام لەهەمانکاتدا تووشی نووقسان و زەعفێکی مەزنن، ئەویش ئەمەیە کە لەسەر بنەمای متمانە و ئیعتیماد

دامەزراون و کاردەکەن. ئەوجار لەکاتی هەڵوەشانەوەی مەعامەلەیەکدا و گێڕاندنەوەی پارەکە لە فرۆشەرەوە بۆ کڕیار یا بکڕ، بەتەواویی و بەساکاریی موومکین نابێت، لەبەر ئەوەی کە ناوەندە داراییەکان ناتوانن لە کاتی دەعوا یا مەرافعەیەکدا بەخۆڕایی ناوبژیوان بن. نرخی ناوبژیوانیی، ڕاستەوخۆ کەمەنرخی مەعامەلەیەک دەباتە سەر و ئیمکانی حەواڵە و ڕەدوبەدەڵێکی ئێلێکترۆنیکی هەرزان ناهێڵێت. خەرجێکی قوورس لە مەعامەلە کلاسیکییەکاندا ئەوکاتە ڕووەدات کە ئەم ئیمکانە لەئارادا نەبێت کە بتوانرێت نرخێکی گێڕدراوە لە فرۆشەرەوە بۆ بکڕ، بەساکاریی و بەبێ ناوپشک بێتە ئاراوە، چوونکە ناوپشک لەهەردوو سەرەوە، هەم کاتی حەواڵە بۆ فرۆشیار و هەم کاتی گێڕاندنەوەی پارە بۆ بکڕ، دووجار بایی حەواڵە دەگێڕێتەوە بۆ خۆی، بۆ ئەو ناوپشکییەی کە دەیکات. گێڕاندنەوەی پارە و حەواڵەکردنەوەی بۆ بکڕ، زەروورەتی بوونی ناوەندێکی جێگای متمانە ئەباتە سەر. بازرگان و فرۆشیارە ئێلێکترۆنیکییەکان (و: وەک Amazon و Wish وZalando بۆ نمونە) ناچارن لەبەر ئیحتیاتی خۆیان بێ متمانە بن بە مووشتەرییەکانیان کە لەهەموو جیهانەوە شتیان لێدەکڕن، وە بۆ ئەم مەبەستەش ناچارن داوای بەڵگەی پێناسەی دیجیتاڵییان لێبکەن، بەڵگەگەلێک کە لە مەعامەلەیەکی ئاسایدا پێویست نین نیشان فرۆشیار بدرێن. بەمحاڵەش لە تەجارەتە ئێلێکترۆنیکییەکاندا کەمەکێک کلاوچییەتی هەردەم هەر لەئارادا دەبێت. ئەم نرخ و بەهایانەی کە لە تەجارەتی ئێلێکترۆنیکیدا جاروبار ڕووەدەن لە مەعامەلەیەکی ڕووەڕووی فیزیکی ئاسایدا و بەپوڵی کاغەزیی ڕوونادەن. کەواتە هیچ میکانیزمێکی دیکە بۆ بەڕێوەبردنی کاروکاسپییەکی ئێلێکترۆنیکی بە بێ بوونی ناوەندێکی دارایی ناوپشک و جێگای متمانە بوونی نییە.

زەروورەتی سیستمێکی ئێلێکترۆنیکی کە لەسەر بنەمای سەلماندنێکی کریپتۆگرافیی، بەجێگای متمانەپێکردن، دامەزرابێت لەم سەردەمەدا لەئارادایە کە هاوکات ئیمکانێک بۆ هەردوو لایەنی مەعامەلەیەک واتە فرۆشەر و کڕیار یا بکڕ ئامادە بکات کە حەواڵەکانیان ڕاستەوخۆ لەنێوان خۆیاندا و بەبێ بوونی ناوەندێکی ناوپشکی جێگای متمانە، بەڕێوە ببەن. حەواڵەگەلێک کە لەواندا پاش ڕەوانە کردنی لە لایەن بکڕەوە بۆ فرۆشیار، لەڕووی حیسابوکیتابگەلێکی ئێلێکترۆنیکییەوە، ئیتر ئیمکانی نییە بکڕ بە بێ ڕەزامەندیی فرۆشیار پارەکە بۆخۆی بگێڕێتەوە، ئەمە فرۆشیارەکان لە ئاست کلاوچییەتی موشتەرییەکاندا ئەپارێزێت و میکانیزمی بازرگانییە ستانداردکراوەکان ئەتوانن بە ساکارترین و هەرزانترین شێوە بەڕێوە ببردرێن، (و: بە بێ بوونی بانک) مافەکانی کڕیار و فرۆشیار بپارێزن. ئێمە لەم سپینامەدا چارەسەرییەک پێشکەش دەکەین بۆ ئەوەی کێشەی دووجار پارەی حەواڵە (Double-Spending-Problem) نەهێڵین، کە لەژێر بەکارهێنانی سێرڤێرێکی واڕۆزەمەنی پەرەپێدراوی هاوتابەهاوتا، وە سەلماندنێکی حیسابوکراوی کرۆنۆلۆژیی (و: واتە بە سەرەی زەمەنیی) حەواڵە یا تڕانسئەکشنەکان ئەخوولقێنن. ئەم سیستمە تەواو دڵنیا و موتمەئینە، تا ئەوکاتەی کە ماینەرەکان زیاتر و زیاتر کارکردی سی پی یووەکان کۆنترۆڵ بکەن و ببنە کۆمەلێک لە گرێدراوە هاوئاهەنگەکان.

٢ حەواڵەکان (Transactions)

ئێمە پارەی ئێلێکترۆنیکی (و: واتە کۆین Coin) وەک زنجیرە واژۆیەکی دیجیتاڵی پێناسە دەکەین. هەرکەس کە خاوەنی ئەم پارە دیجیتاڵییە بێت ئەتوانێت کۆینەکەی بۆ کەسێکی دیکە (و: یا فرۆشیارێک) حەواڵە بکات، بەجۆرێک کە ئەو لەگەڵ هەر حەواڵەیەک، هاشێک (Hash) لە حەواڵەی پێش خۆی، وە هەروەها کلیلێکی دیجیتاڵی ئاشکرا (و: ڕووبەدەرەوە و غەیرە نهێنی) خاوەنی حەواڵەی دووای خۆی بە شێوەی دیجیتاڵی واژۆ دەکات و ئەمەش بە کۆتایی کۆینەکەی خۆیدا ئەلکێت. وەرگری حەواڵەکە ئەتوانێت واژۆکە بناسێت وەیا تەئیدی بکات و هەڵیسەنگێنێت، وە بەمشێوە زنجیرەکەی خاوەن کۆینی پێش خۆی تەئید بکات. (و: دیارە ئەم واژۆیانە هەموویان لە ناو تۆڕی گشتیدا بەشێوەی ئاوتۆماتیک ڕووەدەن و خاوەن کۆین و خاوەن حەواڵە و کڕیار و فرۆشیارەکان ئەم ئاڵۆزیانە نابینن، ئەوان تەنیا دوو کلیلی ئاشکرایان بەدەستەوەیە، کڕیار کۆین بۆ کلیلی فرۆشیار ئەنێرێت و تەواو، باقی حیساباتی ئاڵۆزی پشت قەزییەکە ئوتوماتیک بەڕێوە دەچن!) بڕوانە وێنەی ژمارە یەک



گرفت لێرەدا ئەمەیە ئەو کەسەی کە حەواڵەکە وەردەگرێت ناتوانێت تەئیدی بکات کە یەک لە خاوەن کۆینە پێشووەکان دووجار یا دەبڵ پارەیان نەدابێت. یەک لە چارەسەرییە پێویستەکان بۆ ئەم کێشە ئەمەیە ناوەندێکی جێگای متمانە یاخود زەڕابخانەیەکی چاپی ئەسکەناس بکرێتە بەرپرسی ئەم ئەرکە بۆ تاقیکاری و هەر دەبڵ حەواڵەیەک بناسێتەوە. پاش هەر حەواڵەیک پێویستە ئەسکەناسەکان بدرێنەوە بە زەڕابخانەکە، لەبەر ئەوەی کە ئەویش بتوانێت پارە یا ئەسکەناسی نوێ بداتەوە دەرەوە، وە تەنیا ئەو ئەسکەناسانەی کە ڕاستەوخۆ لەم زەڕابخانە بڕواپێکراوەوە چاپ دەکرێن متمانەیان پێبدرێت و بزاندرێت کە لە ئاستێکی دروستدا چاپکراون و دەبڵ چاپ نەکراون! کێشەی ئەم چارەسەرییەش لەمەدایە کە چارەنووسی سەرتاپای سیستمی ئەسکەناس و پارە بەو ناوەندوە گرێدەدرێتەوە کە ئەسکەناس لەچاپ دەدات، وە هەر حەواڵەیەک بەناچار ئەبێت تەنیا لەڕێگای ئەوەوە و لەژێر چاودێریی ئەودا بەڕێوە بچێت، هەر ڕێک وەکوو کاروباری بانکێک.

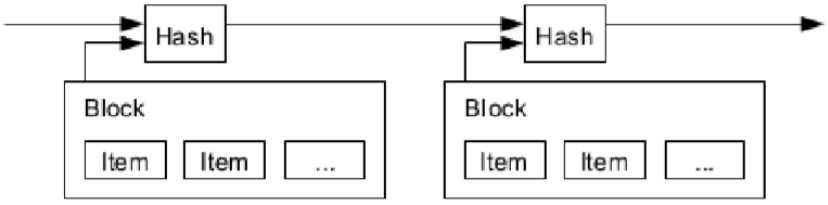
ئێمە (و: لەم سەردەمەدا) پێویستمان بە مێتۆدێکە دڵنیایی بدات بەو کەسەی کە حەواڵە وەردەگرێت، بۆ ئەوەی دڵنیا بێت لەمەی کە خاوەن ئەسکەناسە پێشووەکە حەواڵە پێشووترەکانیان واژۆ (و: واژۆ یا تەئیدی دیجیتاڵی مەبەستە!) کردبێت. بۆ مەبەستەکەی ئێمە، یەکەمین حەواڵە، ئەو حەواڵەیە کە بژێردراوە و لەوێوە هەر هەموو حەواڵەکانی دیکە وەک سلسلە و لەسەر ڕەقەم دەستییانپێکردووە، بەجۆرێک کە ئێمە ئیتر هیچ خەممان نەبێت و دڵنیا بین لەمەی کە پارە لەمە زیاتر و دەبڵ چاپ نابێت. (و: واتە دەوڵەت یا بانکی ناوەندیی یا زەڕابخانە لە خۆڕا بە گۆترە ئەسکەناس چاپ نەکات، ئەوەی کە هەر ئێستاکە لە هەر هەموو جیهان باوە و لەخۆڕا ئەسکەناسی بێ پشتیوان لە لایەن دەوڵەتان و بانکە ناوەندییەکان لە چاپ دەدرێت و نرخی پارەی کاغەزیی یا ئەسکەناسی وڵاتان بەردەوام ئەشکێت و وڵاتانیان تووشی تەوەڕووم کردووە!)

تاقە ئیمکانی ئەمەی کە بتوانین ڕاستی و ئەسڵ بوونی حەواڵەیەک بناسینەوە ئەمەیە کە ئێمە هەر هەموو حەواڵەکان بناسین. لەو مۆدێل و نمونەی پێشوودا کە باسیکرا و لەوێ زەڕابخانەکە حەواڵە کۆنەکانی دەناسیی و ئەیتووانی بڕیار بدات و پێمان بڵێت، کام حەواڵە سەرەتا بۆ کوێ چووە. بۆ ئەوەی ئێمە هەر ئەم ئەرکە بەبێ پێویست بوون بە لایەنێکی سێهەمی ناوپشک و بڕواپێکراو یا جێمتمانە بەڕێوە ببەین، پێویستە حەواڵەکان شەفاف و ڕووبەدەرەوە بەڕێوە ببردرێن و نەک بە نهێنی [١]، وە ئێمە لەمکاتەدا پێویستمان بە سیستەمێکە کە لەودا بەشداربووانی ئەم حەواڵانە یەکبکەون لەسەر تاقە یەک زنجیرە حەواڵەی پێکەوە گرێدراو و هەر ئەم تاقە زنجیرەش موعتەبەر بێت. حەواڵە وەرگر پێویستی بە بەڵگەیەکە کە لەودا لەکاتی هەر حەواڵەیەکدا کە جێگە بە جێگە بووە، زۆرینەی ماینێرەکانی ناو تۆرە گشتییەکە پەیوەندییان پێکەوە هەبێت و (و: وەک پێچومۆرە) بە یەکتر بخۆن، وە گرێ سەرەتایی و حەواڵە سەرەتاییەکان ڕوون و دیار بن و ناسراو بن.

٣ سێرڤێری مۆری زەمەنی (Timestamp-Server)

ئەم ڕێگاچارەی کە لە لایەن ئێمەوە پێشنیاز دەکرێت لە تاقە یەک سێرڤێر بە مۆری زەمەنییەیەوە دەسپێدەکات. سێرڤێرێک بە مۆری زەمەنی بەمجۆرە کار ئەکات کە هاشی بلۆکێک کە مۆری زەمەنی کراوە و لەشێوەی فایلێکدا خوولقاوە و ئەوهاشەش بۆنمونە لە ڕۆژنامەیەکی بەناوبانگدا یاخود لە پۆستێکی بەکارهێنراوی ناو شەبەکەیەک (Usenet-Post) بەڕای گشتی ڕادەگەیەندرێت، کە هەموو بیناسن [٥-٢]. ئەم مۆرەزەمەنییە بەڵگەیەکە و ئەیسەلمێنێت کە فایلەکان لە چ

کات و زەمەنێکدا خوولقێندراون و بوونیان هەیە، بە ئاشکرا و شەفاف، چوون ئەگەر ئاوەها نەبووبایە ئیتر هیچ هاشێک لەوان بوونی نەدەبوو. هەر مۆرێکی زەمەنیی هاشێکی بلۆکی پێشخۆی و هاشی بلۆکی دووایخۆی پێوەیە و ئەم کۆمەڵە هاش و بلۆکە تێکترینجاوانە پێکەوە زنجیرە بلۆکێک پێکدێنن (و: BlockChain)، بەجۆرێک کە لەم زنجیرە بلۆکەدا هەر بلۆکێک کە زیاد دەبێت، بلۆکی پێشخۆی و سەرجەم بلۆکەکانی تریش بەهێزتر دەکات و کاری هەککرانی تەقریبەن ناموومکین دەکات.

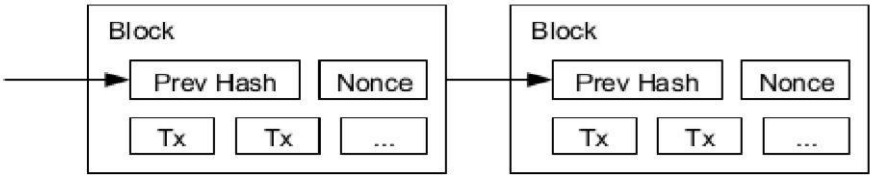


٤ سەلماندنی کارکرد (Proof-of-Work)

بۆ ئەوەی ئێمە بتوانین سێرڤێرێکی پەرەپێدراوی واژۆزەمەنی کە لەسەر بنەمای هاوتابەهاوتا (Peer-to-Peer-Basis) کاردەکات بەکاربێنین، پێویستە ئێمە کەڵک لە سیستمی سەلماندنی کارکرد (Proof-of-Work-System) وەربگرین، ڕێک وەکوو سیستمی هاشکەش (Hashcash-Systems) کە ئادام بەک (Adam Back) دایمەزراندبوو [٦]، ئەمەش بەجێگای کەڵکوەرگرتن لە ڕۆژنامە یاخود یوزنێت پۆست (Usenet-Posts)، (و: لە سەرەوە باسیکرا).

سیستمی سەلماندنی کارکرد بەمشێوەیە کە بەدووای ئەرزشێکدا ئەگەڕێت کە لەودا، ئەوکاتەی کە هاش دەکرێت، بۆنمونە لەڕێگای شا-٢٥٦-ەوە (SHA-256)، کە هاشەکە بە کۆمەڵە ژمارەیەک لە سفربایتەوە (Zero bits) دەسپێدەکاتن. حەدیناوەڕاستی ئەو ئەرکەی کە پێویستە بەڕێوە ببردرێت پەیوەندییەکی ئێکسپۆنێنتییەلی هەیە لەگەڵ ئەو بڕە ژمارە سفربایتە پێویستانە و ئەتوانێت تەنیا لەڕێگای ئیجراکردنی تاقە هاشێک تەئید بکرێت و بلۆکەکەی خۆی تەکمیل بکات.

ئێمە بۆ تۆڕ یا شەبەکە گشتییە واژۆزەمەنییەکەمان کەڵک لە ئیسپاتی کارکرد وەردەگرین، بەجۆرێک کە لەودا نۆنسێک (Nonce بڕوانە وێنەی خوارەوە) لەناو بلۆکی خۆیدا تا ئەو ئاستە ئەڕواتە پێش کە ئەرزشێک (و: لێرە حەلی مەسەلەیەکی ئالۆزی لۆگاریتمی) ئەبینێتەوە، کە لەودا ئەو سفربایتەی بۆ تەکمیلی هاشی بلۆکێک پێویستە-مان بۆ حەل ئەکات و ولامەکەی ئەدۆزێتەوە. پاش ئەوەی کە سی پی یووی کۆمپیوتەرەکە بە حەدی کافی کار و بەرقی مەسرەف کرد، بۆ ئەوەی پرۆسەی سەلماندنی کارکرد بە سەرئەنجام بگەیەنێت، ئیتر ئەم بلۆکە بە هیچ کلۆجێک قابیلی ئالۆگۆڕپێکردن نامێنێت و تازە ئیتر هیچکەس ناتوانێت دەستێوەردات یا بیگۆڕێت، مەگەر ئەوەی کە گشت کارەکان هەر لەسەرەتا و لە خاڵی سفرەوە دەسپێبکرێنەوە. (و: کە ئەویش ئەبێتە هۆی پێکهێنانی زنجیرە بلۆکێکی جیاواز لەمەی کە تا ئیستا پێکهاتووە، چوون حیسابە لۆگاریتمییەکان، هەردەم دەقاودەق وەکوو جاری پێشوو دووپاتە نابنەوە و ئالۆووگۆڕی گەورە دروووست دەبێت!) لەبەر ئەوەی کە بلۆکەکانی دوواتر هەموو لەگەڵ ئەمانەی ئێستا پێوەی و زنجیرەوار وەسڵ دەبن، ئەگەر لە هەر بلۆکێکدا بەهەرهۆیەک ئالۆووگۆڕێک پێکبهێندرێت، ئیتر هەموو بلۆکەکانی دوواتریش لێرە بەدووواوە ئالۆووگۆڕیان تێدا پێکدێت و ئیتر ئەم زنجیرە بلۆکە، زنجیرە بلۆکێکی نوێیە و پەیوەندیی بە بلۆکە پێشووترەکانەوە، ئەوانەی پێش ئالۆووگۆڕەکە هەبوو، نامێنێت. (و: بەم پێکهاتنی زنجیرە بلۆکە نوێیە، کە ئینشیعابێکە لە زنجیری ئەسڵی، لە زمانی کرپێتۆکارێنسی و کرپێتۆگرافیدا دەڵێین فۆرک، وە هەرکات فۆرکێک لە پووڵێکی دیجیتاڵیدا پێک بێت، ئیتر پوڵێکی نوێ دروووست دەبێت، بۆ نمونە بیتکۆین (BTC) لە یەکی مانگی ئاوگووستی ٢٠١٧-دا هارددفۆرکێکی لێ دروووستبوو کە ناوی نرا بیتکۆینکەش (BCC یا BCH) و پاشان لە ٢٥ی ئۆکتۆبەری هەمانسالّ دیسان هارددفۆرکێکی دیکە و ئەمجارە بیتکۆین گۆلّد (BTG) لەدایک بوو و دووواتریش بیتکۆین پریڤات (BTCP) پەیدا بوو!)



سەلماندنی کارکرد هاوکات ئەم گرفتەش چارەسەر ئەکات کە لە کاتی ئەوەدا کە بڕیارگەلێکی زۆر لە ئارادان، نوێنەرەکان بڕیار بدەن. ئەگەر زۆرینە لە دەنگداندا هەرکەسە و تەنیا یەک ئادرەسی ئای پی (IP-Adresse) هەبووبایە، ئەمە ئەتوانرا لەلایەن هەر کەسێکەوە کە بتوانێت ئای پی گەلێکی زۆر بۆخۆی ڕێزێرف بکاتن، نفووزێ تێبکرێت. سیستمی پرووف ئاف وۆرک لە ئەساسدا بەواتای هەر یو پی سی و یەک دەنگە (و: واتە هەر کامپیوتەرێک یەک دەنگی هەیە!). زۆرترین بڕیار نوێنەرایەتی درێژترین زنجیرە بلۆک دەکات، کە لەودا زیاترین هەزینەی ئیسباتی کارکرد سەرمایەگووزاری کرابێت. ئەگەر زۆرینەیەکی هێز یا قودرەتی سی پی یووەکان لەلایەن ماینێرە سادقەکانەوە کۆنترۆڵ بکرێت، ئەوجار زنجیرێکی سادق و سەرڕاست بەخێرایی گەورە ئەبێتەوە و پەرە ئەستێنێت و هەر هەموو ئەو زنجیرە بلۆکانەی دیکە کە ڕەقابەتی لەگەڵ دەکەن بەجێ بێڵێت و پێشێیان کەوێتەوە! بۆ ئەوەی بلۆکێکی پێشووتر بگۆڕدرێت یاخود دەسکاریی بکرێت، پێویستە هێرشکەر یا هەکر پرووف ئاف وۆرکی بلۆکە پێشووترەکان وە هەروەها هەر هەموو بلۆکەکانی پاش ئەو بلۆکەش کە بەتەمایە دەسکاری بکات (و: یا دزیی لێبکات) سەرلەنوێ دروست بکاتەوە، ئەوجار گرێ ڕاستەقینەکان بدۆزێتەوە و داخلی بلۆکە نوێکانی بکاتەوە و ئەوجار ڕەدیفیان بکاتەوە. ئێمە دوواتر نیشانی دەدەین و ئەیسەلمێنین کە هەتا زنجیرە بلۆکەکان زیاتر و درێژتر دەبنەوە، هەر بەو ڕادەش تووانایی هێرشبەر (و: هەکر) کەمتر و خێراییەکەی ئێکسپۆنێنتییەل هێواشتر ئەبێتەوە.

بۆ ئەوەی هێزی هارڈوێرِی یا کۆمپیوتریی و هاوکات بە پێی کات (و: بە پێی چوونەسەرەوەی نرخ و ناسرانی زیاتری بلۆکچاین و لەمباسەدا بیتکۆین بۆ نمونە) چوونەسەرەوەی ئینترێسە و ئەلاقەی خەڵکانێکی زیاتر بە باسەکە، بۆ ئەوەی بتوانرێت ماینێرەکان لەحاڵی کارکردندا، هاوسەنگ بکرێن، دژواریی ئیسباتی کارکرد یا هەمان پرووف ئاف وۆرکیش قوورستر دەبێتەوە و لە ڕێگای ئەرزشێکی حەدی ناوەڕاستی بازنەییەوە هەموجارێک دیاری ئەکرێت خەڵاتی بلۆکە نوێکان بەکام ماینڕ بدرێت کە ئەویش هەر یەک کاتژمێر جارێک تیعدادێکی حەدی ناوەڕاست لە ماینێرەکان ئەکاتە نیشانە و هەڵیان ئەبژێرێت. هەتا بلۆکەکان خێراتر بخووڵقێندرێن، بەو ڕادەش پێکهێنانی بلۆکی نوێ دژوارتر ئەبێتەوە.

٥ شەبەکە یا تۆڕی گشتیی (Network)

هەنگاوەکان بۆ خستنەکاری تۆڕی گشتیی بەمشێوەیەی خوارەوەن:

١ نوسخەیەک لە حەواڵە نوێکان بۆ هەر هەموو ماینێرەکان دەنێردرێت.

٢ هەر ماینێرێک حەواڵە نوێکان لە یەک بلۆکدا کۆدەکاتەوە.

٣ هەر ماینێرێک کار لەسەر ئەمە دەکات کە سەلماندنی کارکردێکی دژوار بۆ بلۆکەکەی خۆی بدۆزێتەوە.

٤ ئەگەر ماینێرێک سەلماندنی کارکردێک بدۆزێتەوە، ئەوجار نوسخەیەک لە بلۆکەکە بۆ هەموو ماینێرەکانیتر ئەنێرێت.

٥ ماینێرەکان تەنیا ئەوکاتە بلۆکەکە قەبووڵ ئەکەن کە نوسخەکانی هەر هەموو حەواڵەکان لەناو ئەودا موعتەبەر بن، (و: تەقەلوب، تەزویر یا هەڵە نەبن!) وە هێشتا تەوزیع نەکرابێتن.

٦ ماینێرەکان تەئیدی دەکەن کە بلۆکەکەیان قەبووڵکردووە و هاوکات کاریش لەسەر ئەمە دەکەن بلۆکی بەعدیی لە زنجیرەکەدا پێکبێنن. بۆ ئەم مەبەستەش هاشی ئەم بلۆکەی کە ئێستا قەبووڵیانکردووە ئیتر وەک هاشێکی دروستکراوی ڕابردوو بەکاردێنن بۆ لکاندنی بە بلۆکی نوێوە کە بڕیارە ئەویش ئەم پرۆسەی بەسەردا تێپەڕێنن و زنجیرەبلۆکە موعتەبەرەکان پێکبێنن.

ماینێڕەکان هەردەم وایدادەنێن کە درێژترین زنجیرەکەیان درووستترین و بێ هەڵەترینە و هەردەم کار لەسەر ئەمە دەکەن ئەم زنجیرە درێژتر بکەنەوە. ئەگەر دوو ماینێڕ هاوکات دوو فۆرژن یا دوو نووسخەی جیاواز لە بلۆکی دووای خۆیان بدەنە دەرەوە، هەندێک لە ماینێڕەکان ئەتوانن سەرەتا ئەم بلۆک و باقییەکەشیان ئەو بلۆکیتر وەربگرن. لەم حاڵەتەدا هەموو ماینێڕەکان کار لەسەر ئەو بلۆکە دەکەن کە سەرەتا وەرگیراوە، بەڵام بۆ مەبادا بلۆکەکەی دیکەش هەر زەخیرە یا خەزن دەکەن بەم مەبەستەی کە ڕەنگە بتوانن بەویدیکەیان زنجیرێکی درێژتر پێکبێنن. یەک لەم دوو بلۆکە ئەوکاتە تێکدەشکێنترێت کە سەلماندنی کارکردیان ئەدۆزرێتەوە (و: دیارە ئەم پرۆسە بە حەلی فورمولە لۆگاریتمییەکان جێبەجێدەکرێت!) و یەک لە زنجیرەکان درێژتر دەردەکەوێت، ئەوجار هەموو ئەو ماینێڕانەش کە بەرەو شاخە لادەرەکە چووبوون دێنەوە سەر ئەم یەکە و ئەویدیکە تێکدەدەن.

مەرج نییە نوسخەی حەواڵە نوێکان بیلئیجبار بۆ هەر هەموو ماینێڕەکان بچن. تا ئەوکاتەی کە نوسخەکان بتوانن خۆیان بە زۆرترین ماینێڕەکان بگەیەنن، ئەوان زوو یا درەنگ لە یەک بلۆکی نوێدا لەناو زنجیرە بلۆکەکان دەردەکەون یا بابڵەین پێکەوە بلۆکێکی نوێ پێکدێنن. لەناو سەرجەم سیستمەکەدا کەمەکێک تۆلێرانس و چاوپۆشیکردن بەدیی دەکرێت. (و: لەجۆرێک دێموکڕاسی ئەچێت، وانییە کە هەموو شتێک پێویست بێت دەقاودەق بەڕێوە بچێت، تەنیا گرنگە زۆرینەیەک لە ماینێڕەکان بلۆکێکی نوێ تەئید بکەن، ئیتر ئەم بلۆکە بە زنجیرە بلۆکەکان زیاد دەبێت و ئەمێنێتەوە!) ئەگەر بێت و ماینێڕێک ئەو بلۆکەی کە بۆی ئەچێت نەدۆزێتەوە، یا واژۆکەی ئەو لەلایەن بلۆکەکەوە وەرنەگیرێت، هەر کە بلۆکێکی مناسبی دیکە دۆزراوە و لەوێ جێگیر بوو، قۆناخەکە کۆتایی پێدێت و بەدوواداگەڕان ڕادەوەستێنێت!

٦ هاندەر (Incentive)

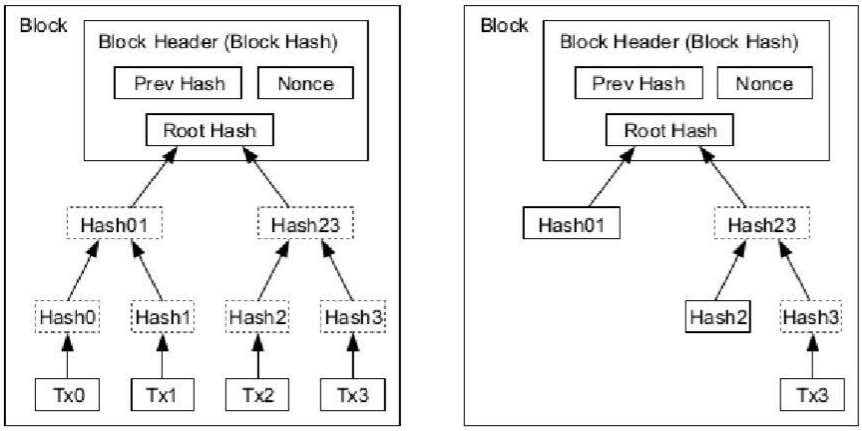
بەپێی بەرنامەی دارێژراو یەکەمین حەواڵە لە بلۆکێکدا حەواڵەیەکی تایبەتە، چوونکە یەکەمین (Coin) یا پارەی نوێی پێ ئەخوولقێت، کە ئەویش ئاسایی هی ئەوکەسەیە کە یەکەم بلۆک پێکدێنێت. ئەم یەکەم بلۆکە هاندەرە یاخود ئەنگیزە دەدات بەو مانێڕانە کە تۆڕی گشتیی بپارێزن و ڕێگایەک ئەخاتە بەردەمیان کە پارەی دیجیتاڵی لەناو شەبەکەدا پێکبێنن بێئەوەی ناوەندێکی ناوپشک بوونی هەبێت. پێزیادبوونی بەردەوامی کۆین یا پارەی نوێ وەکوو ئەمە وایە کە زێر لەناو دڵی خاکدا بدۆزینەوە یا هەڵیبکەنین، وە ئەمەش هەرچی زیاتر هاندەر ئەبێت کە پارەی زیاتر درووستبکەین. مەعدەنچی زێڕ، بە هەڵکەندنی مەعدەن زێر پەیدا دەکات، لە بابەت ئێمەوە، سی پی یووەکان بە حەلی مەسئەلە بیرکارییەکان و مەسرەفی بەرق ئەم کارە بەڕێوە دەبەن و بوونی کۆین موومکین دەکەن.

هاوکات داهاتی ڕەدوبەدەڵی حەواڵەکانیش ئەکرێت مینەڕەکانی ئەم کۆینە هانبدات بۆ بەردەوامبوون لە درووستکردنی. ئەگەر داهاتی حەواڵەکان کەمتر بێت لە تێچوویان، ئەمە ئەنگیزەی مینەرەکان بۆ بەردەوامبوون دێنێتەخوار، لەمحاڵەتەدا ئەبێ نرخی بلۆکەکان ببردرێتەسەر بۆ ئەوەی جیاوازییەکە داپۆشێنێت. ئەگەر جارێک ژمارەیەکی لەپێشدا دیاریکراو لە کۆینەکان بخرێنە بازاڕ، ئەوجار تەنیا داهاتی حەواڵەکان ئەتوانێت داهاتی مینەرەکان دابین بکات و ئەوان ئەتوانن پشت بەم داهاتە ببەستن و بەمشێوە لە تەوەڕووم دوور ئەمێنینەوە.

ئەنگیزەی بەردەوامبوون لەکار بە بێ پچڕان ئەتوانێت یارمەتیدەر بێت بۆ ئەوەی ماینێڕەکان بە دروستی و بێ هەڵە کاریخۆیان بکەن. ئەگەر بێتو هێرشبەرێکی تەماحکار بتوانێت، بەتەنیایی لە هەموو ماینێڕەکانی دیکە زیاتر سی پی یوو بەکار بێنێت، ئەو دەبێت بڕیار بدات و هەڵبژێرێت، ئایا ئەو ئەم هەموو سی پی یووە بەهێزە بەکار دێنێت کە کڵاو بکاتە سەر مرۆڤەکان، لەوەی کە ئەو پارەی زیاتر بۆخۆی دروست ئەکات یا ئەو ئەم پارانە بەکار دێنێت بۆ ئەوەی کە پارەی نوێی پێ بخوولقێنێت. لە قازانجی ئەودا دەبوو کە یاساکان ڕەچاو بکات و پێشێلیان نەکات – یاسا و قاعیدەگەلێک کە بتوانن پارەی نوێی زیاتر بۆ ئەو لەهەمووان زیاتر بەدیی بێنن. – وەکوو ئەمەیە کە ئەو هەم سیستمەکە و هەمیش ئیعتیباری خۆی لەچاڵ دەنێت.

٧ حافزەی کەمتر پڕبکەینەوە (Reclaiming Disk Space)

هەر کە ئەخیر حەواڵەی پارەیەک لەژێر کۆمەڵە بلۆکێکی زۆردا مایەوە، ئەتوانرێت ئەوجار حەواڵە ماوەبەسەرچووەکان بکووژێندرێنەوە، بۆ ئەوەی جێگای زەخیرە بۆ حەواڵەی نوێ خاڵی بکەین. بۆ ئەوەی ئەمکارە موومکین بکەین بە بێ ئەوەی هاشی بلۆکەکان بپسێندرێن، حەواڵەکان لەناو مێرکل-تڕییدا (Merkle-Tree) [٧][٢][٥] هاش دەکرێن، وە تەنیا ڕووتی (Root) هاشی بلۆکەکان ڕادەگیرێن و جێگیردەکرێن. بلۆکە کۆنەکان ئەوجار ئەتوانرێن تێکبترینجێندرێن، وەک داریک کە شاخە دەرچووەکانی مەقەست ئەکرێت، لەوێش شاخە دەرچووەکان ئەبڕدرێن (و: بڕوانە وێنەی خوارەوە). هاشە نێوخۆییەکانیش دەکرێت زەخیرە یا خەزن نەکرێن.



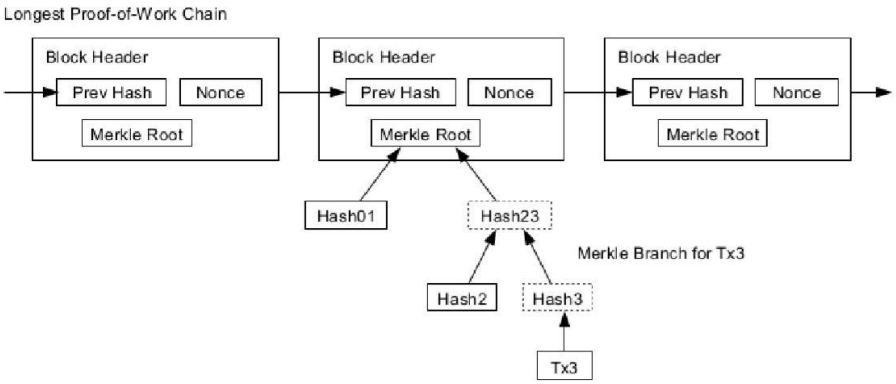
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

بلۆکێکی سەرەکی بە بێ ئەوەی حەواڵەکانی تێدا زەخیرە کرابێت، حدودی ٨٠ بایت جێگا ئەگرێت. ئەگەر ئێمە وایدابنەین کە هەر دە (١٠) خولەکێک یەک بلۆک بخوولقێت، ئەمە یانی ٨٠ بایت زەربی ٦ دانە لەیەک کاتژمێر، زەربی ٢٤ کاتژمێری شەوڕۆژێک، زەربی ٣٦٥ ڕۆژی ساڵێک، هەمووی دەکاتە ٤،٢ میگابایت لە یەک ساڵدا بۆ هەر یەک بلۆک. بە سیستمی کۆمپیوتەرەکان کە لە یەکساڵدا (ئاماری ساڵی ٢٠٠٨) ئاسایی دانەی بە ٢ گیگابایت ڕام یا حافزەی بچووکەوە دەفرۆشرێن، وە یاسای مۆر (Moores Law) کە لە حاڵیحازردا (و: ساڵی ٢٠٠٨) بەرەو ١،٢ سەردەکەوێت، بە پێی ئەم ئامارانە بێت، پێدەچێت جێگای زەخیرە لەداهاتوودا هیچ گرفتێکمان بۆ پێکنەهێنێت، تەنانەت ئەگەر بلۆکە سەرەکییەکانیش لە زەخیرەدا بمێنن یا پێویست بێت زەخیرە بکرێن. (و: ساتۆشی ناکامۆتۆ ڕاستی دەکرد، ئێستا جێگای خاڵی بۆ زەخیرە زۆر و بۆرە!)

٨ ئاسانکاریی تەئیدی گەیشتنی حەواڵەیەک (Payment Verification Simplified)

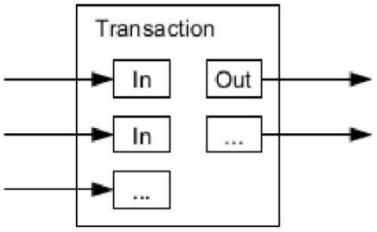
ئێمە ئەتوانین حەواڵەیەک تەئید و مۆر بکەین بێ ئەوەی پێویست بێت هەموو ماینێرەکانی ناو شەبەکەی گشتیی تەئیدیکەن. بەکاربەرێکی ئینترنێت (و: user) ئەبێ تەنیا ئەو کۆپییە لە بلۆکە سەرەتاییەکەی ناو زنجیرەدرێژەکەی سەلماندنی کارکرد لای خۆی بپارێزێت کە پێیدەڕێت، ئەویش بەمجۆرەی کە ئەو گرێکانی دیکەی ناو شەبەکەی گشتیی بەردەوام تاقی بکاتەوە تا بەم قەناعەتە دەگات کە ئەو بەڕاستی درێژترین زنجیری هەیە و شاخە جیابووەکانی مێرکل لەخۆدەگرن کە حەواڵەکە بە بلۆکەکەوە گرێدەدات، ئەوەیش بەمشێوە کە مۆرێکی زەمەنی لێدەراوە. دیارە ئەو ناتوانێت بۆخۆی حەواڵەکە تاقیبکاتەوە، بەڵام کاتێک کە ئەو حەواڵەکە لە شوێنێک لەناو زنجیرەکەدا گرێدەدات، ئەوجار ئەتوانێت ببینێت کە ئەو لەلایەن گرێکانی شەبەکەی گشتیی قەبووڵکراوە و ئەو بلۆکانەی کە پاش ئەو بە زنجیرەکە زیاد دەبن، بە بەردەوامی تەئیدی دەکەنەوە کە حەواڵەکەی ئەو لەلایەن شەبەکەی گشتییەوە وەرگیراوە.



لەم حاڵەتانەدا تەئیدەکانیش تائەوکاتە جێگای متمانەن کە شەبەکەی گشتیی لەلایەن ماینێرە ڕاستگۆکانەوە کۆنترۆڵ بکرێت. شەبەکەکە بەڵام لاوازتر و زیانلێکەوتووتر ئەبێت کاتێک هێرشبەرێک یا هەکرێک بتوانێت شەبەکەی گشتی کۆنترۆڵ بکات. لەکاتێکدا کە ماینێرەکانی ناوشەبەکە خۆیان ئەتوانن حەواڵەکان تەئید بکەن، بەڵام مێتۆدێکی ساکار کراو ئەتوانرێت لەلایەن هەکەرێکەوە بە حەواڵەی تەزویر و ناڕاست خەڵەڵی تێبخرێت و ئەمە نیشانی دەدات کە ئەو چلۆن ئەتوانێت شەبەکە تەسخیر بکات و بیهێنێتە ژێر کۆنترۆڵی خۆی. ڕێگاچارەیەک بۆ ئەوەی خۆمان لەم گرفتە بپارێزین ئەمەیە کە سیگنالی هوشداریدەر کە لە لایەن ماینێرەکانەوە دێن قەبووڵ بکەین، کاتێک ماینێرەکان بلۆکێکی ناموعتەبەریان ناسییەوە کە لە سۆفتوێڕی هەکەرێکەوە نەسبکراوە بۆئەوەی تەواوی بلۆکەکە و ئەوحەواڵەش کە سیگنالی هوشداریدەرەکەی وروژاندووە دابەزێنێت، بەهاتنی سیگنالەکە بوونی خەڵەل و گرفتێک یا بوونی هەکەرێک بناسرێتەوە و خێرا ڕێگای لێبگیردرێت. ئەو ناواندانەی کە بەبەردەوامیی حەواڵەیان بۆ دەچێت یا حەواڵە وەردەگرن، ڕەنگە بیانهەوێت (ئەتوانن) ئیتر ماینەری تایبەت بەخۆیانیان هەبێت، ئەویش بۆئەوەی کە ئەمنییەتی حەواڵەکانیان سەربەخۆ لەدەست خۆیاندا بێت و بەخێرایش بتوانن ڕەدووبەدەڵی حەواڵەکان تەئید بکەن.

٩ کورتکراوەیەکی گشتی و دابەشکردنی ئەرزشەکان (Combining and Splitting Value)

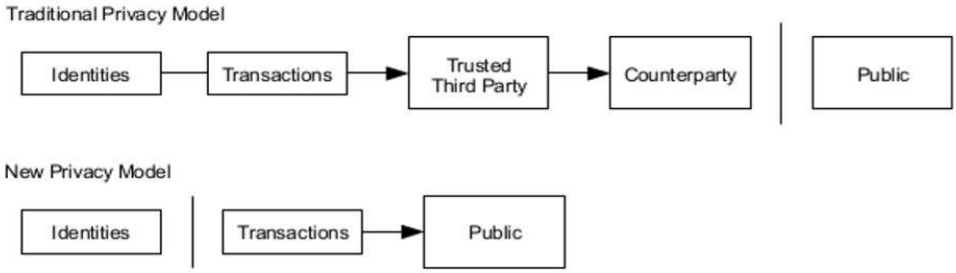
ئەگەر هەرئێستا مومکین بووبایە کە کۆین یا پارە دیجیتاڵییەکانمان بەدەستەوە بوونایە، مەعقوول نەدەبوو ئەگەر بۆ ناردنی هەر سێنتێک لە حەواڵەی جودا جودا کەڵک وەربگرین. بۆ ئەوەی بتوانرێت نرخ و ئەرزشەکان دابەش بکرێن و پێکەوە حیساب بکرێن، حەواڵەکان چەندین دەروازەی بۆچوو و دەرچوو یاخود وروودی و خروجییان (inputs and outputs) پێدەدرێت. ئاسایی یا یەکدانە تاقە بۆچوو لە حەواڵەیەکی گەورەدا بوونی هەیە یاخود چەندین بۆچوو لەئارادان، کە مەبلەغە بچووکەکان پێکەوە کۆدەکەنەوە و لە بەرزترین حاڵەتدا تەنیا دوو دانە دەرچوو: یەکیان بۆ دانی خەرج یا تێچووی حەواڵەکە و ئەویدیکەشیان بۆ گەڕانەوەی باقی پارەی تێچووەکە، دیارە ئەگەر پێویست بە گەڕانەوە بۆ خاوەن حەواڵە بێت، بوونیان هەیە.



لێرەدا پێویستە بگووترێت دەستەبەندیی کردنی حەواڵەیەک بەستراوەتەوە بە چەندین حەواڵەی دیکەشەوە و هەروەتر ئەم چەند حەواڵەش بە چەندەها حەواڵەی دیکەوە بەستراونەتەوە، کە دیارە ئەمە هیچ کێشەیەک بۆ حەواڵەی کەسیتر نانێتەوە. هەرگیز پێویستی و زەڕورەتێک لەئارادا نابێت کە کۆپییەکی تەواوی حەواڵەکان داوابکرێت (و: خاترجەمە).

١٠ حەریمی تایبەتیی یا تاکەکەسیی (Privacy)

مۆدێلی بانکە نەریتیی و کلاسیکیەکان ئاستێکی دیاریکراو لە پاراستنی حەریمی کەسەکانیان هەیە، کە لەواندا دەسپێڕاگەیشتن بە زانیاریی دیجیتاڵییەکانی تەرەفەینی مەعامەلەیەک و تەرەفی سێهەم (وەک: بانک یا ناوەندێکی دارایی)، لەنێوان خۆیاندا سنووردار کراوە و داخراوە. زەرورەتی ئەمەی کە هەر هەموو حەواڵەکان بەئاشکرا و شەفاف ڕوو بەدەرەوە بن کە هەمووان بیانبینن، لەو مێتۆدەی بانکەکاندا جێی نابێتەوە. بەڵام دەکرێت لەگەڵ ئەمەشدا کە فایلی کەسەکان دەپارێزرێت، بڵام زانیارِیی حەواڵەکان لە شوێنێکی دیکەوە بپسێندرێت: ئەویش بەمجۆرەی کە کلیلی ڕووبەدەرەوە شاراوە و نەناسراو ئەمێنێت. خەڵک ئەتوانن ببینن کاتێک کەسێک مەبلەغێک پارە بۆ کەسێکی دیکە حەواڵە ئەکات، بێ ئەوەی بزانن، ئەم حەواڵە لە چ کەسێکەوە بۆ چ کەسێکی دیکە بەڕێکراوە. ئەمە وەکوو ئەو دەستە زانیاریانە دەچێت کە لەلایەن بورسەوە بڵاو دەکرێنەوە، کە لەواندا کات و چەندەیی یا گەورەیی مەعامەلەی کەسەکان، واتە "Tape" بۆ ڕایگشتی بڵاودەکرێنەوە، بێئەوەی دیان بەمەدا بێنن کە تەرەفەینی مەعامەلەکە کێن.



بۆ ئەوەی ئیحتیاتی پێویستمان کردبێت چاکوایە بۆ هەر حەواڵەیەک یەک جووت کلیلی نوێ بەکار بهێنرێت، بۆ ئەوەی بەربەمە بگیردرێت کە کلیلەکان بکەونە دەست کۆمەڵە کەسانێکەوە کە یەکتر ناناسن. هەندێک لە گرێکان لە حەواڵەکاندا بە چەندین وروودییەوە پارێز یا دووربیان لێناکرێت یاخۆیان لێلانادرێت، لەبەر ئەوەی ئەمانە زەرورەتەن نرخدەدەن، بۆئەوەی بۆچوو یا وروودییەکانیان هی هەر هەمان خاوەن حەواڵەن. ڕیسکی ئەمکارە لێرەدایە کە ئەگەر خاوەنی کلیلێک بناسێندرێت بە هەمووان، کە گرێی حەواڵەکانی دیکە بتوانێت بڵاو بکاتەوە، کە هی هەمان خاوەن کلیل بوو!

١١ نرخ و تێچووەکان (Calculations)

ئێمە بیر لە سیناریۆیەک ئەبێ بکەینەوە کە لەودا هەکرێک هەوڵدەدات زنجیرێکی جێگر یا ئەڵتەرناتیف زووتر لە زنجیرە ڕاست و هەقیقییەکەی ئێمە پێکبێنێت. تەنانەت ئەگەر ئەو بتوانێت لەمکارەشیدا سەرکەوتوو بێت، سیستمەکە ڕێگا بە ئاڵوگۆڕی بەئیشتیا نادات، وەکوو بۆنمونە لەخۆڕا نرخ لەسەر شتێکی بێبایەخ دابندرێت یاخود پارەیەک هەڵبگرێت کە هی ئەو نییە. ماینێرەکان هیچ حەواڵەیەکی ناموعتەبەر بەجێگای تێچووی خۆیان قەبوڵ ناکەن، وە ماینێرە سادەکان هەرگیز بلۆکێکیش قەبوڵ ناکەن کە لەوجۆرە داتا نادروستە و ناتەواوانەی لەخۆگرتبێت. هەکرێک تەنیا ئەتوانێت هەوڵبدات ئاڵوگۆڕ لە یەکێک لە حەواڵەکانی خۆیدا پێکبێنێت، بۆ ئەوەی ئەو پارە بگێڕێتەوە بۆخۆی کە ماوەیەکی کورت پێشتر بۆ کەسێکی ناردووە.

کێبەرکێی نێوان زنجیرێکی هەقیقی و زنجیرێکی تەزویری هەکرێک ئەکرێت وەکوو هەنگاوێکی بەهەڵکەوتی داهاتوو (Binomial Random Walk)، (وەک: ئیستلاحێکی بیرکاریە) لێکبدرێتەوە. ئاکامی سەرکەوتوو ئەمەیە کە یەک بلۆک بە زنجیرە هەقیقییەکە زیادبکرێت، بەمجۆرە زنجیرەکەمان (١+) پێشدەکەوێت. بەڵام زنجیرە هەقیقییەکە ئەدۆڕێت ئەگەر بێت و زنجیری هەکرەکە یەکی پێ زیاد ببێت، کە ئەمە (١-) بەزەرەری زنجیرە ئەسڵییەکە تەواو دەبێت و دووایدەخات.

ئیحتیمالی ئەوەی کە هەکرێک پێش ئێمە بکەوێتەوە وەکوو قوماری (Gambler's Ruin problem)، (وەک: بەئاڵمانی Ruin des Spielers)، (وەک: بەفارسی: پاکباختگی قمارباز) وایە! وایدابنەین، یاریکەرێک بە پارەیەکی زۆر و بێسنوورەوە دەست بە یاری بکات بە جۆرێک کە ژمارەیەک یا بڕێک لەدووای حەریفەکەیەوە دەسپێبکاتن، ئەوجار بە هێزوگوورمێکی بیلقووە و بە

پارەیەکی بێسنوورەوە دێتە ناو یارییەکە، ئەویش بەم ئامانجەی کە یارییەکە ببات‌ەوە. ئێمە ئەتوانین ئیحتیمالی ئەوەی کە ئایا ئەم یاریکەرە ئامانجەکەی ئەپێکێت و یارییەکە ئەباتەوە، وەیا لە مەوزوعەکەی خۆماندا ئایا هەکرێک بتوانێت زنجیرە بلۆکە هەقیقییەکانی ئێمە بێنێتە ژێر ڕەکیف و کۆنترۆڵی خۆی، ئەتوانین لە بیرکاریدا بەمشێوەی خوارەوە حەدس لێبدەین یا حیسابی بکەین. [٨]:

(p) = ئیحتیمالی ئەمەی کە ماینێرێکی ڕاستەقینە و هەقیقی بلۆکێی داهاتوو یا نوێ بدۆزێتەوە

(q)= ئیحتیمالی ئەمەی کە هەکر یا دەسدرێژکەر بلۆکی نوێی داهاتوو بدۆزێتەوە

(q_z)= ئیحتیمالی ئەمەی کە هەکر بەو بڕە بلۆکە بگاتەوە، کە بابڵەین (z) بلۆکن، کە لەپاش کەوتووە

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

پاش گریمانەکەی ئێمە کە پی گەورەتر بێت لە کیوو ($p>q$)، ئیحتیمالەکە بە شێوەیەکی ئێکسپۆنێنتیەل دادەکەوێت ئەگەر ژمارەی ئەو بلۆکانەی کە هەکرەکە دەبێت پێیان بگاتەوە، هاوکات بەرزتر یا زۆرتریش ببنەوە. ئەگەر ئیحتیمالەکە لە دژی ئەو بێت و لەقازانجی نەبێت، وە ئەو لەکاتی خۆیدا یا زووتر لە کاتی پێویست بازێکی سەرکەوتووانە هەڵنەدات، شانسەکانی ئەو بە شێوەیەکی زەرەرلێکەوتوو زۆر کەم دەبن، بەتایبەتیش ئەگەر ئەو هەندێک لەوەش کە هەیە دووا‌تریش بکەوێت، واتە بە خاوی بڕواتە پێش.

ئێستا ئێمە لێکیدەدەینەوە کە حەوالە وەرگرێک چەندە ئەبێت ماتڵ بێت، تائەو بەتەواوەتیی دڵنیابێت کە حەوالەنێرەر ئیتر حەوالەکە نەتوانێت دەسکاریی یا کەم و زۆری بکاتن. ئێمە وایدادەنێین یا گریمانە دەکەین کە نێرەری حەوالەکە خۆی هەکرێک بێت، کە بییەوێت بۆماوەیەک حەوالە وەرگر بەم قەناعەتە بگەیەنێت کە ئەو پارەکەی ناردووە و تەواو بووە، ئەوجار پاش ماوەیەک ئاڵوگۆڕ بەسەر حەوالەکەدا دێنێت، بەجۆرێک کە حەوالەکە بۆ هەکرەکە خۆی بگەڕێتەوە. حەوالەوەرگر خەبەردار دەکرێتەوە کاتێک ئەم شتە ڕووبدات، بەڵام حەوالە نێرەر (و: کە خۆی هەکرە و ئەیەوێت کڵاومان سەرکات)، هیواداراە پارەکە بۆخۆی بگێڕێتەوە، پێش ئەوەی حەوالە وەرگر لە دزرانی حەوالەکەی وشیار بکرێتەوە.

حەوالە وەرگر یەکجووت کلیلی نوێ بۆخۆی ئەخوڵقێنێت (generates)، کلیلە گشتییە ڕووبەدەرەوەکەی ماوەیەکی کورت پێش واژۆکردنی دەدات بە نێرەر. (و: بۆ زانیاریی خوێنەر، یەک لەم کلیلانە گشتییە و ڕووبەدەرەوە و بۆ حەوالەیە و ئەویدیکەیان تایبەتییە و ئەبێ لەسەر پارچە کاغەزێک بنووسرێت و هەڵبگیرێت و نابێت نیشان کەسی نادڵنیا بدرێت، چوون هەرکەس ئەو کلیلە تایبەتییەی هەبێت، ئەتوانێت پارەکانت بگوازێتەوە سەر والێت یا کیفە پوڵی خۆی!) ئەمکارە بەر بەوە دەگرێت کە نێرەرێک، (و: دیارە ئەگەر مەبەستی دزیی هەبێت!) پێشتر زنجیرێک لە بلۆکەکانی دروووست و ئامادەکردبێت، چوونکە ئەبێت هێندە کاری لەسەر بکات تائەوکاتەی کە شانسی هەبێت و بازێکی گەورەی هەڵدابێت و وەپێش کەوتبێتەوە و ئەوجار حەوالەکە لە کورتەچرکەیەک یا لە لەحزەیەکدا چێ یا دروووست بکات. ئەگەر حەوالەیەک جارێک نێردرا، ئەوجار نێرەرێکی کڵاوچی بەدزییەوە و هاوکات لەسەر زنجیرێکی موازیی دەستبەکار دەبێت کە ڤێرژنێکی ئاڵوگۆڕپێکراوی حەوالەکەی خۆیەتی.

وەرگری حەوالەکە ماتڵە، تا حەوالەکەی ئەو لە بلۆکێکدا بەڕێوە دەچێت و پاشانیش(z)دانە بلۆکیتر بەدووای ئەودا بەزنجیرە بلۆکەکان زیاد دەبن. ئەو بەتەواوەتی نازانێت کە ئایا هەکرەکە چەندە لەکارەکەی خۆیدا پێشکەوتووە، بەڵام پێیوایە کە بلۆکە هەقیقی و دروستەکان کە کاتێکی مامناوەندییان بۆ هەر بلۆکێک پێویست بووە (و: لە زنجیری بیتکۆیندا هەر دە (١٠) خولەک بلۆکێک پێکدێت.) وەکوو پێشکەوتنێکی خێرا و بیلقووەی هێرشبەرکە وایە، وەکوو دابەشکردنی پۆیسۆن (ئیستلاحێکی بیرکارییە poisson distribution) بە نرخێکی چاوەڕوانکراو:

$$\lambda = z\frac{q}{p}$$

بۆ ئەوەی کە ئیحتیمالاتی ئەوە بەدەست بێنین کە هێرشبەر ئێستا ئیتر توانیبێتی پێشمانبکەوێتەوە، ئێمە گرفتی پۆیسۆن زەربدەکەین لە هەر هەموو کۆکراوەکان یا حاسڵجەمعی ئەو پێشکەوتنانەی کە ڕەنگە ئەو کردبێتی، بەم ئیحتیمالەی کە ئەو لەم خاڵە بەدوواوە ئیتر پێشمانبکەوێتەوە:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

ئێمە فورمولەکە دەگۆڕین، بۆئەوەی بەر بگرین بە پاشکۆما بێسنووورەکان کە لەگەڵ دابەشبووەکە کۆدەکرێنەوە....

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

وە ئەمانە وەردەگێڕینەوە بۆسەر کۆدی سی (C Code)....

```
#include <math.h>

double AttackerSuccessProbability(double q, int z)

{

        double p = 1.0 - q;

        double lambda = z * (q / p); double sum = 1.0;

        int i, k;

        for (k = 0; k <= z; k++)

        {

                double poisson = exp(-lambda); for (i = 1; i <= k; i++)

                poisson *= lambda / i;

                sum -= poisson * (1 - pow(q / p, z - k));

        }

        return sum;

}
```

ئەگەر ئێمە بێڵین کۆمەڵێک لە ئاکامەکان بکەونە گەڕ، ئەشتوانین لێکیبدەینەوە کە چلۆن ئیحتیمالاتەکان بە شێوەیەکی ئێکسپۆنێنتیەل بە (z) ئەکەون.

```
q=0.1

z=0   P=1.0000000

z=1   P=0,2045873

z=2   P=0,0509779
```

z=3 P=0,0131722

z=4 P=0,0034552

z=5 P=0,0009137

z=6 P=0,0002428

z=7 P=0,0000647

z=8 P=0,0000173

z=9 P=0,0000046

z=10 P=0,0000012

q=0,3

z=0 P=1.0000000

z=5 P=0.1773523

z=10 P=0.0416605

z=15 P=0.0101008

z=20 P=0.0024804

z=25 P=0.0006132

z=30 P=0.0001522

z=35 P=0.0000379

z=40 P=0.0000095

z=45 P=0.0000024

z=50 P=0.0000006

حەلی پی (p) چکۆلەترە لە ٪١،٠

P < 0.001

q=0.10 z=5

q=0.15 z=8

q=0.20 z=11

q=0.25 z=15

q=0.30 z=24

q=0.35 z=41

q=0.40 z=89

q=0.45 z=340

١٢ کورتە و ئاکام (Conclusion)

ئێمە سیستمێکمان بۆ حەواڵە ئێلێکترۆنیکییەکان پێشنیاز کردووە، بە بێ ئەوەی ناچاربین پشت بە متمانەی تەرەفێکی ناوپشکی سێهەم ببەستین. ئێمە ئاسایی ئێستا (و: بە مێتۆدە کلاسیکیەکانی وەک بانک) بە سیستمێک کار دەکەین کە ئەگەرچی کۆنترۆڵێکی بەهێز ئەبەخشێتە تاکی مرۆڤ بەسەر دارایییەکانی خۆیدا، بەڵام هێشتا ناتەواوە بەبێ بوونی مێتۆدێک کە بەربگرێت بە هەزینەی چەند کەرتەی حەواڵەکان. (و: ئیرادی دیکەی بانک ئەمەیە کە سێنترالیزەیە و لە کۆنترۆڵی کۆمەڵە دەوڵەمەندێک یا دەوڵەتدایە). بۆ ئەوەی ئەم کێشە و گرفتە چارەسەر بکەین، ئێمە شەبەکەیەکی گشتیی هاوتابەهاوتامان پێشنیاز کردووە کە کەڵک لە سەلماندنی کارکرد وەردەگرێت، بۆ ئەوەی لەسەر لەوحێکی بەرینی گشتی و ڕووکراوە هەموو (چەندوچۆنی) حەواڵەکان زەخیرە دەکات و لای هەمووان دیارە، کە بۆ هەکر یا هێرشبەرێک ناومکینە کە بتوانێت بەخێرایی ئاڵوگۆڕی (و: یا دزی) تێدا بکاتن، تا ئەوکاتەی کە ماینێرە سادقەکان زۆرینەی هێزی سی پی یووەکان لەکۆنترۆڵی خۆیاندا بێت. ئەم شەبەکە لە عەینی ساکاری خۆیدا، زۆریش بەهێز و پابەرجایە. ماینێرەکان هەموویان هاوکات پێکەوە کاردەکەن بە کەمترین هاوئاهەنگی نێوانیان. ئەوان ناچار نین بەمەی کە دەبێ حەتمەن بناسرێن، لەبەر ئەوەی کە هەواڵەکان بۆ ناوەندێکی تایبەت نانێردرێت و تەنیا لەسەر بنەمای زیاترین و باشترین زەحمەت و خزمەتگوزارییەکاندا دەبێت بنێردرێت. ماینێرەکان ئەتوانن شەبەکەکە بەجێبێڵن، هەرکات خۆیان حەزیان لێبێت، هەروەها ئەشتوانن بەدڵی خۆیان بێنە ناو شەبەکەکەوە و پڕۆسەی سەلماندنی کارکرد قەبوڵ بکەن و بەڕێوەی ببەن و درێژەی پێبدەن بەوەی کە لە نەبوونی ئەواندا بوونی هەبووە و ئێستا خۆیانیش هاتوونەتە ناوی. ئەوان بە هێزی سی پی یووەکانیان دەنگ دەدەن، قەبوولکردنی درووستبوونی بلۆکێکی هەقیقی بەمە ئەسەلمێنن کە ئەوان لەسەر درووستکردنی بەردەوامی بلۆکی زیاتردا کاردەکەن و بلۆکە ناموعتەبەرەکان ڕەتدەکەنەوە، لەمەی کە بەهیچ کلۆجێک کار لەسەر بلۆکی فەرعی و ناڕاست ناکەن و بەر بە پەرە سەندنی ئەگرن. هەر هەموو یاسا و قاعیدە پێویستەکان و ئەنگیزە و هاندرانەکان ئەتوانرێن بەم میکانیزمە گشتییە تا کۆتایی بەڕێوە ببردرێن.

سەرچاوەکان:

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

وەرگێڕانێکی ئازادە لە ئاڵمانییەوە و بەهەڵسەنگاندنی لەگەڵ زمانی سەرچاوە واتە ئینگلیزی!

کۆتایی: یەکشەممە، ٢ی بانەمەڕی ٢٧١٨ یاخود ٢٢-٠٤-٢٠١٨

Donation, only BTC: 3MM9P4teD765gFwKceAetQvf4HPUiE7V1a

یارمەتی, تەنیا بۆ بیتکۆینە، سپاس: 3MM9P4teD765gFwKceAetQvf4HPUiE7V1a

X

Ayub Rahmani
Übersetzer, Translator