

বিটকয়েন: পিয়ার-টু-পিয়ার বৈদ্যুতিক নগদ সিস্টেম

সাতোশি নাকমোটো

satoshin@gmx.com

www.bitcoin.org

এর থেকে বাংলায় অনুবাদ: bitcoin.org/bitcoin.pdf

অনুবাদক: সাফিউন মিরাজ এবং তন্ময় সরকার

বিমূর্ত। বৈদ্যুতিক নগদের একটি পিয়ার-টু-পিয়ার সংস্করণ অনলাইনে অর্থ প্রদানকারী কোনও আর্থিক প্রতিষ্ঠানের মাধ্যমে না গিয়ে সরাসরি এক পক্ষ থেকে অন্য পক্ষের কাছে প্রেরণের অনুমতি দেয়। ডিজিটাল স্বাক্ষরগুলি সমাধানটির অংশ সরবরাহ করে, তবে যদি কোনও বিশ্বস্ত তৃতীয় পক্ষের দ্বিগুণ ব্যয় রোধ করার জন্য এখনও প্রয়োজনীয় প্রয়োজন হয় তবে প্রধান সুবিধাগুলি হারাতে পারে। পিয়ার-টু-পিয়ার অন্তর্জাল ব্যবহার করে আমরা দ্বিগুণ ব্যয়ের সমস্যার সমাধানের প্রস্তাব দিই। অন্তর্জাল টাইমস্ট্যাম্পগুলি হ্যাশ-ভিত্তিক প্রুফ অফ ওয়ার্কের চলমান শৃঙ্খলে নিয়ে লেনদেন করে, এমন একটি রেকর্ড তৈরি করে যা প্রুফ-অফ-ওয়ার্কটি পুনরায় না করে পরিবর্তন করা যায় না। দীর্ঘতম চেইন কেবল সাক্ষরিত ঘটনাবলী ক্রম প্রমাণ হিসাবেই কাজ করে না তবে এটি প্রমাণ করে যে এটি সিপিইউ শক্তির বৃহত্তম পুল থেকে এসেছে। যতক্ষণ না বেশিরভাগ সিপিইউ শক্তি নোডগুলি দ্বারা নিয়ন্ত্রিত হয় যা অন্তর্জাল আক্রমণ করতে সহায়তা করে না, তারা দীর্ঘতম শৃঙ্খল এবং দ্রুততর বেগে চলা আক্রমণকারী তৈরি করবে। অন্তর্জাল নিজেই ন্যূনতম কাঠামো প্রয়োজন। বার্তাগুলি একটি সর্বোত্তম প্রচেষ্টার ভিত্তিতে সম্প্রচারিত হয় এবং নোডগুলি ইচ্ছামত অন্তর্জালটি ছেড়ে যেতে এবং পুনরায় যোগদান করতে পারে, দীর্ঘস্থায়ী প্রমাণ-কার্য-শৃঙ্খলা গ্রহণের পরে যা ঘটেছিল তার প্রমাণ হিসাবে।

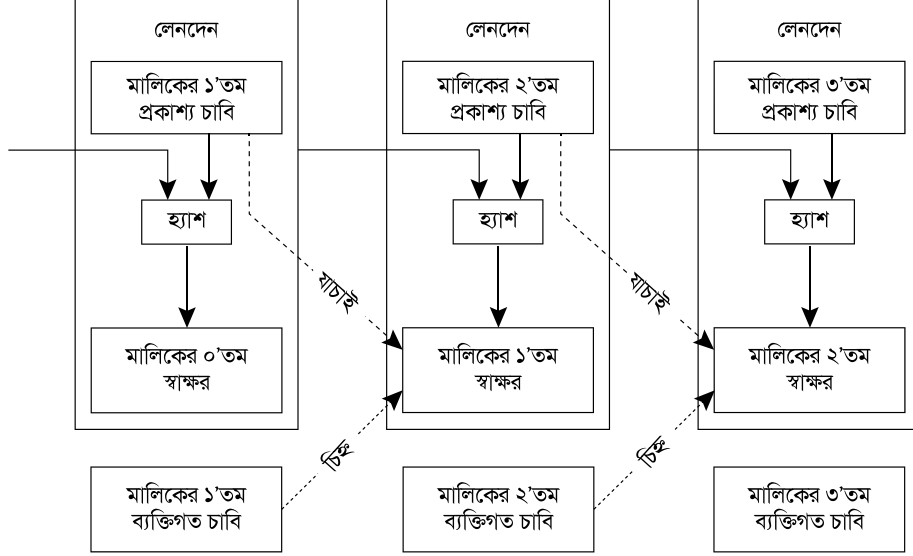
১। পরিচিতি

ইন্টারনেটে বাণিজ্য বৈদ্যুতিক পেমেন্ট প্রক্রিয়াজাত করতে তাৎপর্যপূর্ণ তৃতীয় পক্ষের পরিবেশিত আর্থিক সংস্থা গুলিতে প্রায় একচেটিয়া ভাবে নির্ভর করতে এসেছে। যদিও পদ্ধতিটি পর্যাপ্ত পরিমাণে লেনদেনের কাজ করে, তবুও এটি বিশ্বাস ভিত্তিক মডেলটির অন্তর্নিহিত দুর্বলতাগুলি ভোগ করে মধ্যস্থতার ব্যয় লেনদেনের ব্যয় বৃদ্ধি করে, এগুলি ব্যবহারিক লেনদেনের সর্বনিম্ন আকার সীমাবদ্ধ করে এবং ছোট ছোট নৈমিত্তিক লেনদেনের সম্ভাবনা কেটে দেয়, এবং অবিবর্তনীয় পরিষেবার জন্য অবিবর্তনীয় পেমেন্টগুলি করার ক্ষমতা হ্রাস করার ক্ষেত্রে বিস্তৃত ব্যয় হয়। বিপর্যয়ের সম্ভাবনা সহ, বিশ্বাসের প্রয়োজনীয়তা ছড়িয়ে পড়ে। ব্যবসায়ীরা তাদের গ্রাহকদের সতর্ক থাকতে হবে, অন্যথায় প্রয়োজনের চেয়ে আরও তথ্যের জন্য তাদেরকে ঝামেলা করছে এই ব্যয়গুলি এবং অর্থ প্রদানের অনিশ্চয়তা শারীরিক মুদ্রা ব্যবহার করে ব্যক্তিগতভাবে এড়ানো যেতে পারে, তবে কোনও বিশ্বস্ত দল ছাড়া কোনও যোগাযোগের চ্যানেলে অর্থ প্রদানের কোনও ব্যবস্থা নেই।

যা প্রয়োজন তা হ'ল আস্থার পরিবর্তে ক্রিপ্টোগ্রাফিক প্রমাণের ভিত্তিতে একটি বৈদ্যুতিক অর্থ প্রদানের ব্যবস্থা, যে কোনও দুটি ইচ্ছুক পক্ষকে বিশ্বাসযোগ্য পক্ষের প্রয়োজন ছাড়াই একে অপরের সাথে সরাসরি লেনদেনের অনুমতি দেয়। যে লেনদেনগুলি গণনাগতভাবে বিপরীতে অবৈধ হয় সেগুলি বিক্রয়কারীদের প্রতারণার হাত থেকে রক্ষা করে এবং ক্রেতাদের সুরক্ষার জন্য নিত্যকার্যসূচি এসক্রো পদ্ধতিগুলি সহজেই প্রয়োগ করা যেতে পারে। এই কাগজে, আমরা লেনদেনের কালানুক্রমিক ক্রমের গণ্যমান্য প্রমাণ উৎপন্ন করতে পিয়ার-টু-পিয়ার বিতরণ টাইমস্ট্যাম্প সার্ভার ব্যবহার করে ডাবল-ব্যয়ের সমস্যার সমাধানের প্রস্তাব করি। সিস্টেম ততক্ষণ সুরক্ষিত থাকবে যতক্ষণ না সং নোডগুলি সম্মিলিতভাবে আক্রমণকারী নোডগুলির কোনও সহযোগী গোষ্ঠীর চেয়ে বেশি সিপিইউ শক্তি নিয়ন্ত্রণ করে।

২। লেনদেন

আমরা একটি বৈদ্যুতিক মুদ্রা ডিজিটাল স্বাক্ষরের একটি শৃঙ্খল হিসাবে সংজ্ঞায়িত করি। প্রতিটি মালিক পূর্ববর্তী লেনদেনের একটি হ্যাশ এবং পরবর্তী মালিকের পাবলিক কীতে ডিজিটালি স্বাক্ষর করে এবং মুদ্রার শেষে যুক্ত করে মুদ্রাটি পরবর্তীটিতে স্থানান্তর করে। একজন প্রাপক মালিকানার শৃঙ্খলা যাচাই করতে স্বাক্ষরগুলি যাচাই করতে পারবেন

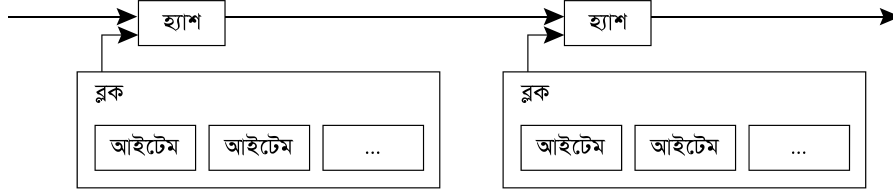


অবশ্যই সমস্যাটি হ'ল প্রাপক যাচাই করতে পারবেন না যে কোনও মালিকের মুদ্রায় দ্বিগুণ ব্যয় হয়নি। একটি সাধারণ সমাধান হ'ল বিশ্বস্ত কেন্দ্রীয় কর্তৃপক্ষ বা পুদিনা প্রবর্তন করা, যা দ্বিগুণ ব্যয়ের জন্য প্রতিটি লেনদেন পরীক্ষা করে। প্রতিটি লেনদেনের পরে, নতুন মুদ্রা জারির জন্য মুদ্রাটি অবশ্যই পুদিনায় ফিরিয়ে দিতে হবে, এবং কেবল পুদিনা থেকে সরাসরি জারি করা কয়েনগুলি দ্বিগুণ ব্যয় না করার জন্য বিশ্বাসযোগ্য। এই সমাধানের সাথে সমস্যাটি হ'ল পুরো অর্থ ব্যবস্থার ভাগ্য নির্ভর করে যে কোনও টাকার মতো প্রতিটি লেনদেনের মধ্য দিয়ে যেতে হবে, পুদিনা চালাচ্ছে সংস্থাটির উপর।

পূর্ববর্তী মালিকরা কোনও পূর্ববর্তী লেনদেনে স্বাক্ষর করেন নি তা জানার জন্য আমাদের প্রাপকের জন্য একটি উপায় প্রয়োজন। আমাদের উদ্দেশ্যগুলির জন্য, প্রাচীনতম লেনদেনটি সেই হিসাবে গণনা করা হয়, তাই আমরা দ্বিগুণ ব্যয়ের পরবর্তী প্রচেষ্টা সম্পর্কে চিন্তা করি না। কোনও লেনদেনের অনুপস্থিতি নিশ্চিত করার একমাত্র উপায় হ'ল সমস্ত লেনদেন সম্পর্কে সচেতন হওয়া। পুদিনা ভিত্তিক মডেলটিতে, পুদিনাটি সমস্ত লেনদেন সম্পর্কে সচেতন ছিল এবং সিদ্ধান্ত নিয়েছে যে কোনটি আগে পৌঁছেছে। কোনও বিশ্বস্ত দল ছাড়াই এটি সম্পাদন করার জন্য, লেনদেনগুলি অবশ্যই প্রকাশ্যে ঘোষণা করতে হবে [১], এবং অংশগ্রহণকারীদের যে অর্ডার প্রাপ্ত হয়েছিল তার একক ইতিহাসে একমত হওয়ার জন্য আমাদের একটি সিস্টেমের প্রয়োজন। প্রদানকারীর এমন প্রমাণ প্রয়োজন যে প্রতিটি লেনদেনের সময়, বেশিরভাগ নোড সম্মত হন যে এটি প্রথম প্রাপ্ত।

৩। টাইমস্ট্যাম্প সার্ভার

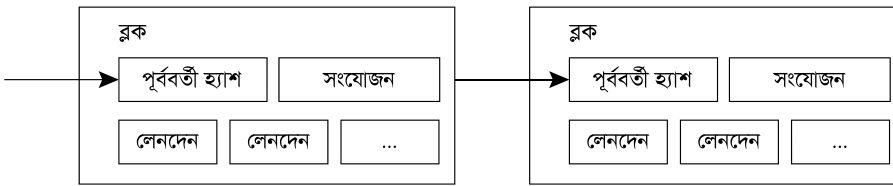
আমাদের প্রস্তাবিত সমাধানটি একটি টাইমস্ট্যাম্প সার্ভার দিয়ে শুরু হয়। একটি টাইমস্ট্যাম্প সার্ভার টাইমস্ট্যাম্প করার জন্য আইটেমগুলির একটি ব্লকের একটি হ্যাশ নিয়ে এবং হ্যাশকে ব্যাপকভাবে প্রকাশ করার মাধ্যমে কাজ করে, যেমন একটি সংবাদপত্র বা ইউজনেট পোস্টে [২-৫]। টাইমস্ট্যাম্পটি প্রমাণ করে যে হ্যাশটিতে প্রবেশের জন্য অবশ্যই ডেটা অবশ্যই উপস্থিত ছিল। প্রতিটি টাইমস্ট্যাম্পটিতে তার হ্যাশটিতে পূর্ববর্তী টাইমস্ট্যাম্প অন্তর্ভুক্ত থাকে, একটি শৃঙ্খলা তৈরি করে প্রতিটি অতিরিক্ত টাইমস্ট্যাম্প এর আগেটিকে আরও শক্তিশালী করে।



৪। প্রফ অফ ওয়ার্ক

পিয়র-টু-পিয়র ভিত্তিতে বিতরণ করা টাইমস্ট্যাম্প সার্ভারটি প্রয়োগ করার জন্য আমাদের অ্যাডাম ব্যাকের হ্যাশক্যাশ [৬] এর মতো একটি কাজের প্রমাণ পদ্ধতি ব্যবহার করতে হবে, সংবাদপত্র বা ইউজনেট পোস্টের পরিবর্তে। প্রফ-অফ-ওয়ার্ক এমন কোনও মানের জন্য স্ক্যান করা জড়িত যা হ্যাশ করার পরে যেমন SHA-256 এর সাথে হ্যাশটি শূন্য বিটগুলির সাথে শুরু হয়। প্রয়োজনীয় গড় কাজ প্রয়োজনীয় শূন্য বিটের সংখ্যায় তাৎপর্যপূর্ণ এবং একক হ্যাশ চালিয়ে যাচাই করা যেতে পারে।

আমাদের টাইমস্ট্যাম্প নেটওয়ার্কের জন্য, আমরা ব্লকটিতে একটি নাক বাড়াতে কাজের প্রমাণ বাস্তবায়ন করি যতক্ষণ না কোনও মান পাওয়া যায় যা ব্লকের হ্যাশকে প্রয়োজনীয় শূন্য বিট দেয়। কাজের প্রমাণটিকে সম্ভব করার জন্য একবার সিপিইউ প্রচেষ্টা ব্যয় হয়ে গেলে, কাজটি আবার করা ছাড়া ব্লকটি পরিবর্তন করা যাবে না। যেহেতু পরে ব্লকগুলি বেঁধে রাখা হয়েছে, ব্লকটি পরিবর্তন করার কাজটির পরে সমস্ত ব্লক পুনরায় করা অন্তর্ভুক্ত থাকবে।



কাজের প্রমাণ সংখ্যাগরিষ্ঠ সিদ্ধান্ত গ্রহণে প্রতিনিধিত্ব নির্ধারণের সমস্যাও সমাধান করে। যদি সংখ্যাগরিষ্ঠতা এক-আইপি-ঠিকানা-এক-ভোটের ভিত্তিতে হয়, তবে এটি অনেকগুলি আইপি বরাদ্দ করতে সক্ষম যে কেউ বিপর্যস্ত হতে পারে। প্রফ অফ ওয়ার্কটি মূলত এক-সিপিইউ-এক-ভোট। সর্বাধিক সিদ্ধান্তটি দীর্ঘতম চেইনের দ্বারা প্রতিনিধিত্ব করা হয়, এতে এতে বিনিয়োগের সবচেয়ে বড় প্রমাণের কাজ রয়েছে। যদি বেশিরভাগ সিপিইউ শক্তি সং নোড দ্বারা নিয়ন্ত্রিত হয় তবে সং চেইনটি দ্রুততম বৃদ্ধি পাবে এবং যে কোনও প্রতিযোগী শৃঙ্খলা ছাড়িয়ে যাবে। অতীতের ব্লকটি সংশোধন করতে, আক্রমণকারীকে ব্লকের প্রফ-ওয়ার্ক এবং তার পরে সমস্ত ব্লক আবার করতে হবে এবং তারপরে সং নোডগুলির কাজটি ধরে ফেলতে এবং ছাড়িয়ে যেতে হবে। আমরা পরে দেখাব যে পরবর্তী ব্লকগুলি যুক্ত হওয়ার সাথে সাথে ধীর আক্রমণকারী ধরার সম্ভাবনা তাৎপর্যপূর্ণভাবে হ্রাস পাবে।

সময়ের সাথে সাথে হার্ডওয়্যার গতি বৃদ্ধি এবং চলমান নোডগুলিতে আর্থের ভিন্নতার জন্য ক্ষতিপূরণ দেওয়ার জন্য, কার্য-প্রমাণের অসুবিধাটি একটি চলন্ত গড়কে প্রতি ঘন্টা গড়ে কয়েকটি ব্লকের লক্ষ্যবস্তু করে নির্ধারিত হয়। এগুলি যদি খুব দ্রুত উৎপন্ন হয় তবে অসুবিধা বাড়ে।

৫। অন্তর্জাল

অন্তর্জালটি চালবার পদক্ষেপ গুলি নিম্নরূপ:

১. নতুন লেনদেন সমস্ত নোডে সম্প্রচারিত হয়।
২. প্রতিটি নোড একটি ব্লকে নতুন লেনদেন সংগ্রহ করে।
৩. প্রতিটি নোড তার ব্লকটির জন্য কার্য-প্রমাণের কার্যকর কাজ সন্ধানে কাজ করে।
৪. যখন কোনও নোড একটি কাজের প্রমাণ খুঁজে পায়, তখন এটি সমস্ত নোডে ব্লকটি সম্প্রচার করে।
৫. নোডগুলি কেবলমাত্র যদি এতে সমস্ত লেনদেন বৈধ হয় এবং ইতিমধ্যে ব্যয় না হয় তবে ব্লকটিকে তা গ্রহণ করে।
৬. নোডগুলি পূর্ববর্তী হ্যাশ হিসাবে স্বীকৃত ব্লকের হ্যাশ ব্যবহার করে শৃঙ্খলে পরবর্তী ব্লক তৈরির কাজ করে ব্লকের তাদের গ্রহণযোগ্যতা প্রকাশ করে।

নোডগুলি সর্বদা দীর্ঘতম চেইনটিকে সঠিক বলে মনে করে এবং এটি প্রসারিত করার জন্য কাজ চালিয়ে যাবে। যদি দুটি নোড একই সাথে পরবর্তী ব্লকের বিভিন্ন সংস্করণ সম্প্রচার করে তবে কিছু নোড প্রথমে একটি বা অন্যটি গ্রহণ করতে পারে। সেক্ষেত্রে তারা প্রাপ্ত প্রথমটিতে তারা কাজ করে, তবে অন্য শাখাটি দীর্ঘায়িত হলে সংরক্ষণ করে। বন্ধনটি ভাঙ্গা হবে যখন পরবর্তী প্রফ-অফ-ওয়ার্কটি পাওয়া যায় এবং একটি শাখা দীর্ঘ হয়; যে নোডগুলি অন্য শাখায় কাজ করছিল সেগুলি দীর্ঘতর স্থানে চলে যাবে।

নতুন লেনদেনের সম্প্রচারগুলি সমস্ত নোডে পৌঁছানোর প্রয়োজন হয় না। যতক্ষণ না তারা অনেকগুলি নোডে পৌঁছে যায়, তারা দীর্ঘক্ষণের মধ্যে একটি ব্লকে প্রবেশ করবে। ব্লক সম্প্রচারগুলি বাদ দেওয়া বার্তাগুলি সহনীয়। যদি কোনও নোড কোনও ব্লক না পেয়ে থাকে তবে এটি পরবর্তী ব্লকটি গ্রহণ করলে এবং এটি বুঝতে পারে যে এটি একটি ব্লক হারিয়ে ফেলেছে।

৬। উদ্দীপক

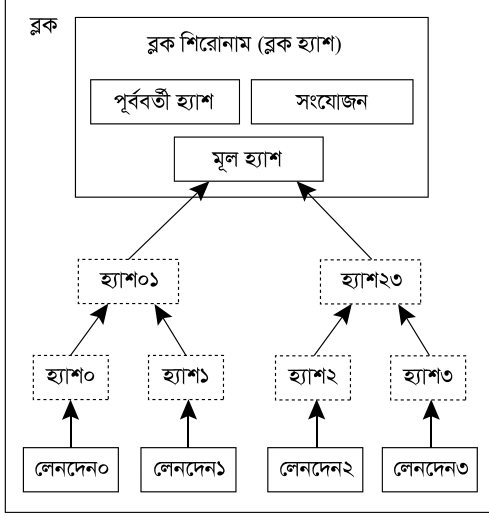
রীতি অনুসারে, কোনও ব্লকের প্রথম লেনদেন হল একটি বিশেষ লেনদেন যা ব্লকের স্রষ্টার মালিকানাধীন একটি নতুন মুদ্রা শুরু করে। এটি নেটওয়ার্ককে সমর্থন করার জন্য নোডগুলির জন্য একটি উৎসাহ যোগ করে, এবং প্রাথমিকভাবে মুদ্রা বিতরণ করার একটি উপায় সরবরাহ করে যেহেতু তাদের জারি করার কোনও কেন্দ্রীয় কর্তৃপক্ষ নেই। অবিচ্ছিন্ন পরিমাণে নতুন মুদ্রার অবিচলিত সংযোজন সোনার খনিজদের সঞ্চয়ে সোনার যোগ করার জন্য সম্পদ ব্যয় করার অনুরূপ। আমাদের ক্ষেত্রে এটি ব্যয় হয় সিপিইউ সময় এবং বিদ্যুৎ।

উৎসাহটি লেনদেনের ফি দিয়েও অর্থায়ন করা যায়। যদি কোনও লেনদেনের আউটপুট মান তার ইনপুট মানের থেকে কম হয় তবে পার্থক্য হ'ল লেনদেনের ফিটি যা লেনদেন সহ ব্লকের প্রেরণামূলক মানের সাথে যুক্ত হয়। একবার নির্ধারিত সংখ্যক কয়েন প্রচলিত প্রবেশের পরে, উৎসাহটি পুরোপুরি লেনদেনের ফিতে স্থানান্তর করতে পারে এবং সম্পূর্ণ মুদ্রাস্বীতিমুক্ত হতে পারে।

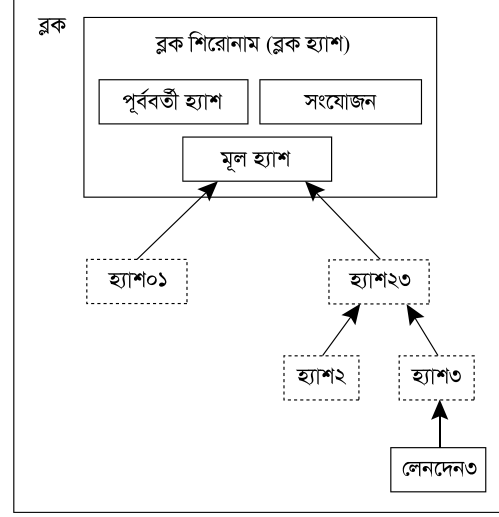
উদ্দীপনাটি নোডগুলিকে সং থাকতে উৎসাহিত করতে সহায়তা করতে পারে। যদি কোনও লোভী আক্রমণকারী সমস্ত সং নোডের চেয়ে বেশি সিপিইউ শক্তি একত্রিত করতে সক্ষম হয়, তবে তার অর্থ প্রদানগুলি চুরি করে বা নতুন মুদ্রা তৈরি করতে ব্যবহার করে লোকেদের প্রতারণা করার জন্য এটি ব্যবহার করতে হবে। নিয়মগুলি খেলে তাকে আরও লাভজনক বলে মনে করা উচিত, এই জাতীয় বিধিগুলি যে সমস্ত ব্যক্তিকে একত্রিত করার চেয়ে বেশি নতুন মুদ্রা দিয়ে তাকে সমর্থন করে, তার নিজের সম্পদের বৈধতা এবং বৈধতা ক্ষুণ্ণ করার চেয়ে।

৭। পুনরায় দাবিকৃত ডিস্ক স্পেস

একবার একটি মুদ্রার সর্বশেষ লেনদেন পর্যাপ্ত ব্লকের নীচে সমাহিত হয়ে গেলে, ব্যয় হওয়া লেনদেনের আগে এটি ডিস্কের স্থান বাঁচাতে ফেলে দেওয়া যায়। ব্লকের হ্যাশটি না ভেঙে এটিকে সহজ করার জন্য, লেনদেনগুলি একটি মর্কলে গাছে হ্যাশ করা হয় [৭] [২] [৫], ব্লকের হ্যাশের সাথে কেবলমাত্র মূল অন্তর্ভুক্ত থাকে। পুরানো ব্লকগুলি তখন গাছের ডালগুলিতে স্ট্যাব করে সংক্ষিপ্ত করা যায়। অভ্যন্তর হ্যাশগুলি সংরক্ষণ করার প্রয়োজন নেই।



লেনদেনগুলি মর্কলে(Merkle) গাছের সাথে মিশে গেছে

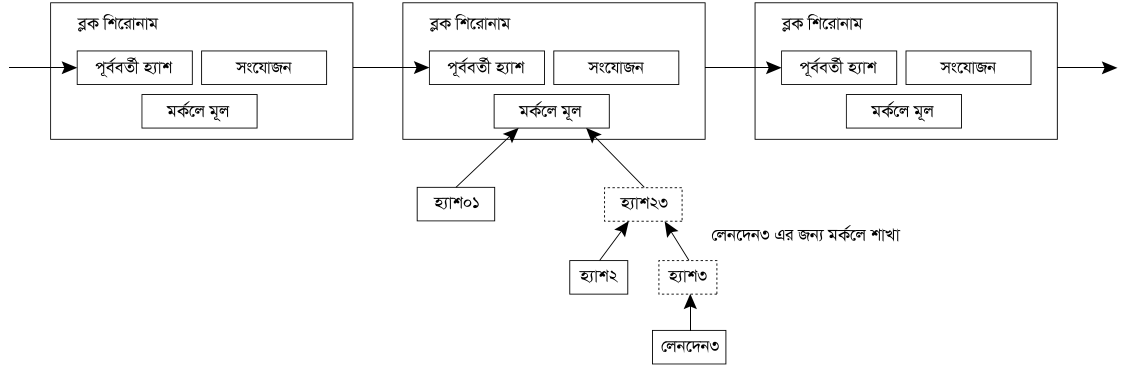


ব্লক থেকে লেনদেন০-২ ছাড়াইয়ের পরে

কোনও লেনদেন ছাড়াই একটি ব্লক শিরোনামটি প্রায় ৮০ বাইট হবে। যদি আমরা ধরে নিই যে প্রতি ১০ মিনিটের মধ্যে ব্লকগুলি উৎপন্ন হয়, প্রতি বছর $৮০ \text{ বাইট} * ৬ * ২৪ * ৩৬৫ = ৪.২ \text{ এমবি}$ । কম্পিউটার সিস্টেমগুলি ২০০৮ সালের হিসাবে সাধারণত ২ গিগাবাইট র‍্যামের সাথে বিক্রি করে এবং মুরের আইন প্রতি বছর ১.২ জিবি বর্তমান বর্ধনের প্রত্যাশা দিয়েছিল, ব্লক শিরোনামগুলি স্মরণে রাখতে হবে এমনকি স্টোরেজ কোনও সমস্যা হবে না।

৮। সরল অর্থ প্রদানের যাচাইকরণ

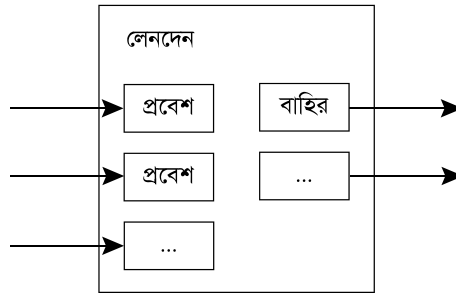
পূর্ণ অন্তর্জাল নোড না চালিয়ে পেমেন্টগুলি যাচাই করা সম্ভব। ব্যবহারকারীর কেবলমাত্র দীর্ঘতম কাজের প্রমাণ শৃঙ্খল ব্লক শিরোনামের একটি অনুলিপি রাখা দরকার, যা সে তার দীর্ঘতম চেইন রয়েছে তা নিশ্চিত না হওয়া অবধি নেটওয়ার্ক নোডগুলি জিজ্ঞাসা করে তা পেতে পারে এবং লেনদেনের সাথে ব্লকের সাথে সংযোগ স্থাপনকারী মর্কলে শাখা পেতে পারে এটি টাইমস্ট্যাম্পড। এটি নিজের জন্য লেনদেনটি পরীক্ষা করতে পারে না, তবে এটি চেইনের কোনও জায়গার সাথে সংযুক্ত করে, তিনি দেখতে পাবে যে কোনও নেটওয়ার্ক নোড এটি গ্রহণ করেছে এবং নেটওয়ার্ক এটি স্বীকার করেছে কিনা তা আরও নিশ্চিত হওয়ার পরে ব্লকগুলি যুক্ত হয়েছে।



যেমন, সং নোডগুলি যতক্ষণ না নেটওয়ার্কটি নিয়ন্ত্রণ করে ততক্ষণ যাচাইযোগ্যতা নির্ভরযোগ্য তবে যদি আক্রমণকারী দ্বারা নেটওয়ার্ককে বাড়িয়ে তোলা হয় তবে এটি আরও ঝুঁকিপূর্ণ। অন্তর্জাল নোডগুলি নিজের জন্য লেনদেন যাচাই করতে পারে, তবে আক্রমণকারীর মনগড়া লেনদেনের দ্বারা সরলীকৃত পদ্ধতিটিকে বোকা করা যায় যতক্ষণ আক্রমণকারী নেটওয়ার্কটিকে পরাভূত করতে পারে। এর বিরুদ্ধে সুরক্ষার জন্য একটি কৌশল হ'ল নেটওয়ার্ক নোডগুলি যখন কোনও অবৈধ ব্লক সনাক্ত করে তখন সতর্কতা গ্রহণ করা, ব্যবহারকারীর সফটওয়্যারটিকে সম্পূর্ণ ব্লকটি ডাউনলোড করার অনুরোধ জানায় এবং অসঙ্গতি নিশ্চিত করার জন্য সতর্কতাপূর্ণ লেনদেন হয়। যে ব্যবসায়গুলি ঘন ঘন অর্থ প্রদান করে তারা সম্ভবত আরও স্বতন্ত্র সুরক্ষা এবং দ্রুত যাচাইয়ের জন্য তাদের নিজস্ব নোড চালাতে চাইবে।

৯। সংমিশ্রণ এবং পৃথকীকরণের মান

যদিও স্বতন্ত্রভাবে কয়েনগুলি পরিচালনা করা সম্ভব হবে, তবে স্থানান্তরের ক্ষেত্রে প্রতি শতাংশের জন্য আলাদা লেনদেন করা অযৌক্তিক হবে। মানটি বিভক্ত এবং একত্রিত হওয়ার অনুমতি দেওয়ার জন্য, লেনদেনে একাধিক ইনপুট এবং আউটপুট থাকে। সাধারণত পূর্বের লেনদেনের একক ইনপুট বা স্বল্প পরিমাণের সংমিশ্রণকারী একাধিক ইনপুট থাকবে এবং সর্বাধিক দুটি আউটপুট থাকবে: একটি অর্থ প্রদানের জন্য, এবং একটি যদি প্রেরকের কাছে ফিরে আসে তবে ফেরত দেওয়া হবে।

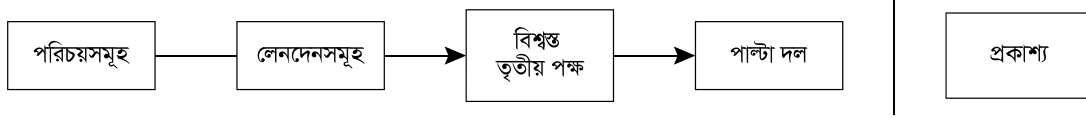


এটি লক্ষ করা উচিত যে ফ্যান-আউট, যেখানে কোনও লেনদেন বিভিন্ন লেনদেনের উপর নির্ভর করে এবং সেই লেনদেনগুলি আরও অনেকের উপর নির্ভর করে, এখানে কোনও সমস্যা নয়। কোনও লেনদেনের ইতিহাসের সম্পূর্ণ স্বতন্ত্র অনুলিপি বের করার প্রয়োজন নেই।

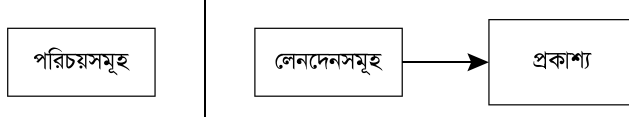
১০। গোপনীয়তা

ঐতিহ্যবাহী ব্যাংকিং মডেল জড়িত পক্ষগুলি এবং বিশ্বস্ত তৃতীয় পক্ষের তথ্যে অ্যাক্সেস সীমাবদ্ধ করে এক স্তরের গোপনীয়তা অর্জন করে। সমস্ত লেনদেনের প্রকাশ্যে ঘোষণা করার প্রয়োজনীয়তা এই পদ্ধতিটিকে বাদ দেয়, তবে তথ্যের প্রবাহকে অন্য জায়গায় ভাগুর মাধ্যমে গোপনীয়তা বজায় রাখা যায়: পাবলিক কীগুলি বেনামে রেখে। জনসাধারণ দেখতে পাচ্ছেন যে কেউ অন্য কাউকে অর্থ পাঠাচ্ছে, তবে কারও সাথে লেনদেনের লিঙ্ক সম্পর্কিত তথ্য ছাড়াই। এটি স্টক এক্সচেঞ্জগুলির দ্বারা প্রকাশিত তথ্যের স্তরের মতো, যেখানে পৃথক ব্যবসায়ের সময় এবং আকার, "টেপ" প্রকাশিত হয়, তবে দলগুলি কারা ছিল তা না জানিয়ে।

চিরাচরিত গোপনীয় মডেল



নতুন গোপনীয় মডেল



অতিরিক্ত ফায়ারওয়াল হিসাবে, প্রতিটি লেনদেনের জন্য একটি নতুন কী জুড়ি ব্যবহার করা উচিত যাতে এগুলি একটি সাধারণ মালিকের সাথে সংযুক্ত না হয়। কিছু সংযোগ এখনও মাল্টি-ইনপুট লেনদেনের সাথে অপরিহার্য, যা অগত্যা প্রকাশ করে যে তাদের ইনপুটগুলি একই মালিকের মালিকানাধীন ছিল। ঝুঁকিটি হ'ল যদি কোনও চাবির মালিক প্রকাশিত হয় তবে লিঙ্কিংয়ের ফলে একই মালিকের সাথে সম্পর্কিত অন্য লেনদেনগুলি প্রকাশিত হতে পারে।

১১। গণনা

আমরা কোনও আক্রমণকারী সৎ চেইনের চেয়ে দ্রুত বিকল্প চেইন উৎপন্ন করার চেষ্টা করার দৃশ্য বিবেচনা করি। এটি সম্পাদন করা সত্ত্বেও, এটি সিস্টেমকে নির্বিচারে পরিবর্তনের জন্য উন্মুক্ত করে না, যেমন পাতলা বাতাসের মূল্য তৈরি করা বা অর্থ গ্রহণ করা যা আক্রমণকারীর অন্তর্ভুক্ত নয়। নোডগুলি অর্থপ্রদান হিসাবে কোনও অবৈধ লেনদেন গ্রহণ করবে না, এবং সৎ নোডগুলি এতে থাকা কোনও ব্লক কখনই গ্রহণ করবে না। একজন আক্রমণকারী তার সম্প্রতি ব্যয় করা অর্থ ফেরত নেওয়ার জন্য কেবল তার নিজের একটি লেনদেন পরিবর্তন করার চেষ্টা করতে পারে।

সৎ চেইন এবং আক্রমণকারী চেইনের মধ্যকার দৌড় বিনোমিয়ালআরডম ওয়াক হিসাবে চিহ্নিত করা যেতে পারে। সাফল্য ইভেন্টটি হ'ল সৎ চেইনটি একটি ব্লক দ্বারা প্রসারিত করা হয়, এর নেতৃত্বকে +১ দ্বারা বৃদ্ধি করা হয় এবং ব্যর্থতার ঘটনাটি হ'ল আক্রমণকারীটির শৃঙ্খলাটি একটি ব্লক দ্বারা প্রসারিত করা হয়, ব্যবধানটি -১ দ্বারা হ্রাস করে।

প্রদত্ত ঘাটতি থেকে আক্রমণকারী ধরা পড়ার সম্ভাবনাটি জুয়ার্স রুইন সমস্যার সাথে মিলে যায়। মনে করুন সীমাহীন creditণের এক জুয়াড়ি ঘাটতিতে শুরু হয় এবং ব্রেক ব্রেকে পৌঁছানোর চেষ্টা করার জন্য সম্ভাব্য অসীম সংখ্যক ট্রায়াল খেলেন। তিনি কখনই ব্রেকিংভেনে পৌঁছায় এমন সম্ভাবনাটি আমরা গণনা করতে পারি, বা আক্রমণকারী কখনই সততার শৃঙ্খলটি ধরে রাখে, [৮]:

p = সম্ভাবনা একটি সৎ নোড পরবর্তী ব্লক সন্ধান করে

q = সম্ভাব্যতা আক্রমণকারীটি পরবর্তী ব্লকটি আবিষ্কার করে

q_z = সম্ভাব্যতাটি আক্রমণকারী কখনই পিছনে z ব্লকগুলি থেকে ধরা পড়বে

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^2 & \text{if } p > q \end{cases}$$

আমাদের অনুমানটি দেওয়া হয়েছে যে $p > q$, আক্রমণকারীকে যে পরিমাণ ব্লক বাড়িয়ে তুলতে হবে তার সংখ্যা হ্রাস হওয়ায় সম্ভাবনা তত দ্রুত হ্রাস পাবে। তার বিরুদ্ধে প্রতিকূলতার সাথে, যদি তিনি প্রথম দিকে কোনও ভাগ্যবান ল্যাংগুয়েজ না করেন তবে আরও পিছনে পড়ার সাথে সাথে তার সম্ভাবনাগুলি অদৃশ্য হয়ে যায়।

আমরা এখন বিবেচনা করছি যে কোনও নতুন লেনদেনের প্রাপক পর্যাপ্ত পরিমাণে নিশ্চিত হওয়ার আগে প্রেরক লেনদেনটি পরিবর্তন করতে পারবেন না তার জন্য অপেক্ষা করতে হবে। আমরা ধরে নিই যে প্রেরক হলেন একজন আক্রমণকারী যিনি প্রাপককে বিশ্বাস করতে চান যে তিনি কিছুক্ষণের জন্য তাকে অর্থ প্রদান করেছেন, তারপরে কিছু সময় কেটে যাওয়ার পরে নিজের কাছে ফেরত দিতে এটিকে হস্তান্তর করুন। যখন এটি ঘটে তখন প্রেরককে সতর্ক করা হবে, তবে প্রেরক আশা করছেন এটি অনেক দেরিতে হবে।

রিসিভার একটি নতুন কী জুড়ি উৎপন্ন করে এবং স্বাক্ষর করার অল্প সময়ের আগে প্রেরককে সর্বজনীন কী দেয়। এটি প্রেরককে অদূরে এগিয়ে যাওয়ার পক্ষে যথেষ্ট ভাগ্যবান না হওয়া অবধি, তারপরে সেই মুহূর্তে লেনদেনটি সম্পাদন না করা অবধি অবিরত কাজ করে এটির আগে অবরুদ্ধ কাজ করে বাধা দেয়। লেনদেনটি পাঠানোর পরে, অসাধু প্রেরক তার লেনদেনের একটি বিকল্প সংস্করণ সমান্তরাল চেইনে গোপনে কাজ শুরু করে।

লেনদেনটি একটি ব্লকে যোগ না করা এবং জেড ব্লকগুলি তার পরে সংযুক্ত হওয়া পর্যন্ত প্রাপক অপেক্ষা করে। আক্রমণকারী কী পরিমাণ অগ্রগতি করেছে তা তিনি জানেন না, তবে সং ব্লকগুলি প্রতি ব্লক হিসাবে গড় প্রত্যাশিত সময় নিয়েছিল, আক্রমণকারীর সম্ভাবনাময় প্রত্যাশিত মান সহ পোইসন বিতরণ হবে:

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

আক্রমণকারীটি এখনও এখন ধরে ফেলতে পারে তার সম্ভাবনা পাওয়ার জন্য, আমরা যে পরিমাণ অগ্রগতি অর্জন করতে পেরেছি তার সম্ভাব্যতার দ্বারা তিনি যে পরিমাণ অগ্রগতি অর্জন করতে পেরেছিলেন, তার জন্য আমরা পোইসনের ঘনত্বকে বহুগুণ করি:

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

বিতরণের অসীম লেজের সংক্ষিপ্তসার এড়াতে পুনরায় সাজানো ...

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

C কোডে রূপান্তর করা হচ্ছে ...

```
#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;
}
```

কিছু ফলাফল চলমান, আমরা z এর সাহায্যে দ্রুততার সম্ভাবনা ছাড়তে দেখি।

```
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
```

P এর জন্য 0.1% এর চেয়ে কম সমাধান করা হচ্ছে ...

```
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
```

১২। উপসংহার

আমরা আস্থার উপর নির্ভর না করে বৈদ্যুতিক লেনদেনের জন্য একটি সিস্টেম প্রস্তাব করেছি। আমরা ডিজিটাল স্বাক্ষরগুলি থেকে তৈরি কয়েনগুলির স্বাভাবিক কাঠামো দিয়ে শুরু করি যা মালিকানার শক্তিশালী নিয়ন্ত্রণ সরবরাহ করে তবে দ্বিগুণ ব্যয় রোধ করার উপায় ছাড়াই অসম্পূর্ণ। এটি সমাধানের জন্য, আমরা লেনদেনের সার্বজনীন ইতিহাস রেকর্ড করার জন্য একটি পিয়ার-টু-পিয়ার অন্তর্জাল এর প্রস্তাব দিয়েছিলাম যে কোনও সতর্ককারী নোডস সিপিইউ ক্ষমতার বেশিরভাগ নিয়ন্ত্রণ করে যদি কোনও আক্রমণকারীর পক্ষে পরিবর্তন ঘটে যায় তবে তা দ্রুত কম্পিউটারের অবৈধ হয়ে ওঠে। অন্তর্জালটি তার কাঠামোহীন সরলতায় বলিষ্ঠ। নোডগুলি সামান্য সমন্বয় নিয়ে একসাথে সব কাজ করে। এগুলি সনাক্ত করার দরকার নেই, যেহেতু বার্তাগুলি কোনও নির্দিষ্ট স্থানে স্থানান্তরিত হয় না এবং কেবল সর্বোত্তম প্রচেষ্টা ভিত্তিতে সরবরাহ করা প্রয়োজন। নোডগুলি চলে যেতে এবং ইচ্ছামতো অন্তর্জালটিতে পুনরায় যোগদান করতে পারে, কাজের প্রমাণ শৃঙ্খলা গ্রহণ করার পরে যা ঘটেছিল তার প্রমাণ হিসাবে গ্রহণ করে। তারা তাদের সিপিইউ শক্তি দিয়ে ভোট দেয়, বৈধ ব্লকগুলিকে প্রসারিত করে কাজ করার মাধ্যমে তাদের গ্রহণযোগ্যতা প্রকাশ করে এবং তাদের উপর কাজ করতে অস্বীকার করে অবৈধ ব্লকগুলিকে প্রত্যাখ্যান করে। যে কোনও প্রয়োজনীয় বিধি এবং প্রণোদনা এই ঐক্যমত্য প্রক্রিয়া দ্বারা প্রয়োগ করা যেতে পারে।

তথ্যসূত্র

- [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.