Lietuvos matematikos rinkinys
Proc. of the Lithuanian Mathematical Society, Ser. A
DOI: 10.15388/LMR.A.2016.01

ISSN 0132-2818
Vol. **57**, 2016
pages 1–6

Bitcoin – a way to reach consensus in a completely decentralized manner

Rytis Bieliauskas[1], **Eugenijus Paliokas**[2]

[1] *UAB „Virtualios Valiutos" (CoinGate)*
Ukmergės str. 315B, LT-06306 Vilnius, Lithuania
[2] *Faculty of Fundamental Sciences, Vilnius Gediminas Technical University*
Saulėtekio al. 11, LT-10223 Vilnius, Lithuania
E-mail: rytis@coingate.com, eugenijus.paliokas@vgtu.lt

Abstract. Bitcoin is a digital currency currently being legalized throughout the European Union [2], whose operating principles were published publicly [5], but not in scientific or mathematical sources. The goal of this report is to encourage discussions about decentralization and security of the Bitcoin system, as well as about reasonableness of the Bitcoin network fees. Bitcoin is a fully decentralized peer-to-peer electronic currency system, which lets its users to send transactions directly from one user to another, without any third-parties. Electronic signature ensures that transaction is sent by the person who owns the money, but the main problem of such a system is to ensure, without any third-parties, that the same money could not be spent twice. This problem in the Bitcoin system is solved using a peer-to-peer network. The Bitcoin network timestamps all transactions, by grouping them to an ongoing chain of transaction blocks, where each block must have a hash (SHA256) result which would meet certain conditions, thus ensuring that in order to cancel or modify a past transaction, one would need to find more hashes which meet the required conditions than the whole Bitcoin network combined since the time of transaction. This allows users to leave and rejoin the network at will, and always be sure which transaction history is the correct one.

Keywords: Bitcoin, bitcoins, blockchain, SHA256, proof of work, ECDSA.

Introduction

The principle of the Bitcoin system is not actually new – a very similar system was used several hundred years ago by the people on the island of Yap. They used huge stones (called "Rai stones") as currency [3]. Here is the explanation how it worked and a comparison to how the Bitcoin system works:

1 Rai stones

The stones themselves had no practical use, and were used only as tokens (system would have still worked if the stones did not exist). A transaction was done by publicly announcing that a particular stone (that you own) now belongs to someone else instead of you. Buying an item with these stones was as easy as saying it no longer belongs to you. All transactions were recorded in the oral history. Ownership of stones relied on mental accounting of ownership and no physical movement of stones was required. This is best illustrated by an event when one of the stones was nevertheless being transported to another place by ship. There was a storm, and the ship sank together with the stone. This sunken stone was still used for transactions for decades to come, because everyone knew that such stone existed and who it belonged to.

In such a system counterfeiting was impossible, because even if someone managed to dig out a new stone for themselves, no one would accept this stone for transactions, because no one would know about it – the stone would have no public history.

Direct theft was impossible, because even if the stone was stolen, it would simply be treated like the sunken stone was treated – everyone would still know who owns that stone. Theft was only possible through deceit or extortion.

Using Rai stones, the problem of spending the same stone twice (double-spending) was prevented by the majority vote, on the condition that 1 human = 1 vote. It worked, because creating new humans, and therefore new votes, is expensive and takes a long time.

2 Bitcoin

The bitcoins themselves exist only as tokens – as entries in a distributed global database of all Bitcoin transactions (called "the Blockchain"), and not as files, numbers, or other kind intangible objects. Every full node in the Bitcoin network has a copy of the Blockchain. A Bitcoin transaction is done by publicly announcing that these particular bitcoins (that you own) now belong to someone else instead of you and signing that message with your private key (electronic signature). Anyone can generate a public key/private key pair using the rules of the Bitcoin protocol (this can be done even offline), which allows users to receive and send Bitcoin transactions: a hash of the public key serves as an address to which the user can receive transactions and the private key allows the user to sign transactions from the address derived from the associated public key. All transactions are forever recorded in the Blockchain and ownership of bitcoins relies on history of ownership recorded in the Blockchain [8].

In such a system counterfeiting is impossible, because while anyone could "create" millions of bitcoins for themselves in their own copy the Blockchain, no one else would accept these bitcoins for transactions, because no one else would know about them – they would have no public history. This ensures that bitcoins can not be "multiplied" or "printed" at will like traditional currencies. This also means that bitcoins are not based on debt, like traditional currencies are.

Direct theft is impossible, as long as Elliptic Curve Digital Signature Algorithm (ECDSA) [6] is secure. Theft is only possible from a particular user, by stealing their private key used to sign transactions, or by a method of deception, when a used would entrust their bitcoins to a third-party for safe-keeping and that third-party would not give them back.

However, there is a problem which did not exist in the Rai stones system – it is very easy and cheap to create thousands of virtual computers, which would be indistinguishable from a real computer, so the method of preventing double-spending by the majority vote, on the condition that 1 computer = 1 vote, does not work.

3 Double-spending problem

This problem can be expressed in the system of Rai stones like this – imagine that a wizard had power to create “phantom” humans, which looked and talked like real humans, but could not perform any real work. If this were true, then 1 human = 1 vote would no longer work. The solution to this problem would be to use proof of work for voting, for example 1 cubic meter ditch dug up = 1 vote. The results of the work would only be used to prove that the work was done, and would be completely useless for any other purpose.

This raises another problem – why would anyone waste their time to dig up useless ditches? The solution – after each agreed period of time a lottery happens, where the winner receives permission to create a new Rai stone for themselves, of which they become the owner. The chance to win the lottery is directly proportional to the amount of work done. This also solves the problem of how (by what rules) new Rai stones should be created and distributed.

Getting back to the problem of double-spending in the Bitcoin system, it is solved in a very similar way. While it is very easy and cheap to create thousands of virtual computers which are indistinguishable from real computers, these virtual computers can not perform more work (calculations) than the real computer used to simulate them. Therefore, the solution is to use proof of work for voting, by the principle that 1 performed calculation = 1 vote. The results of the calculations are only used to prove that the calculations were done, and are completely useless for any other purpose.

This raises the same problem as in the example with Rai stones – why would anyone waste their computer resources to perform worthless calculations? The solution is the same as before – after each agreed period of time a lottery should happen, where the winner receives permission to create new bitcoins for themselves, of which they become the owner. The chance to win the lottery should be directly proportional to the amount of work done. This would also solve the problem of how (by what rules) new bitcoins should be created and distributed.

However, this raises two new problems:

1. How can someone prove that they performed a certain number of calculations?
2. How to pick a lottery winner in a decentralized manner?

The solution to both of these problems is to use a one-way algorithm, with a task to find an answer which would satisfy the required conditions. In the Bitcoin system SHA256 algorithm [7] is used, with a condition to calculate such a hash of a transaction block, that a specific number of first bits in the hash would be all zeros (in the Bitcoin system this process is called “mining”). As of today, the only way to solve such a task is to try to calculate the hash by changing a random nonce, until an answer which fulfills the conditions is found (brute-force). When the answer is found, anyone can quickly and easily check if it is correct. The answer itself is useless, but it is valuable to the finder, because it gives them permission to create a new batch of bitcoins for themselves [4].

4 Bitcoin “mining”

For the input into SHA256 algorithm, miners take a block of unconfirmed Bitcoin transactions, a reference to a previous block, a timestamp, and a random nonce. Each

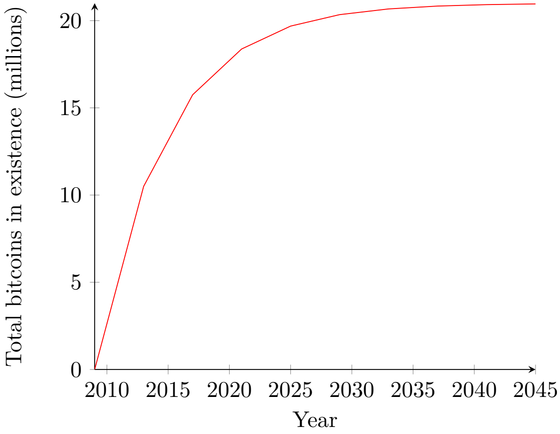

Fig. 1.

miner also creates a transaction of n bitcoins "from nowhere" to their own Bitcoin address, and adds it to the block which hash they are calculating. The result (the hash which meets the required conditions) itself is worthless, but it is valuable to its finder, because only their block becomes valid, and therefore only their transaction "creating" bitcoins becomes valid. n is defined in the operating principles of the Bitcoin system and in the programming code of the Bitcoin protocol and is equal to 50, but each 210000 blocks (about 4 years) is reduced by half. This ensures that the total number of bitcoins in existence is based on geometrical progression and can never be higher than 21000000 [1]. Each bitcoin can be subdivided into 100000000 smaller parts.

Each 2016 blocks (about 2 weeks) the system automatically adjusts the required number of zeros in front of the hash in such a way, that the valid hashes would be found every 10 minutes on average. If during the last 2016 blocks, hashes having the required number of zeros in front of them were generated slower than 10 minutes on average, then the required number of zeros in front of a hash is reduced, if they were generated faster – the required number of zeros in front of a hash is increased.

The miner who finds the hash of a transaction block, which meets the required conditions, receives not only the newly created bitcoins, but also the transaction fees of all Bitcoin transactions in that block. The transaction fee can be added by the sender of each transaction, and is completely voluntary – it can range from 0 to any amount of bitcoins. Because the size of the transaction block is limited, the miners prioritize transactions with highest added fees. At this time, the main part of the miners' earnings comes from the newly created bitcoins, but as the amount of new bitcoins gets halved every 4 years, in the future transaction fees will make the bigger part of miners' earnings, while finally will become the main (and practically only) source of the miners' earnings.

However, this describes only how the system is working at this date – there are various proposals on how to scale the Bitcoin system further, and these improvements to the system may change how many transactions fit in a block or even how the transactions are confirmed.

Conclusion

The scientific foundations in both finance and economics were usually laid down by mathematicians, therefore we would like to encourage debate regarding these questions in the mathematical community:

Is it possible to scale the Bitcoin system to encompass all transactions in the world, while keeping it decentralized?

Is Bitcoin system really secure? Is there any way it could be destroyed or “hacked”?

Will there be a smooth transition to a state where the most earnings of the miners are made from the Bitcoin transaction fees and how will it affect the average fee of a Bitcoin transaction.

References

[1] A.M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O’Reilly Media, 1st edition, 2014.

[2] Court of Justice of the European Union. Press release no. 128/15. Available from Internet: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf, 2015. Accessed: 2016-06-15.

[3] M. Friedman. *The Island of Stone Money.* Working papers in economics, No. e-91-3, 1991.

[4] D. Lee and K. Chuen. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.* Academic Press, 1st edition, 2015.

[5] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. Available from Internet: https://bitcoin.org/bitcoin.pdf, 2008. Accessed: 2016-06-15.

[6] National Institute of Standards and Technology. *Federal Information Processing Standards Publication Digital Signature Standard (DSS).* Available from Internet: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf, 2013. Accessed: 2016-06-16.

[7] National Institute of Standards and Technology. *Federal Information Processing Standards Publication Secure Hash Standard (SHS).* Available from Internet: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf, 2015. Accessed: 2016-06-16.

[8] P. Vigna and M.J. Casey. *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order.* St. Martin’s Press, 2015.

REZIUMĖ

Bitcoin – priemonė konsensusui pilnai decentralizuotoje sistemoje pasiekti

R. Bieliauskas, E. Paliokas

Bitkoinai – pastaraisiais mėnesiais Europos Sąjungoje legalizuojama virtuali valiuta, kurios veikimo principai viešai paskelbti, bet “nemoksliniuose”, taigi, “nematematiniuose” internetiniuose šaltiniuose. Šiuo pranešimu siekiama sužadinti matematikų bendruomenės diskusiją pranešimo pavadinime deklaruojamu, taip pat ir kitais išties svarbiais – šios tarpusavio atsiskaitymų sistemos patikimumo ir jos naudotojo mokesčio pagrįstumo – klausimais. Bitcoin – tai pilnai decentralizuota (peer-to-peer) elektroninių pinigų sistema, kuri leidžia siųsti transakcijas internetu tiesiai iš vieno vartotojo kitam, be jokių tarpininkų. Elektroninis parašas užtikrina, kad transakciją siunčia tikrai tas asmuo, kuriam priklauso siunčiami pinigai, tačiau pagrindinė tokios sistemos problema yra užtikrinimas, kad tų pačių pinigų negalima būtų išleisti du kartus, tam neįvedant jokių trečiųjų šalių (tarpininkų). Ši problema Bitcoin sistemoje išspręsta panaudojant peer-to-peer tinklą. Tinklas sužymi visas transakcijas laiko žyma, sudėdamas jas į transakcijų blokų grandinę, kurioje kiekvienas blokas privalo turėti tam tikras sąlygas atitinkantį maišos funkcijos (SHA256) rezultatą. Tokiu būdu užtikrinama, kad norint pakeisti praeityje įvykusias transakcijas, reikėtų surasti daugiau sąlygas atitinkančių SHA256 rezultatų, nei nuo transakcijos patvirtinimo laiko jų surado visas Bitcoin tinklas kartu sudėjus. Tai leidžia vartotojams, bet kada atsijungti bei prisijungti prie tinklo, ir visada žinoti, kuri transakcijų istorija yra teisinga.

Raktiniai žodžiai: Bitcoin, bitkoinai, blockchain, SHA256, atlikto darbo įrodymas, ECDSA.