Available online at www.sciencedirect.com

ScienceDirect

Current Opinion in Environmental Sustainability

Sustainability of bitcoin and blockchains

Harald Vranken[1,2]

Bitcoin is an electronic currency that has become increasingly popular since its introduction in 2008. Transactions in the bitcoin system are stored in a public transaction ledger ('the blockchain'), which is stored in a decentralized, peer-to-peer network. Bitcoin provides decentralized currency issuance and transaction clearance. The security of the blockchain depends on a compute-intensive algorithm for bitcoin mining, which prevents double spending of bitcoins and tampering with confirmed transactions. This 'proof-of-work' algorithm is energy demanding. How much energy is actually consumed, is subject of debate. We argue that this energy consumption currently is in the range of 100–500 MW. We discuss the developments in bitcoin mining hardware. We also briefly outline alternative schemes that are less energy demanding. We finally look at other blockchain applications, and argue that also here energy consumption is not of primary concern.

Addresses
[1] Open University of the Netherlands, P.O. Box 2960, 6401 DL Heerlen, The Netherlands
[2] Radboud University, P.O. Box 9010, 6500 GL Nijmegen, The Netherlands

Corresponding author: Vranken, Harald (harald.vranken@ou.nl)

Current Opinion in Environmental Sustainability 2017, **28**:xx-yy

This review comes from a themed issue on **Sustainability governance and transformation**

Edited by **Carolien Kroeze**, **Harald Vranken**, **Marjolein Caniels** and **Dave Huitema**

Received: 10 February 2017; Accepted: 23 April 2017

http://dx.doi.org/10.1016/j.cosust.2017.04.011

Introduction

People have been using currencies for thousands of years. Initially, currencies were minted directly from precious metals such as gold and silver. Later on, paper money was introduced and the face value of cash was decoupled from its nominal value, but currencies were still backed up by gold depositories. Nowadays, fiat currencies are allowed to float freely, only backed up by the faith and credit of the states that issue them. Bitcoin is a decentralized system that attempts to overcome the weaknesses of fiat and gold-based currencies. It is not governed by central authorities, such as governments or central banks, and intermediaries for currency issuance or settlement and validation of transactions, and can provide lower transaction fees for payments [1,2]. The Bitcoin Foundation provides some centralized governance for standardization, protection and promotion of bitcoin, but it does not act as a central bank and does not issue currency [3].

Bitcoin was introduced in 2008 by Satoshi Nakamoto [4], which is a pseudonym of an author or group of authors whose identity is covered in mysteries. The term 'Bitcoin' often refers to the system, while the term 'bitcoin' or BTC refers to the unit of currency. In this paper, for simplicity we just use the term bitcoin. Bitcoin is an electronic, virtual currency that has no physical representation such as coins or banknotes. The bitcoin ecosystem is a network of users that communicate with each other using the bitcoin protocol via the Internet. The bitcoin protocol is available as an open source software application and allows users to store and transfer bitcoins for purchasing and selling goods, or to exchange bitcoins for other currencies. The issuance of bitcoins takes places in the network while handling transactions in a process called bitcoin mining. The bitcoin network started in 2009 and ever since bitcoin has been the most popular decentralized currency. In January 2017 there were 16 million bitcoins in circulation with a total value of roughly 16 billion US dollars, although the exchange rate of bitcoins has shown very large fluctuations.

Both scientific and professional literature on digital currencies, with bitcoin as prime example, is extensive. Some provide gentle, general introductions to the technology applied in bitcoin (e.g. [5]), while others provide more detailed overviews of the technical operation of bitcoin (e.g. [6•,7•,8]) as well as economical and financial aspects (e.g. [9•]).

In this review paper we provide an overview and synthesis of recent literature published in the last two years that addresses the sustainability of bitcoin. The sustainability of bitcoin is depending on a mix of environmental [10••,11••], economical [1,12], financial [2,13,14] and ethical [15] aspects. Bitcoin may pose risks to the stability of the current financial system, while also lack of controls over bitcoin exchanges and the volatility of the bitcoin currency raises concerns. Our focus in this review is on sustainability in the context of environmental and economical aspects. We try to answer the question whether the bitcoin system is sustainable given the energy consumption required for bitcoin mining, which has been

subject of debate in the last few years. The contributions of this paper are: firstly, to synthesize and critically assess the viewpoints in scientific literature; and finally, to argue that the energy consumption of the bitcoin system is not excessive, which stands in contrast to the public opinion that bitcoin mining is a gross waste of energy. We explore four subquestions: What factors play a role in the energy consumption of bitcoin mining, how large is this energy consumption, does this impede sustainability, and if so are there alternatives that can reduce energy consumption? In the following sections we outline the basic operation of the bitcoin system, we summarize trends in the hardware used for bitcoin mining, we discuss the energy footprint of bitcoin mining, we present some of the alternatives that have been proposed to reduce energy consumption, and we briefly discuss other applications of the blockchain technology that is at the basis of the bitcoin system.

Overview of the bitcoin system

The bitcoin system is a distributed, peer-to-peer network. There is no central server or point of control, and all nodes in the network are equal peers. Each transaction to transfer an amount of bitcoins among users is transmitted to the bitcoin network where it is stored in a distributed transaction ledger, the blockchain. The blockchain contains the entire history of bitcoin transactions. Each node in the network stores a (complete or partial) copy of the blockchain. New transactions are propagated rapidly across the nodes in the network. A transaction is in fact a transfer from a source of funds (called an input) to a destination (called an output). Transaction inputs and outputs are not related to accounts or balances: an input is a reference to an unspent transaction output of the sender in a previous transaction. Before forwarding a transaction to its neighbors, each node first verifies the transaction, which includes checking the syntax and structure, and whether it is a valid transfer of an amount of yet unspent transaction outputs. Each node independently verifies the transactions received, propagates valid transactions, and builds a pool of valid transactions. The valid transactions are added to the blockchain in a process called bitcoin mining. Each node collects a number of valid transactions into a block and tries to compute a cryptographic hash of the block that meets certain constraints (based on the ideas of Hashcash [16]). A cryptographic hash is a kind of checksum for the block, that is one-way (meaning that it is easy to compute a hash of a given block, but difficult to compute a block that matches a given hash) and collision resistant (meaning that it is difficult to find two blocks that yield the same hash). Finding a hash that meets the constraints imposed by the bitcoin system, is a compute-intensive task that can be executed only by brute-force trying. This implies a race among the nodes in the network to find a valid hash as quickly as possible. The first node that finds such a hash, wins the block, which means that this block is added to the blockchain and propagated to the network. Although computing a valid hash is difficult, verifying whether a hash is valid is easy and hence each node that receives the block can quickly identify whether the new block is valid. When a node receives a new valid block, it stops the mining process for the current block and starts mining for a new block. The node that won the block receives a block reward, which is a fixed amount of new bitcoins. Hence, the issuance of bitcoins (minting) is done during the bitcoin mining process. The node that won the block also receives the transaction fees for every transaction included in the block. Every 10 min on average, a node is able to mine a new block. It can be the case that multiple nodes simultaneously generate a valid block, which causes that multiple versions of the blockchain ('forks') occur temporarily. Forks are resolved as soon as one of the forks contains more blocks. The computations to find and verify a cryptographic hash of a block during bitcoin mining allows the bitcoin network to gain consensus about the state of transactions. This elegantly solves the issue of double spending and hence an amount of bitcoins cannot be spent twice. The bitcoin mining process decentralizes the currency issuance and the transaction clearing normally done by central banks and clearinghouses. In economics bitcoin is considered as money to some extent, since it offers a unit of account, means of payment, and store of value [1,3]. It can even be argued that bitcoin has an intrinsic value due to the computational effort for bitcoin mining [17].

Each block does not only contain transactions, but also the hash of the previously accepted block in the blockchain. Hence, the blocks in the blockchain are linked to each other: they form a chain of blocks, thence the term 'blockchain'. This provides security, as a node with malicious intent cannot easily replace or modify an already accepted transaction or add a new transaction to an already accepted block, since this would require to redo the computations to find a valid hash for the modified block. And since new blocks are continuously added to the blockchain, each block linking to the previous block, also the hashes of the newly added blocks would have to be recomputed.

The initial block reward was set to 50 BTC. The reward is halved every 210 000 blocks, which is approximately every four years. This will continue until 2140 when the mining reward drops below 10^{-8} BTC, which is the minimal unit of bitcoin also known as satoshi. Afterwards, transaction fees will provide the necessary incentive to continue mining of new blocks [18]. The bitcoin protocol includes an algorithm to regulate that on average every 10 min a new block is mined, by adjusting the difficulty to find a valid hash. This is required to keep up with the improvements in the performance of mining hardware which allows bitcoin miners to compute more and more hashes per second.