Critical mining
blockchain and bitcoin in contemporary art

Martín Nadal & César Escudero Andaluz.

Abstract
The bitcoin was originally conceived as an electronic decentralized system for capital transactions. Each node (user) has the same opportunities to get a reward when validating a collection of transactions (block). In the last years, this system has triggered a competitive struggle in which computing power is the most important variable for earning bitcoins. This involves the use of large computers farms spending physical and environmental resources, creating a struggle that benefits only the owner of the most powerful and efficient technology.
This text examines different examples of artworks based on blockchain technology, in particularly how artistic practices are able to explore critically bitcoin mining processes and which are the factors provoking a suspicion that bitcoin is dangerous for society. The objective is to connect aesthetic experiences, creative practices and artistic products, analyzing four different spheres; technical, ideological, ecological, and economical. Practically the essay introduces three artworks *Bittercoin - the worst miner ever, Bitcoin of things (BoTs)* and *Bitcoin traces*, developed between 2015 to 2017, examples helping to expand frontiers, opening a dialog, and tracing their historical influences in contemporary and critical art.

Keywords: *bitcoins, blockchain, economy, art, ecology, ideology, technology*

Introduction

A Cryptocurrency is a medium for exchanging digital information conceived as a payment technology. In layman's terms, a cryptocurrency is electricity converted into lines of code with monetary value following algorithmic rules to maintain a fixed production rate. Following previous digital cash technologies[1] such as *eCash*, the bitcoin appeared in 2009[2] by a pseudonymous developer named Satoshi Nakamoto. Bitcoin is based on the proof-of-work system, using a set of cryptographic hash functions called SHA-256 designed by the U.S National Security Agency.

[1] David Chaum, wrote the first paper that outlined an anonymous payment system by using blind signatures.

[2] The first paper was self-published in 2008 by anonymous person (or people) named Satoshi Nakamoto.

The only way to generate bitcoins is through a process called mining[3]. Mining is a calculation process to confirm transactions realized by bitcoin users and used to secure the transactions and to control the creation of new coins, writing them into a public ledger of past transactions called the blockchain. A block in the blockchain is where the most recent bitcoin transactions are stored.

The primary purpose of mining is to allow bitcoin nodes to reach a secure, tamper-resistant consensus. When a miner discovers a new block, they receive a certain number of bitcoins. Currently a block contains 12.5 BTC, (This number changes throughout time and gets smaller by a factor of 0.5 every four years). Bitcoin mining is a giant lottery where miners compete against other miners on the network to earn bitcoins.

Bitcoin Criticism

Technically, a bitcoin miner is a computer specifically designed to solve problems according to the proof of work algorithm (PoW). Proof of work is a measure that is used to prevent unwanted behaviors, abuse or misuse in a system, using special software to solve it mathematically. This problem must have the characteristic of being very difficult to solve, but with a very simple way to verify. This result can be easily checked by any other machine in the network. The type of PoW used by bitcoin consists in solution - verification. This process requires work and processing time from the service requester. Currently bitcoin miners use highly specialized chips called ASICs (Application Specific Integrated Circuits).

The PoW has several consequences, for example, the difficulty increases every two weeks based on the time that the network takes to solve it, and miners have to be constantly upgraded. Bitcoin mining has become hardware intense and miners compete for the limited supply of blocks, working for months without finding a block and receiving any reward for their mining efforts. Therefore, as it is an expensive process, most individual miners join a so-called mining pool. Pooled mining is comprised of different miners contributing their processing power to calculate a block together. One of the mining pools you can connect to is BitMinter for example. Bitcoin farmers are located in factories, making it hard to track their numbers, with 70% of the total operating autonomously in China. In the last three years the computing capacity of mining pools has multiplied by 4000, which is equivalent to a network 43,000 times more powerful than the world's top 500 supercomputers combined" (Reuters, 2016). Speaking metaphorically, the network every 6 seconds calculate as many hashes as there are sand grains of the planet Earth.
Later Cryptocurrencies such as PeerCoin or Ethereum use the Proof of Stake (PoS).
PoS, addresses the high energy consumption by using an only client software on a computer, spending 70% less that the bitcoin. (PoS). The PoS aim is to avoid the "tragedy of the

---

[3] Mining process. The objective in the mining process is to calculate the hash function value of a concatenated Blockheader with a random number (nonce) and to obtain, as a result, a hash value starting with a sufficient number of zeros. Obtaining this number, the miner gets a reward of 12,5 BTC. BLOCKHEADER + nonce = hash.
To mine a new block it is necessary to know the hash function of the previous block and the unconfirmed transactions. It is from these transactions where the Merkleroot is generated, with the Merkleroot and the previous block the Blockheader is generated. The Blockheader hash is the main way of identifying a block in the blockchain. It is An 80- byte header belonging to a single block which is hashed repeatedly to create the proof of work. The Blockheader is a set of structured data representing the block with all its transactions using the Merkletree. The hash of the previous block is included to ensure that this block was generated from the previous one. So if someone wanted to modify a block, they would have to rewrite all the previous ones. The blockheader hash is calculated by running the blockheader through the SHA256 algorithm twice. It is calculated by each node as part of the verification process of each block.

commons[4]". It works by requesting evidence of possession of coins. The advantage of this approach is that mining is less profitable reducing competition and energy use.

2. Environmentally, it cannot be estimated how many miners are actually mining bitcoins, but the energy consumed in farms is prominent. A paper from 2015 estimated that the mining network at the time consumed about the same amount of electricity as Ireland (Malone and O'Dwyer). Mining is only likely to be profitable if you pay less than about 5 cents per kWh for electricity. Some bitcoin farmers have been obliged, in order to continue subsisting, to migrate elsewhere in search of cheaper energy. To cite a specific example, one farm still operating has been told to have 10,000 S3 mining units ("My Life Inside a Remote Chinese Bitcoin Mine"). The Antminer S3 is able to produce 441 Gigahashes per second and consumes 800 Watts per Terahash: that is roughly 4761 Watts in a day, for just one unit. A farm with 10,000 of these units would consume 47,616 Kilowatts a day. A farmer can spend approximately 60,000$ of energy per month (Velasco González, 2016).

3. Economically, the money works according to three characteristics: exchange, accounting unit, and value storage. Bitcoin works most of the time as a speculative investment rather than as a currency.
The bitcoin currency transactions[5] are performed between two users through a virtual Wallet and stored in the blockchain. Each block is processed every ten minutes and limited to a Megabyte, a single block can store an amount of one thousand to two thousand transactions, this restriction provokes problems of scalability and limits the rate of transactions the network can handle, e.g. Visa can manage 250.000 payments every ten minutes. Which translates in an increased price paid in each transaction when the demand rises, breaking down one of the main ideas of bitcoin; to do transferences of capital cheaper than ordinary transferences.
In terms of anonymity, bitcoin transactions can be tracked since they are publicly archived in the blockchain. CoinJoin is an anonymization method for bitcoin transactions proposed by Gregory Maxwell that works by grouping a set of payments in one transaction making impossible to establish a correspondence between the parties of a particular transaction.
The "Silk Road" was a popular black marketplace that operated in the Deepweb from 2011 until it founder Ross William was arrested in 2013, played an important role in the use and acceptance of bitcoin. But It's not all bad though, the bitcoin and blockchain have socially beneficial effects against economical censorships, an example is the well-known blocking of Wikileaks donations using Paypal, Mastercard, Visa, Bank America and Western Union which was bypassed through the use of bitcoin.

4. Ideologically, to understand bitcoin is complex, but no less complex than the current monetary system in which we are immersed. Probably this economic normalization prevents us from considering what entities, mechanisms, and strategies really govern the creation, use and control of capital. "Bitcoin is fundamentally an alternative to the corrupt and failed

---

[4] Understood as a situation in which several individuals, motivated only by self-interest and acting independently but rationally, end up destroying a limited shared resource (Blockchain), although neither of them wants such destruction to happen. The advantages of this approach is that mining is less profitable, reducing competition and energy use. Also the 51% attack is less likely because in this system the attacker should own 51% of the total number of Bitcoins.

[5] The first Bitcoin real word transaction took place in May of 2010 when Laszlo Hanyecz, a programmer living in Florida, sent 10,000BTC to a volunteer in the United Kingdom, who then ordered two pizzas for Hanyecz, which cost him 25 USD [5]. Today, 10,000 BTC have value of over 10 million USD. (Vavrinec Cermak, 2017).

banking industry, the biggest driver of which is money creation" (Daniel Krawisz, 2014).

Bitcoin has an ideology where the government and current banking systems have no jurisprudence. Bitcoin skips democratic vigilance without any role of governments, this means, that capital has all the power. This also reveals the deeper reason why algorithms are an essential part of the process of common money creation, but those algorithms also have politics. According to Tiziana Terranova, current attempts to develop new kinds of cryptocurrencies must be judged, valued and rethought.

We venerate the bitcoin decentralization, but in reality there are power relations and vulnerability weaknesses. One is the so-called *51% attack,* if a pool grows and gets more that 50% of the hash power could potentially allow double expending and prevent transaction confirmations.

4. Concusion

Bitcoin can be understood as a first implementation, an exercise in progress where developers, hackers, activists, banks, governments, artists and researchers pay attention, investing efforts to create a reliable system based on maths and algorithms for peer to peer digital transactions. Bitcoin and especially blockchain can have socially beneficial effects helping to fight against economical censorships.

On the other hand, bitcoin has an ideology by virtue of the fact that the government and current banking have no jurisprudence over it. Bitcoin skips democratic vigilance avoiding the role of governments, which means that capital has all the power. Algorithms are an essential part of the process of money creation. Cryptocurrencies must be questioned! They hide problems concerning the limited rate of transactions, power relations, vulnerability errors, problems of scalability and the so-called *51% Attack* that would allow the double spending of coins and the ability to prevent transaction confirmations. Another consequence derived from the bitcoins mining process lies directly in the calculation power needed to obtain bitcoins, and the economical investment that miners realize on equipment and electricity.

Artistic examples

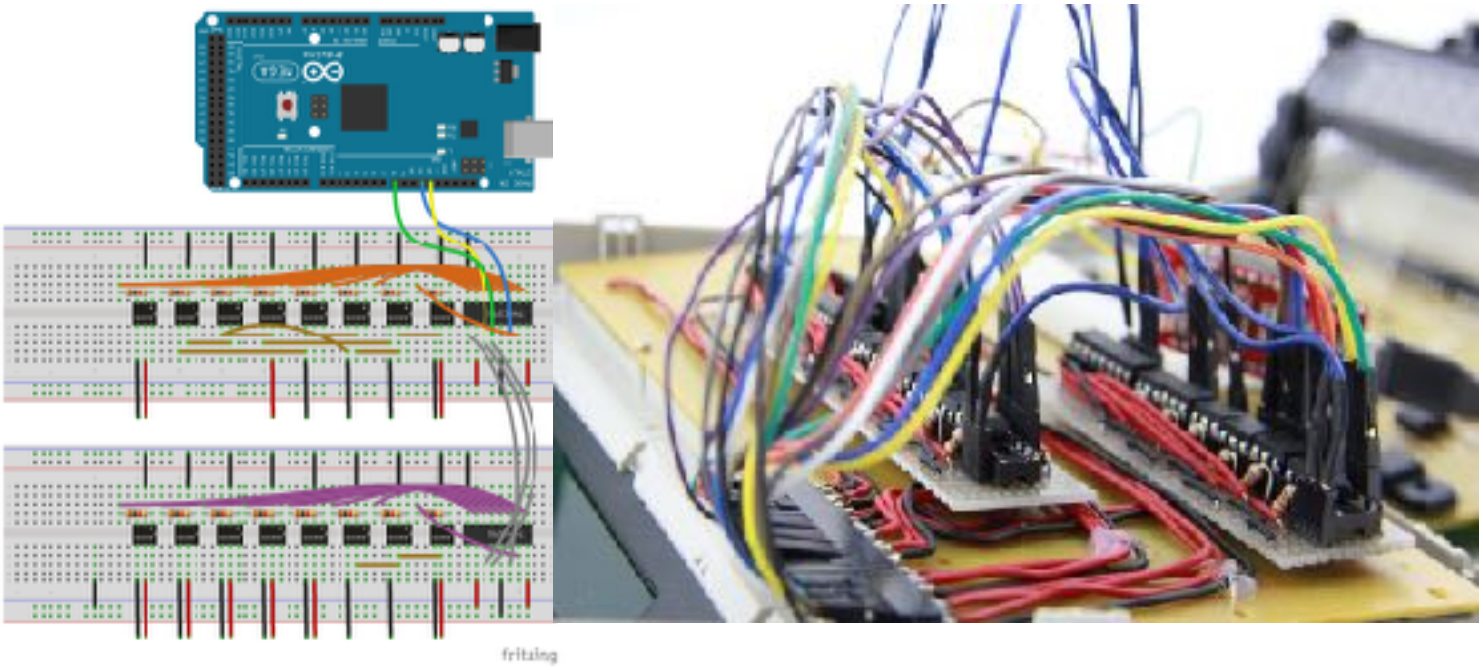
Bittercoin, *the worst miner ever*

Bitttercoin[6] is an old calculator machine hacked to be used as a miner validating the pending bitcoin transactions in the blockchain. *Bittercoin* combines Internet of Things (IoT), media archaeology and economics. It works as the most basic computer, increasing the time needed to produce bitcoins to almost an eternity. The operations are displayed on the calculator screen and printed afterwards.
For the duration of its exhibition period it seeks to produce money insistently and using an economic system wholly different from the traditional art market. Paper accumulates around the machine making visible the amount of calculation required, as well as, the natural resources expended in the process, often covering the whole room and the calculator itself. *Bittercoin* talks about the effort and the working time expended that is conditioned by technological devices. *Bittercoin* is a fully functional miner that connects to blockchain. Although it is very unlikely, in the event of successfully mining a block, the *nonce* would be sent back to the server, entering the corresponding bitcoins of the reward to our bitcoin Wallet.
Originally, the calculator consumes 80mA, Watts 220V * 0.08A = 17.6W and 10m of paper per hour.

6 Bittercoin, *the worst miner ever*. *WEB*/INFO: https://escuderoandaluz.com/2016/03/03/bittercoin/ & http://spectrum.muimota.net/bittercoin.html

Bittercoin, the worst miner ever, Ars Electronica 2016. Images by Patricia Cadavid

Inside the calculator, there is embedded a bluetooth microcontroller compatible with Arduino. This microcontroller allows the control of the calculator keys remotely by means of a mobile phone. Thephone functions are three: to connect the calculator to the blockchain, get the blockheader, and send it to the calculator. Once it is received the calculator adds a random *nonce* in order to begin the verification process. The verification process consists of a double SHA256 algorithm, which is displayed by the calculator screen, printing the intermediate steps of its calculation. If the calculator finds a nonce that produces a hash smaller than the blockchain target hash, a new block would have been successfully mined.



Bittercoin, the worst miner ever, Circuit assembly.

The connection with the blockchain is made using a phone for two reasons: to have a visual output of the calculation process and to be able to exhibit the piece using the 3G Wi-Fi connections. A goal of the whole project is to maintain the original calculator aesthetic. In *Bittercoin*, the SHA256 verification process is made visible in the calculator display, printing afterwards the intermediate values generated in each of the 64 rounds (A and E) of the second verification.

Calculator printing.

How is it connected to blockchain? The blockchain is a distributed file, in April 2017 it was 250Gb in size, growing by more than 100 Mb per day. The first version of *Bittercoin* used a node running on our server, *Bittercoin* could connect to this server receiving a blockheader to sign. In the last version *Bittercoin* uses a solo mining pool. This kind of pool serves updated blockheaders, and if the block is mined they receive 0.5% of the Coinbase transaction plus fees. The goal of this approach was to simplify the project and not force us to have a full node server running. A standard mining pool protocol called *Stratum* is used. It is based on Json + tcp and as *proof of concept* we developed miniminer.py, a minimum client that is also used in the project *BoT*, (Bitcoin of Things).

```
merkle_root = ''.join([merkle_root[i]+merkle_root[i+1] for i in range(0,len(merkle_root),2)][::-1])

print 'merkle_root:{}\n'.format(merkle_root)

blockheader = version + prevhash + merkle_root + nbits + ntime + nonce +\
    '000000800000000000000000000000000000000000000000000000000000000000000000000000000000000080020000'

print 'blockheader:\n{}\n'.format(blockheader)

hash = hashlib.sha256(hashlib.sha256(binascii.unhexlify(blockheader)).digest()).digest()
hash = binascii.hexlify(hash)
print 'hash: {}'.format(hash)

if hash < target :
    print 'success!!'
    payload = '{"params": [" +address+'", "'+job_id+'", "'+extranonce2 \
        +'", "'+ntime+'", "'+nonce+'"], "id": 1, "method": "mining.submit"}\n'
    sock.sendall(payload)
    print sock.recv(1024)
else:
    print 'failed mine, hash is greater than target'
```

miniminer.py POW verification.

Bitcoin is designed to verify a block and generate a Coinbase transaction approximately every 10 mins. In order to have a chance we designed *Bittercoin* to be able to verify one block every 10 mins.

Bitcoin of things (BoTs)

Based on *Bittercoin, the worst miner ever,* this project crosses the boundary of the exhibition space, to hang out in a didactic workshop where participants get information about Media Art, Digital Culture, Critical Economy, Electronics and Internet of Things (IoT).

Bitcoin of Things (BoT), Bitcoin of Things assembly KIT.

Theoretically, it introduces concepts, art-works and books in order to understand the bitcoin and blockchain world. Practically it proposes to work with a basic electronic circuit, welding and microcontrollers building a playful bitcoin miner. The objective is to transform daily life objects (e.g. Maracas, hammers or salt shakers) into bitcoin miners able to connect to the blockchain, mine the latest block, and if successful get the reward, that in May 2017 is 12.5 BTCs.

Participants build a *BitCoin of Things* (*BoT*) miner combining a Wi-Fi microcontroller and different sensors such as an accelerometer, microphones or buttons, and generating a *nonce* from its readings will try to validate all the blockchain pending transactions. The possibilities are lower, but it decreases the use of energy of the calculation processes making it more sustainable. *BoT* is without any doubt, the lottery with the worst chance of winning.

Finally, the microcontroller is attached to daily life objects, like keyboards, computer mice or salt- shakers, by using them the object can potentially generate big number of bitcoins, playing with the idea of finding the philosopher's stone capable of turning any object into gold (in this case bitcoins).

Bitcoin Traces

Bitcoin Traces data-visualization

Bitcoin Traces, draws an infographic data-visualization of bitcoin transactions from the point when the currency is created by a miner until a particular transaction is made. To make a real world example let's say that a person buys a coffee and he or she pays with a 5 € bill. The 5 € bill was earned in the company he or she works for, which in turn the company earned from their clients, and their clients from other clients, and so on until the money is created by the European Central Bank.

The process begins by picking a transaction as a starting point, analysing which was its source transactions and draws a line for every wallet involved in this transaction. As we progress in time we draw these transactions further away from the center, producing a radial shape. When we reach the transaction where a set of bitcoins were generated we won't be able explore further, so we draw this line in red. In this drawings we can appreciate when the transactions have been processed by anonymization techniques like Coinjoin in the form of darker rings and that most of the bitcoins are mined by few big pools in the form of long red lines.

This kind of analysis wouldn't be possible to do with Euros since we don't have access to the ledger's book as we do in bitcoin and blockchain. What makes bitcoin interesting from an artistic

point of view is that processes like transactions are public while in the wider world economic transactions are only known by governments and banks, and are kept outside the scrutiny of society.

What transpires is a new way of seeing money, deprived of its materiality. Considering money as a network where each node is a good or a service and each edge a transaction with which it participates. These graphs can also be read in the opposite direction. Starting from the 'mined' bitcoins, the origin of which are a set of numbers that have no utility, but by consensus has been decided to give them a value by generating bitcoins and using them as a foundation to build a structure of consumption and exchange.

4. Concusion

Bittercoin, the worst miner ever, Bitcoin of Things and Bitcoin Traces are methods for educating people to understand what happens behind the surface of the first wave of technological advances. They work with the increasing influence of algorithms in the economy, translating them into aesthetic positions and criticism, finding models of anticipation transforming human behaviors in machine decisions. They are focused on showing connections between art, technology and society, and not only training audiences to see concepts inside objects, but also teaching critically and implementing thoughts into the heads of people.

5. References

Golumbia, David. "Bitcoin as Politics: Distributed Right-Wing Extremism," in Lovink, G, N Tkacz and P De Vries (eds) *MoneyLab Reader: An Intervention in Digital Economy* (Amsterdam: Institute of Network Cultures)

Langdon Winner, "Do Artifacts Have Politics?" The MIT Press on behalf of American Academy of Arts & Sciences, 1980.

Malone and O'Dwyer, "Bitcoin Mining and its Energy Footprint," Hamilton Institute National University of Ireland Maynooth, 2014.

Nakamoto, Shatoshi, "Bitcoin: A peer-to-peer electronic cash system", 2008.

Roio, Denis Jaromil, "Bitcoin, the end of the Taboo on Money." Planetary Collegium Ph.D. candidate, M- Node 6. 2013, version 1.0

Terranova, Tiziana. "Red Stack Attack! Algorithms, Capital, and the Automation of the Common". Quaderni di San Precario, 2014, P14.

Vavrinec Cermak, "Can Bitcoin Become a Viable Alternative to Fiat Currencies? An empirical analysis of Bitcoin's volatility based on a GARCH model." Skidmore College, New York, U.S. 2017

Velasco González, Pablo R. "Superabundant design: from waste to control in Bitcoin." PhD candidate, Centre for Interdisciplinary Methodologies, University of Warwick. 2015 URL: http://www.aprja.net/superabundant-design-from-waste-to-control-in-bitcoin-mining/