Dominic Whyte

December 26th, 2015

DomCoin: Ensuring Financial Security in an Online Society

Abstract: In October 2008, Satoshi Nakamoto published a revolutionary paper describing a purely peer-to-peer version of electronic cash known as Bitcoin. [3] Today, with a market cap of almost 6.5 billion US dollars [16], it is as important as ever to consider the social and financial security of this cryptocurrency especially with regards to the new advances in technology that are being made every day. Bearing in mind the release of the National Security Agency's statement in August 2015 raising questions on the Elliptic Curve Cryptography encryption mechanism upon which Bitcoin is based, we suggest implementing a new cryptocurrency DomCoin with another user authentication protocol offering the possible secondary benefit of leaving a more manageable environmental footprint for the years to come. In a globalized world where even our finances are digitalized, it is vital to analyze the ramifications our technologies have on our society and to adapt them to fit the world's ever changing needs.

1 Introduction

Throughout history, the way humans have exchanged goods and services has changed drastically with the arrival of new technologies and the alterations in how societies function. In its most primitive form, currency has taken the form of gold coins that people used to replace bartering, a way of using a substance with an actual value to trade with others. Then, with the need to create a more efficient system, currency developed into the paper bills we still see today: pieces of paper which, until 1971 with the termination of the dollar to gold convertibility by President Nixon [1], were guaranteed to be worth a certain value. Today, over four decades after Nixon's change in policy, our currencies are as abstract as ever. Not only do we have no direct value fixed to the United States Dollar (we simply accept that it can be used as a form of payment), but we also store a significant part of our assets online and in bank databases, with a number next to one's bank account dictating how wealthy one is and what type of lifestyle one can live.

It is in this context that the first cryptocurrencies emerged, notably with Satoshi Nakamoto's paper "Bitcoin: A Peer-to-Peer Electronic Cash System"[1], revolutionizing the way money is stored, spent, and even created. While with Bitcoin the value of each coin is still abstract (people choose to assign coins value by accepting them as a legitimate currency), the cryptocurrency no longer

[1] Interestingly, no single person has proven him or herself to be Satoshi Nakamoto. Many theorize that the paper published in October, 2008 was written by a group of people due to its simple yet elegant perfection [2]

relies on a “trust base model”, a model in which a third party, such as a bank or government, is required to mediate transactions and keep track of balances. There is simultaneously a large degree of transparency, due to all transaction being publicly visible, and a previously inconceivable opportunity for anonymity, stemming from the fact that any person can create an “account” without disclosing their private details [3]. How, however, does a currency with no mediator not spiral into anarchy and chaos? Does the currency need to adapt in a society where advances in technology are continually being made?

The Basics of Bitcoin

Introduction

Before analyzing how Bitcoin can adapt itself in a world of constant technological advancements, it is useful to look at a brief overview of how the cryptocurrency works as per Nakamoto’s design. The biggest difference between a traditional currency and Bitcoin lies with the removal of a third party mediator, such as a bank or government, which would usually oversee transactions and manage the production of the currency. With Bitcoin, no user must put their trust with anyone else, a feat that is ensured with clever mathematics and a design that relies on the majority of nodes (computers) working in accordance to the rules and not in a fraudulent or malicious manner. [3][10]

In Bitcoin, a transaction, or an exchange of coins between users, is directed towards one or more “public keys” (analogous to a “username”), which are owned by the person who is in possession of the private key (analogous to a “password”) that goes along with it. Account balances are not kept track of in the traditional sense: instead, owning Bitcoins means that a person, say Alice, can show that she has transactions which were sent to her that she has not yet “spent” (a transaction is considered spent when it is used to pay for another transaction in which Alice was the sender). To figure out how many Bitcoins Alice has, one would have to add up all the unused transactions which are linked to all of the public keys that Alice has matching private keys for. A notable point is that with Bitcoin, if Alice were to somehow lose access to her private keys (due to her computer crashing, for example, if she did not have the keys stored online), she would lose the Bitcoins associated with the matching public keys because she would have no way of proving that the

keys were actually hers. By definition, Bitcoin has no bank or overarching power she could appeal to – the currency is based solely on a set of protocols from which no user may be exempted. [3][10]

Transactions:

In order to actually keep track of Alice's and other users' transactions, there has to be a system put in place that can be verified by the network to confirm validity. A global ledger called the transaction blockchain keeps track of all Bitcoin movements, with a set method of recording and validating bitcoins. Each transaction is stated to have inputs and outputs, with hash identifiers incorporated into the outputs which allow other users to see that the outputs came from that specific transaction. The inputs to a transaction have "hash pointers" that point to previous transactions, allowing the network to verify that the user claiming to have received a certain amount of funds did in fact receive them. The outputs of the transactions which are pointed to must be unused and add up to the output of the current transaction, which includes so called "change addresses" that return any surplus coins back to the sender to ensure that all transactions are fully consumed. [11]

If Alice wants to pay for a transaction with transactions she received under another address, all she has to do is use the private key of the other address to encrypt a hash of that transaction to prove it was actually sent to her. Other users can confirm that she is in fact the owner of the other public key by applying the public key (which is visible to all) to the encrypted hash, which should yield the original hash due to the two paired keys being inverses of each other[2]. [12]

Proof of work:

The major problem which is solved in Nakamoto's paper is that of preventing the double spending of funds without a third party present to decide at what point in time and in which order each transaction was made. [3] While one might initially think of simply requiring a timestamp to be put on each transaction, malicious users could simply lie about when the exchange was initiated

[2] Note: Transaction authentication as well as many of the finer mechanics behind Bitcoin are discussed further on in the paper with the in-depth description of the DomCoin cryptocurrency, a cryptocurrency also largely based on Nakamoto's paper.

and, since transactions in Bitcoin travel node by node across the network, a certain set of transactions might arrive to a user in Germany in a different order than, say, a user in Brazil. [3] [5]

The solution to this dilemma is to place transactions in blocks, with all the transactions in a given block defined to have been conducted at the same point in time. Transactions not yet in a block are deemed "unconfirmed" or "unordered", and can be placed into a potential block by any node in the network that will then attempt to confirm and broadcast the new block as the latest item in the ordered blockchain[3]. [11]

To ensure that no single user may decide the ordering of the blockchain, Bitcoin puts into place a "proof-of-work" scheme, a computational problem of a certain difficulty which demonstrates that the computer has put effort in making the block. [5] A simplified example of a proof-of-work could be requiring nodes to successfully flip a coin and get 40 heads in a row, a task which would require a significant amount of trials and could be made more time consuming by simply increasing the amount of coins that needed to turn up as heads[4]. Critically, Bitcoin defines the longest blockchain to be the accurate blockchain, meaning that if an attacker Eve were to try and double spend coins she would have to create a blockchain longer than all other blockchains in order to dictate the order transactions were made in. Trying to solve the proof-of-work problem, known in Bitcoin as "mining", is done by nodes all around the world, meaning that in order for Eve to double spend coins she would have to have computing power comparable to the entire rest of the world's computing power. [5] [3]

Furthermore, each miner is actually solving a slightly different mining problem because the problem is based on the textual contents of the block, which will differ for different users. This difference comes from users receiving transactions in slightly different orders but also because, as stated by Bitcoin's original regulations, miners are allowed to include a special transaction at the beginning of each block. This is a transaction which will be directed to their own public key,

[3] A blockchain is a chain that connects successive blocks to each other allowing users to figure out which transactions were performed before which other transactions. Double spending is thus prevented because a user will never accept an "unused" transaction as payment if it is already listed as payment in a previous block (because it would therefore, by definition, already have been "used").

[4] We will see later on with DomCoin the actual proof-of-work task that Bitcoin requires nodes to do.

crediting them with a certain given amount of Bitcoins and thus providing an incentive for users to help create blocks and sustain the blockchain. The randomness in the different mining problems that users have to solve results in a fairly even distribution of some node creating a block on average every 10 minutes, a time which is assured by the system reevaluating the proof-of-work difficulty every two weeks and adjusting the mining difficulty according to the computing power currently in use. [10] [3]

More on Security

Finally, it is crucial to look further into how Bitcoin remains secure for individual users and the entire community. While it might initially appear that Eve, the user wishing to perform a double spend transaction, could precompute a chain of blocks to spring on the blockchain at a given time, Bitcoin actually prevents this by allowing a new block to be solved only once the previous one has been created. Each block has an identifying name, or "hash", that is based on the contents of the block which, by default, must include the name of the previous block in the blockchain. Since the particular mining problem is based on the contents of any given block, it would be impossible to begin mining without full knowledge of the block's contents (including the hash of the previous block). There is no way for Eve to get a head start with the block creation process and she is therefore in a race with the rest of the nodes in the network to add the newest item to the blockchain. [10] [3]

With the ordering of the blocks in the blockchain assured, and the requirement that individual transactions be signed for using private keys to ensure their authenticity, the Bitcoin system now appears to be secure. Transactions cannot be changed after they are made because this would change the transaction hashes, thus resulting in no new nodes accepting the faulty version of the blockchain due to it being invalid.

The NSA's New Stance on Elliptic Curve Cryptography

We have seen that the mathematics and protocols behind Bitcoin prevent fraudulent transactions from being integrated into the blockchain and that, so long as the majority of the computing power working to create blocks follow the rules that are set out, the minority that seek to cheat the system will be thwarted. What happens, however, when new technology is

released or when the assumptions behind Bitcoin become invalid (as they certainly will in a society where advancements are taking place every single day)?

One possible threat to Bitcoin's overall security emerged as recently as August 2015, with the release of a statement on today's cryptography by the National Security Agency (NSA) [6]. The statement seems to discourage the use of Elliptic Curve Cryptography (ECC) [7] as a part of the transition towards quantum resistant algorithms ("elliptic curve cryptography is not the long term solution many once hoped it would be" [6]), leading to much speculation and many deciding that it is "inescapable that the NSA [is] distancing itself from ECC" [7].

While much of this is speculation, it would be unusual for the NSA to announce to the security community that ECC is no longer as secure as it was once believed without some sort of substantiated evidence. Keeping in mind that Bitcoin's authentication system for guaranteeing that funds only be spent by their rightful owners is based heavily on ECC [8], and with the knowledge in hand that if ECC were broken there would be nothing stopping malicious users from stealing from the accounts of others, it would not be unwise to consider a cryptocurrency based on another type of encryption.

It is under these circumstance that we would like to introduce DomCoin, a new cryptocurrency based on the functioning ideas from Satoshi Nakamoto's paper but with transaction authentication provided by RSA encryption, a public key cryptography system developed by Ron Rivest, Adi Shamir, and Leonard Adleman which uses prime factorization as a means of encrypting information [9]. While it is unclear as to why the NSA is distancing itself from ECC, we believe it wise to have a cryptocurrency already in operation in the scenario that, in the near future, ECC is shown to have a major security flaw that RSA would not be subjected to.

DomCoin[5] [3]

In many ways, DomCoin functions similarly to Bitcoin, with the principle ideas described in Satoshi Nakamoto's original paper guiding the safeguards put in place to keep DomCoin secure

[5] Preliminary note: many of the concepts used in DomCoin are based upon those behind Satoshi Nakamoto's original paper. Therefore, reference [3] was vital for the entire creation and the following description of DomCoin.

in an anonymous society where no single user can be trusted. To understand the way in which DomCoin works, in practice and in theory, it is helpful to track a transaction from inception to completion by following the standard transaction procedure.

First, the user must download the required programs to format the transaction and, most importantly, the longest available blockchain (with its corresponding ledger)[6]. These items are available on the currency website, www.domcoins.ezzycorporation.com, and a copy of the ledger and blockchain used for the following transaction can be found under Appendix A.

Blockchain and Ledger Verification

At this point in time the user should verify that the ledger and blockchain are valid, that is that all the preceding blocks and corresponding transactions were created correctly and that all the signatures correspond with the public keys given (proof that transactions were done by those in possession of the private keys corresponding to the given public keys). In practice, the user runs a program which first verifies that the blocks are in order (that is, that the String listed under "Previous_Block_Hash:" in the blockchain is the same as the String under "Block_Hash:" of the previous block). Then, the program verifies that applying the public key of the sender to the transaction signature gives the transaction hash and that the inputs and outputs of all the transactions ever performed correspond to the current state of the ledger. The program also checks that the mining solutions are valid and that no transaction was used twice, in addition to ensuring that the block hashes match the hashes of the blocks plus the mining solutions (all of this is explained in more detail below).

Generating Public and Private Key Pairs

Once the ledger and blockchain have been proven to be authentic, the user may proceed with performing the transaction. For this example, we will consider the case where a current account

[6] Downloading the longest blockchain is vital in DomCoin just as in Bitcoin because it ensures that one is using the blockchain which has had the most proof-of-work put into it. In other words, it is the blockchain which is in use by the majority of the population and, hence, considered to give the accurate order of transactions (thus preventing double spending as seen with Bitcoin).

holder Alice with 7000 DomCoins[7] wishes to transfer 5000 DomCoins to another account Bob that will also be under her control. To do this, Alice must first generate the account for Bob: an RSA public and private key pair which will be the receiver of the transaction must be created.

In practice, the program GenerateKeys.java (see Appendix B) is compiled and the following line is typed into the terminal:

java-introcs GenerateKeys bobprivatekey bobpublickey

This creates private and public keys with the file names specified as command line arguments (bobprivatekey and bobpublickey) which are then saved under C:/keys/private_bobprivatekey.key and C:/keys/private_bobpublickey.key. As output, the program prints the following:

Your public key is:

30819f300d06092a864886f70d010101050003818d0030818902818100b0d545404cc4b8eb1990
18f4cf1d08da50ba18528f81598cfab33c99215b3ed129689af12abc7c2fd1a7a77ef021aca4d5fb2
1c0684b62a25de3804e969c3eaeeece3888954633a4e0f5e2c6c97eaceaff4fe453d829ebf686c95
4be268fb9d532277e66e0495088af4578ebc9f63474a28ef5f8919dc5bc5bd2e470fc50479102030
10001

Original: Text to be encrypted

Encrypted: [B@1f91529c

Decrypted: Text to be encrypted

This provides Alice with the public key in hexadecimal for the Bob account and tests the encryption/decryption mechanism. The Bob RSA public key is applied to the original text and the corresponding private key is applied to this ciphertext, resulting in the original text and showing that the two keys are, indeed, inverses of each other.

[7] Here it is helpful to examine the ledger to see how it works in DomCoin. Just as in Bitcoin, the ledger in DomCoin keeps track of transactions sent to the user which have not been "spent". We can see under the ledger in Appendix A that there is one public key which has been credited with two unused transactions of 4000 and 3000 DomCoins respectively. This will be the user Alice sending the DomCoins to the new public key Bob in our example.

Preparing a Transaction

The next step is running PrepareTransaction.java (see Appendix C) which takes the following command line arguments, in this order: receiver public key in hexadecimal, name of file containing private key of sender, name of file containing public key of sender, and amount of coin to be transferred. Therefore, for this example, the following must be typed into the terminal:

java-introcs PrepareTransaction
30819f300d06092a864886f70d010101050003818d0030818902818100b0d545404cc4b8eb1990
18f4cf1d08da50ba18528f81598cfab33c99215b3ed129689af12abc7c2fd1a7a77ef021aca4d5fb2
1c0684b62a25de3804e969c3eaeeece3888954633a4e0f5e2c6c97eaceaff4fe453d829ebf686c95
4be268fb9d532277e66e0495088af4578ebc9f63474a28ef5f8919dc5bc5bd2e470fc50479102030
10001 aliceprivatekey alicepublickey 5000

The function of PrepareTransaction.java is to create a correctly formatted text description of the transaction, as seen in the program output below:

To:
30819f300d06092a864886f70d010101050003818d0030818902818100b0d545404cc4b8eb1990
18f4cf1d08da50ba18528f81598cfab33c99215b3ed129689af12abc7c2fd1a7a77ef021aca4d5fb2
1c0684b62a25de3804e969c3eaeeece3888954633a4e0f5e2c6c97eaceaff4fe453d829ebf686c95
4be268fb9d532277e66e0495088af4578ebc9f63474a28ef5f8919dc5bc5bd2e470fc50479102030
10001 From:
30819f300d06092a864886f70d010101050003818d0030818902818100b0d59dcddfd2d4e2b879
251a4bc24eb5542e8258ecb310c79c009e752429732f5f3e76d72f8f2f4d122fa1b090109637b9f9
9ea71fe105f376ebf0eba0f2ed66dd12919103c54e62bc3677b3c148c9670f20fe26d40c04535db0
c19568e062d81d7f9e37c7653c8e75a10d5f93003dcbb0cbade46c23d77f7a861cf3e0a51ebb020
3010001 Amount: 5000 Hash:
ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363 Signature:
[B@5171d6fa

The text description of the transaction first gives the public key of the receiver (Bob's public key), the public key of the sender (Alice's public key), and the amount the transaction is for (5000

DomCoin in this example). Then, a hash of the above information is found using another program, Sha256.java (see Appendix D) [8] which is then printed both as plaintext and with Alice's private key applied to it (that is, as the signature). In the blockchain and ledger verification step mentioned at the beginning of this example, a program must apply Alice's public key to the signature and make sure that it returns the plaintext hash, showing that Alice is in possession of the private key corresponding to her public key (thus proving that she is indeed Alice). From here, all Alice has to do is post the output of PrepareTransaction.java to the DomCoin website, hence completing the required steps to perform a transaction.

New Block Creation

While Alice may have finished the necessary steps to perform the transaction, the exchange of the DomCoins has not yet gone into place because the ledger and blockchain have not been updated. By posting the transaction text to the currency website, Alice has introduced it to the pool of unconfirmed transactions which must be added to the blockchain by a user, called a miner. In practice, a miner will take the oldest unconfirmed transaction and attempt to add it to the longest existing blockchain, with the key difference between Bitcoin and DomCoin being that in the latter currency, each block contains only one transaction (more on the mining process below). The miner (the user with 88030 DomCoins in the ledger, in this case) will run Block.java (see Appendix E) with the following input:

java-introcs Block 00000bf09e61f44449f91be613a0db6c87a5db1f24ed127a4a8a54ac901c808c
[insert PrepareTransaction.java transaction description output here]
30819f300d06092a864886f70d010101050003818d00308189028181009 0f1de4c291970420e87
28c0e23a9737c20d2b68ab91edf9c917e586b851abcca902f5a55db8a713fb2de6fbd63fe0269ee
a667af0211bf01d3c04c30e193de96d7d77b32c294c5dfd376ca86dff651881a0de8f32aed2ad486
c855ab727d0e185b83a798c18bfd558e11e83c7c9f6b07383d5e7d2594d5751a9b75df9eff45902
03010001 < ledger.txt

[8] The hash is found using a Secure Hash Algorithm of 256 bits (SHA-256), which is a cryptographic hash function designed by the National Security Agency (NSA) [4]. Changing even just one character of the input text will yield a completely different hash, thus preventing an attacker from editing a transaction after it has been completed. SHA-256 is also used in Bitcoin.

The first command line argument is the hash listed under “Block_Hash” of the last block in the blockchain (the newest), hence linking the block with Alice’s transaction in chronological order to the existing blockchain. Following this, the entire transaction description is inserted into the block, ensuring that it can be checked (once integrated into the blockchain) for validity by other users to prevent fraudulent coin exchanges. Finally, the miner enters his/her public key as a command line argument, giving the program an address to send the compensation coins for successfully aiding the system[9]. With the latest ledger.txt file entered as standard input, Block.java is now ready to run and will output the following text upon completion:

```
1.  Authentication Success
2.  New Block:
3.
4.  Previous_Block_Hash:
5.  00000bf09e61f44449f91be613a0db6c87a5db1f24ed127a4a8a54ac901c808c
6.
7.  To:
8.  30819f300d06092a864886f70d010101050003818d003081890281810 0b0d545404cc4b8eb199018f4cf1d0
    8da50ba18528f81598cfab33c99215b3ed129689af12abc7c2fd1a7a77ef021aca4d5fb21c0684b62a25de3
    804e969c3eaeeece3888954633a4e0f5e2c6c97eaceaff4fe453d829ebf686c954be268fb9d532277e66e04
    95088af4578ebc9f63474a28ef5f8919dc5bc5bd2e470fc5047910203010001
9.
10. From:
11. 30819f300d06092a864886f70d010101050003818d003081890281810 0b0d59dcddfd2d4e2b879251a4bc24
    eb5542e8258ecb310c79c009e752429732f5f3e76d72f8f2f4d122fa1b090109637b9f99ea71fe105f376eb
    f0eba0f2ed66dd12919103c54e62bc3677b3c148c9670f20fe26d40c04535db0c19568e062d81d7f9e37c76
    53c8e75a10d5f93003dcbb0cbade46c23d77f7a861cf3e0a51ebb0203010001
12.
13. Amount:
14. 5000
15.
16. Hash:
17. ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363
18.
19. Signature:
20. [B@5171d6fa
21.
22. Inputs:
23. de5f04609e97985626e9b8ab294272cd276dcdf83031b4b7b9eb2754042ac007 4000.0
24. 2d0cce04e54d257a157f16b0d42c77e1076ebd114c49479b1163e24ae54ea5e4 3000.0
25.
26. Outputs:
27. ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363 2000.0
28. ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363 5000.0
29.
30. Miner_Reward_Public_Key:
```

[9] This is very similar to the way Bitcoin operates. With Bitcoin, however, the transaction to the miner is simply listed as a “special transaction” at the beginning of a block, crediting the user with a certain fixed number of Bitcoins which decreases over time (about every four years). In January 2009, the reward for creating a block was 50 BTC, whereas it is currently only 25 BTC and is speculated to half again in July, 2016 (it halves every 210,000 blocks created) [5]. With DomCoin, creating a block is worth a constant 10 DomCoins (no change over time).

```
30819f300d06092a864886f70d010101050003818d0030818902818100f1de4c291970420e8728c0e23a9
737c20d2b68ab91edf9c917e586b851abcca902f5a55db8a713fb2de6fbd63fe0269eea667af0211bf01d3c
04c30e193de96d7d77b32c294c5dfd376ca86dff651881a0de8f32aed2ad486c855ab727d0e185b83a798c1
8bfd558e11e83c7c9f6b07383d5e7d2594d5751a9b75df9eff4590203010001

Miner_Solution:
%jO

Block_Hash:
0000b7f19ee9158ac01247ee2122b2db6b4972b06d668644e4285dd76e473fd0

Updated Ledger:

Public_Key:
30819f300d06092a864886f70d010101050003818d0030818902818100f1de4c291970420e8728c0e23a9
737c20d2b68ab91edf9c917e586b851abcca902f5a55db8a713fb2de6fbd63fe0269eea667af0211bf01d3c
04c30e193de96d7d77b32c294c5dfd376ca86dff651881a0de8f32aed2ad486c855ab727d0e185b83a798c1
8bfd558e11e83c7c9f6b07383d5e7d2594d5751a9b75df9eff4590203010001
Unused_Transactions:
de5f04609e97985626e9b8ab294272cd276dcdf83031b4b7b9eb2754042ac007 10
2d0cce04e54d257a157f16b0d42c77e1076ebd114c49479b1163e24ae54ea5e4 88020.0
ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363 10
Public_Key:
30819f300d06092a864886f70d010101050003818d0030818902818100bda7757642474dc726b914db3cb0
98f30e36fb9dcd383437b1d776b871bb741d5fca7f762b9d7715ba91e3553302a83821c5302e783fc3bbf09
2cbc65195426c6004dfc472395bb376a6500bf609d7ca7256dcbd6704991407034b010f27192c3f610e924c
461316fed6f1c8669520df00f6dd86cda28970be3bf330d416ed70203010001
Unused_Transactions:
974dadd9665237a50a386904e38804e79842d8969aac563516edeb618bcad8ba 5000.0
2d0cce04e54d257a157f16b0d42c77e1076ebd114c49479b1163e24ae54ea5e4 10
Public_Key:
30819f300d06092a864886f70d010101050003818d0030818902818100b0d545404cc4b8eb199018f4cf1d0
8da50ba18528f81598cfab33c99215b3ed129689af12abc7c2fd1a7a77ef021aca4d5fb21c0684b62a25de3
804e969c3eaeeece3888954633a4e0f5e2c6c97eaceaff4fe453d829ebf686c954be268fb9d532277e66e04
95088af4578ebc9f63474a28ef5f8919dc5bc5bd2e470fc5047910203010001
Unused_Transactions:
ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363 5000.0
Public_Key:
30819f300d06092a864886f70d010101050003818d0030818902818100b0d59dcddfd2d4e2b879251a4bc24
eb5542e8258ecb310c79c009e752429732f5f3e76d72f8f2f4d122fa1b090109637b9f99ea71fe105f376eb
f0eba0f2ed66dd12919103c54e62bc3677b3c148c9670f20fe26d40c04535db0c19568e062d81d7f9e37c76
53c8e75a10d5f93003dcbb0cbade46c23d77f7a861cf3e0a51ebb0203010001
Unused_Transactions:
ce2386e06b00c0ff9a1fdf9e2a1992e11cc3561b5ae074218bc923199eeeb363 2000.0
```

Careful analysis of this output provides a unique insight into the way DomCoins allows the transfer, creation, and storage of currency without the opportunity for fraud and inauthentic transactions. Firstly, “Authentication Success” on line 1 confirms that the transaction hash given still matches the hash of the transaction[10]. Then, one can see a formatted description of the new block which is to be added to the end of the current blockchain, therefore confirming the transaction and logging it for others to see. The block text features all the details concerning the

[10] This is done by hashing the transaction again and comparing it to the given hash. It prevents another individual from changing any part of the transaction (since any change will result in a change of the hash).

transaction: who it is from, who it is to, the amount it is for, hash and signatures for authentication, and finally the inputs and outputs, which correspond to which transactions were spent and which new ones were created[11] [12].

Since one cannot only partially use a transaction, change will be given back to the sender in the form of an output transaction listed to him/her. Here, Alice "spent" both of the unused transactions listed under her public key in the ledger in Appendix A (the ones she had received for 4000 and 3000 DomCoins which are rightfully listed as block inputs), meaning that she should receive 2000 DomCoins in return as one of the outputs in addition to the output which should be directed to Bob with the intended 5000 coins. As is seen in the outputs section of the block, both of these transactions are listed with the unique transaction hash confirming that the transaction came from this particular exchange.

Finally, an updated version of the ledger is printed with the necessary transactions added and omitted. In addition to the ones described above, a 10 DomCoin transaction is credited to the miner's public key for his/her efforts in creating the block. The miner then posts the new ledger and blockchain to the DomCoin website and, unless a longer blockchain has already been created, other users will quickly adopt these versions of the files since the longest blockchain is considered to be the actual blockchain by default.

Mining

In the above creation of the block, we neglected to talk about the actual mining mechanism which prevents double spending just as in Bitcoin (by ensuring that the longest blockchain is the one which the majority of CPUs on the network performed proof-of-work for). Miner.java (see Appendix F) is called from Block.java with the block text as well as a predetermined mining "difficulty" N, which specifies how "hard" the problem in question is to be. The program mines for a special key which, when concatenated to the end of the given block text from Block.java, can be hashed using SHA-256 to yield a String with N leading zeros (again, with strong

[11] In DomCoin much like in Bitcoin, the ledger keeps track of unused transactions, not net balances. Unused transactions become used when they are listed as inputs to a block (when they are used to pay for a transaction).
[12] The "Miner_Solution" is also listed in the block text, see the following section on mining.

resemblance to the way Bitcoin works). In actuality, Mining.java hashes random Strings generated by RandomString.java (see Appendix G) of ever increasing length until a concatenated String/String combination yields a hash as output with at least N leading zeros. For this example, a mining difficulty of only N equal to four was used, taking at most several seconds on an average personal computer. If the cryptocurrency begins to see higher transaction traffic, the mining difficulty will be adjusted such that, just as in Bitcoin, it takes a certain amount of time for the entire network to generate a block (thus reducing the chance that blocks will be created simultaneously but not so much as to render transaction confirmation impracticably slow).

The following calls to Miner.java give a good idea of how long different values of N take to be solved:

java-introcs Miner 1 asdfasfd ➔ Trials: 11 Time taken: 0.015 seconds

java-introcs Miner 2 asdfasfd ➔ Trials: 453 Time taken: 0.047 seconds

java-introcs Miner 3 asdfasfd ➔ Trials: 1050 Time taken: 0.084 seconds

java-introcs Miner 4 asdfasfd ➔ Trials: 9296 Time taken: 0.285 seconds

java-introcs Miner 5 asdfasfd ➔ Trials: 234335 Time taken: 1.169 seconds

java-introcs Miner 6 asdfasfd ➔ Trials: 38795347 Time taken: about 2 minutes

java-introcs Miner 7 asdfasfd ➔ Trials: 425918263 Time taken: about 47 minutes (Solution: ": 53l")

While the time taken and the number of trials needed to solve a given mining problem will vary tremendously from trial to trial, these numbers give a good idea of how rapidly the time to find the key String increases with increases in N. To reiterate, taking the last trial with an N value of seven, Miner.java has found the key ": 53l" which, when concatenated with the String "asdfasfd" to form "asdfasfd: 53l", yields a SHA-256 hash with at least seven leading zeros ("000000084a0b8684de135161e04274b2fb223540461097ef450c9ba6d6759dfa", in this case). The advantage of such a problem is that it is very time consuming to find the solution, but extremely easy to check that a given solution yields the correct output. With this tool in hand,

DomCoin users can easily confirm that proof-of-work was put into making a block and that, with a high statistical probability, the block was formed due to the majority of DomCoin users attempting to solve its unique mining problem. [13]

With the mining process complete, the entire mechanism behind DomCoin has been covered and any user possessing a computer with access to the internet can now send and receive coins in this system. Having introduced a new cryptocurrency, it is now important to look further into the social ramifications behind cryptocurrencies in general in order to better understand how a tool like DomCoin can positively or negatively affect the real world.

Further Social Consequences of Cryptocurrencies

Cryptocurrencies and Terrorism

We have already seen several major ways society affects the nature of cryptocurrencies, namely the manner in which technological advancements or news in the security industry can lead to the creation of new currencies as well as how the theory in Nakamoto's paper can be applied to form real, usable systems in societies around the world. While we have discussed the features of these cryptocurrencies in a primarily positive light, it is important to also recognize the opportunities for illicit use that these technologies provide. To consider what (if anything) should be done about the possibilities of corrupting this relatively new tool, we will place particular emphasis on the recent rise in terrorist threats around the world and how Bitcoin as well as DomCoin could be involved.

The annual *Defense Against Terrorism Review* says on the topic: "features associated with these so-called 'cryptocurrencies,' such as transaction anonymity and irreversibility of payments, have made them extremely attractive to cybercriminals, drug dealers, money launderers and those involved in global terrorist funding" [14]. The report goes on to highlight many of the selling points behind Bitcoin and currencies like DomCoin as reasons for which terrorist cells may choose to use cryptocurrencies as a way of fundraising and transferring money for illegal activities.

[13] "Unique" being a key word- each mining problem is based on the block text, meaning that it cannot be computed ahead of time since the block text includes the previous block hash (which only becomes available once the previous block is created).

Aspects such as virtual anonymity, global reach, ease-of-use, speed, and non-repudiation are all mentioned to be features which aid terrorist organizations, despite these being the same features which make the currency so attractive to those not intending to abuse the technology. Does this mean that Bitcoins, which are not considered legal tender in any country, should be banned from existence for aiding the actions of groups with harmful intentions? [14]

Some people, such as startup entrepreneur Jonathan Chester, believe that the solution lies with adapting Bitcoin to decrease the chance of terrorists misusing the currency. He founded Bitwage, a company that allows users to receive part or all of their wages in cryptocurrencies, with a plan to "minimize the threat of terrorist financing by implementing a thorough risk-based anti-money laundering policy that includes customer due diligence and transaction monitoring" [14]. While some claim that introducing a third party into the mix to screen out potential terrorists and criminals, a person Chester calls the "in-house compliance officer", goes against Nakamoto's founding ideas, the young entrepreneur believes that it is a key step to assuring safety in a world where anonymity has become a possibility [14].

Requiring background checks or in-depth identity verification to receive public keys was a feature that was considered in the creation of DomCoin, however it was ultimately rejected due to the conclusion that it would limit the cryptocurrency's growth potential and could result in transactions being even less anonymous than those in the traditional banking system[14]. With the banks of today, a degree of privacy is obtained by restricting the access of information by third parties and other users. While with a traditional bank it is not possible to simply look up a friend's or even a stranger's net balance, all transactions are made public in the DomCoin blockchain and requiring background checks could increase the chance that leaks would link people to their public keys. [3] While it is true that the anonymity which DomCoin provides for the majority of users with no ill intentions can also be used for evil, it is important to note that this is true for a plethora of modern-day technologies. One must look no further than the internet, a tool which has united the world and led to a wealth of information transfer, to find an example of a

[14] Note on Bitcoin and DomCoin anonymity: with both cryptocurrencies it is recommended that users generate a new key pair for each transaction. This avoids the possibility of external parties linking public keys together and compiling information on user account balances and funds. [3]

technology which regularly facilitates illegal action (such as online recruitment for terrorist groups) which is allowed to prosper due to the majority of users having moral intentions.

Cryptocurrencies and the Environment

While the Bitcoin and DomCoin mining processes are necessary for maintaining stable cryptocurrencies without the possibility of double spending, it is important to note that the computations done by the mining computers are, as they are designed to be, computationally heavy. This means that a significant amount of electricity is spent maintaining a virtual system, doing large calculations which are not useful to anybody outside of the cryptocurrency community (and even within it, the solutions to the calculations serve only to prove that the calculations were actually performed).

The Long Future Foundation, an Australian organization promoting the use of sustainable energy, states that if the price for individual Bitcoins were to increase dramatically (due to a probable spike in use as the technology becomes more widespread and the fact that there are only a finite number of Bitcoins available), say to one million dollars per coin, it would be profitable for miners to spend as much as 13,140 terawatt hours (TWh) per annum in creating the currency[15] [15]. This figure is based on a price of $0.05 per kilowatt hour and a 50% profit margin – more than enough of an incentive for miners around the world. [15] The problem lies with the fact that so long as it is profitable for companies to purchase more computing power, and thus use more electricity, there will be nothing stopping them from increasing their energy consumption. An increase in total computing power will mean an increase in the mining problem difficulty required to create a block, implying that the blockchain will be maintained to the same degree as it is now but simply with a much higher energy footprint.

The DomCoin currency seeks to mitigate this problem with the way in which miner incentives are provided –- namely by issuing a constant ten DomCoins per successful block creation as incentive instead of a decreasing amount of Bitcoins until no more Bitcoins are produced. Crucially, DomCoin avoids a drastic increase in the currency's value by not restricting the total number of

[15] To put this into perspective, this is enough energy to power 1.5 billion average homes. [15]

coins which can be produced (which would lead to a deflation over time and a more desirable Bitcoin), therefore greatly reducing the incentive for large companies to invest in mining plants which negatively affect the environment. Since the value of a DomCoin will not reach the heights of that of a Bitcoin (because DomCoin undergoes a constant, steady inflation), there will be almost no financial incentive for companies to invest millions of dollars into increasing the mining difficulty. This in turn prevents an increase in the cryptocurrency's energy footprint which would have had no positive effect on the security or reliability of the currency. Combined with the traditional advantages that cryptocurrencies inherently possess, such as not needing a physical, resource-heavy medium like paper or metal, DomCoin appears to be a viable solution for reducing electricity usage and ultimately helping to play a part in the mitigation of climate change.

Conclusion

We have reexamined the ideas of Satoshi Nakamoto seven years after the release of the revolutionary paper on the peer-to-peer Bitcoin system. While the majority of the system remains as secure as ever, certain technological and social advancements, such as the possibility of a weakness in the Elliptic Curve Cryptography encryption system and the need for an environmentally friendly cryptocurrency, have created an opportunity for a new version of electronic cash. DomCoin, a cryptocurrency with a steady value inflation based on RSA encryption, seeks to fill this gap by providing smaller monetary rewards to miners (therefore discouraging large companies from using significant energy resources) and an authentication system which may not be susceptible to the possible insecurities voiced by the National Security agency.

References

[1]	"1971 Termination of Gold/Dollar Convertibility." UC Berkeley Library. Berkeley, n.d. Web. 03 Jan. 2016. <http://vm136.lib.berkeley.edu/BANC/ROHO/projects/debt/terminationgolddollar.html>.

[2]	"Who Is Satoshi Nakamoto?" The Economist. The Economist Newspaper, 02 Nov. 2015. Web. 03 Jan. 2016.
[3]	Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." The Cryptographic Mailing List (2008): n. pag. https://bitcoin.org/bitcoin.pdf. Bitcoin. Web. 26 Dec. 2015. <www.bitcoin.org>.
[4]	"Secure Hashing." National Institute of Standards and Technology. N.p., n.d. Web. 03 Jan. 2016. <http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html>.
[5]	"Bitcoin: Proof of Work." Khan Academy. N.p., n.d. Web. 03 Jan. 2016. <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work>.
[6]	"Cryptography Today." www.nsa.gov/. National Security Agency, 19 Aug. 2015. Web. 04 Jan. 2016. <https://www.nsa.gov/ia/programs/suiteb_cryptography/>.
[7]	Koblitz, Neal, and Alfred Menezes. "A Riddle Wrapped in an Enigma." (n.d.): n. pag. Web. 1 Jan. 2016. <https://eprint.iacr.org/2015/1018.pdf>.
[8]	"Elliptic Curve Digital Signature Algorithm." Bitcoin Wiki. N.p., 10 Feb. 2015. Web. 04 Jan. 2016. <https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm>.
[9]	"RSA Encryption." Wolfram MathWorld. N.p., n.d. Web. 04 Jan. 2016. <http://mathworld.wolfram.com/RSAEncryption.html>.
[10]	Driscoll, Scott. "How Bitcoin Works under the Hood." How Bitcoin Works Under the Hood. N.p., 14 July 2013. Web. 05 Jan. 2016. <http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html>. <https://www.youtube.com/watch?v=Lx9zgZCMqXE>.
[11]	Narayanan, Arvind. "Princeton Bitcoin and Cryptocurrency Technologies Online Course." Princeton Course Website. N.p., n.d. Web. 06 Jan. 2016. <https://piazza.com/princeton/spring2015/btctech/resources>.
[12]	Khan, Salman. "Bitcoin: Transaction Records." Khan Academy. N.p., n.d. Web. 06 Jan. 2016. <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-records>.

[13]	Chester, Jonathan. "How Questions about Terrorism Challenge Bitcoin Startups." Forbes. Forbes Magazine, n.d. Web. 06 Jan. 2016. <http://www.forbes.com/sites/jonathanchester/2015/12/14/is-bitcoin-the-currency-of-terrorism/>.
[14]	"Defense Against Terrorism Review." (n.d.): n. pag. Centre of Excellence - Defence Against Terrorism, Fall 2014. Web. 6 Jan. 2016. <http://insct.syr.edu/wp-content/uploads/2015/05/Brill_Cryptocurrencies.pdf>.
[15]	Perez, Yessi. "Think Tank Reignites Debate Over Bitcoin Mining's Environmental Effects." CoinDesk. CoinDesk, 27 May 2015. Web. 06 Jan. 2016. <http://www.coindesk.com/think-tank-debate-bitcoin-mining-environment/>.
[16]	"Crypto-Currency Market Capitalizations." Crypto-Currency Market Capitalizations. N.p., n.d. Web. 06 Jan. 2016. <http://coinmarketcap.com/>.