Blockchain Technologies

Orhun Barış *orhunbaris@sabanciuniv.edu*
Computer Science and Engineering/ Faculty of Engineering and Natural Sciences, 2014

Umut Barut *umutbarut@sabanciuniv.edu*
Mechatronics Engineering/ Faculty of Engineering and Natural Sciences, 2015

Görkem Kır gorkemkir@sabanciuniv.edu
Computer Science and Engineering/ Faculty of Engineering and Natural Sciences, 2015

Ekin Oskay ekinoskay@sabanciuniv.edu
Computer Science and Engineering/ Faculty of Engineering and Natural Sciences, 2016

Supervisor: Kamer Kaya, *Computer Science and Engineering*

Abstract

Blockchain is a distributed ledger and by many authorities, it is considered to be one of the game-changing technologies around. The most important add-on of Blockchain is providing and maintaining trust between parties who do not trust each other in real world. In addition, it has many applications and many more is coming. In this PURE project, our main motivation is understanding this technology and finding a use-case for our living environment: SU campus. We searched cryptocurrencies, how they work and try to digested the ideas behind them.

Developing a cryptocurrency for a university campus can be a promising use case since making a cryptocurrency roam around the campus and let the students get discounts by staking some amount of currency will be useful for the students. This idea will make the students to save money, hence the wallets will correspond to the saving accounts in real life. The incentives for them will be discounts.

Keywords: Cryptocurrency, Blockchain, Smart contract, Bitcoin, Ethereum

1 Introduction

In this project we are trying to develop a cryptocurrency that will work within the campus. Students and staff will be encouraged to use the currency. Currency will roam around the campus. We also looked up about how cryptocurrencies work and how they are implemented. We searched how “Blockchain” works and how cryptocurrencies are implemented on it. We followed the “Blockchain at Berkeley” (Blockchain at

Berkeley,Berkeley, 2018)lectures for that particular purpose. We also made a list about currencies that have weird ideas behind them and made an “Funcoins” writing.

2 Research Topics

2.1 Bitcoin

2.1.1 What is Bitcoin

Bitcoin is a kind of cryptocurrency which exists purely in the digital realm first time used in 2009. It born out of the Cypherpunk movement, a libertarian struggle for privacy and self-governance. Invention of blockchain inspired the creation of Bitcoin by Satoshi Nakamoto who an anonymous identity.

Retrieved from:Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview at Berkeley

2.1.1.1 What does Bitcoin provide?

- Account and identity management: Every user has an address and each of them relevant with amounts of currency.
- Services: Users can do transactions between each other via other users.
- Record management: Redundant information is stored by other users which are on the system via a blockchain.
- Trust: Trust comes from personal encouragement aligning with community goals.

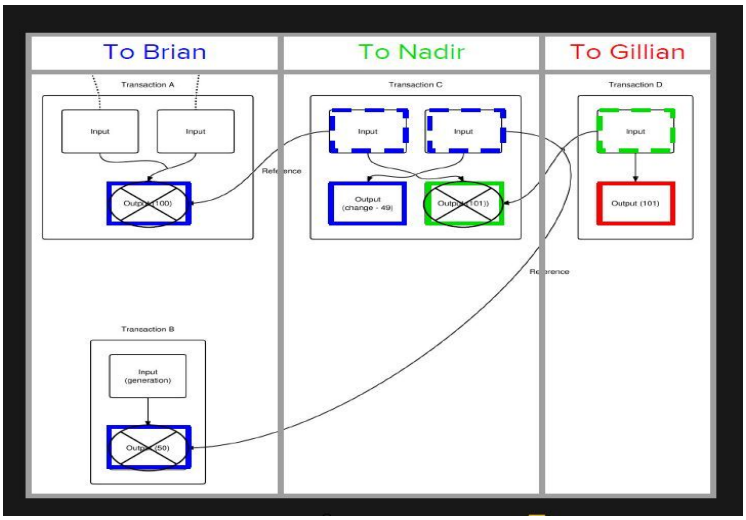
2.1.1.2 Identity

With identity, people can receive, claim, spend the Bitcoin. Identity provides a random private key, then public key is created corresponding private key. Public key is for receiving money, private key is for accessing the account to manage. There are 2^160 possible public key (1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,97 possible addresses). Practically, it is impossible to guess someone’s private key.

There are possible public keys more than grain of sand on earth.

2.1.1.3 Transaction

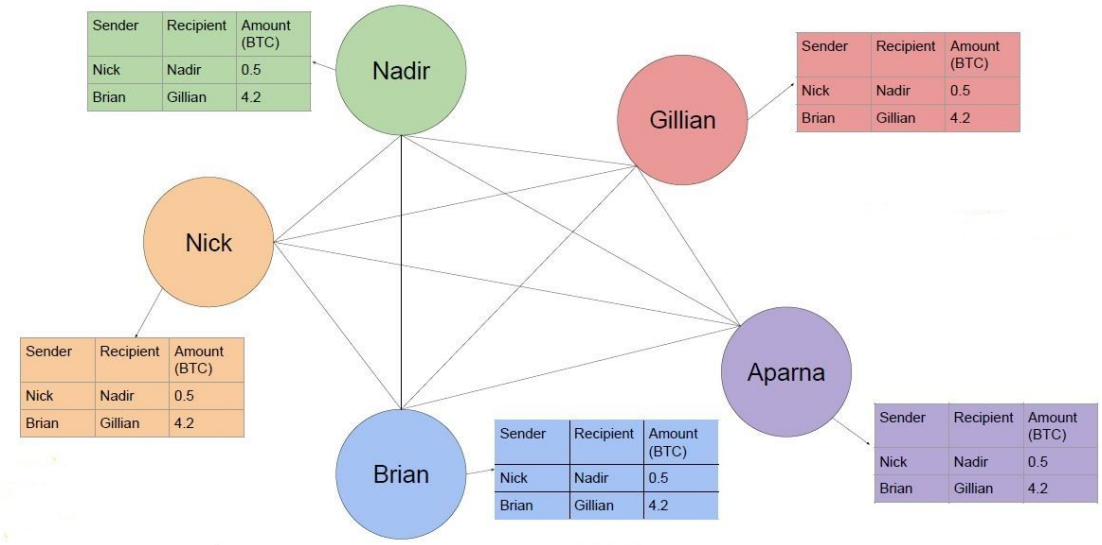
Transaction is valid when three conditions are satisfied;
Proof of ownership: There must be a signature of ownership.
Available funds: Users must have enough amount of Bitcoin.
No double spending: Other transactions can't use the same funds.



Retrieved from:Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview at Berkeley

2.1.1.4 Record Keeping: The Blockchain

Transaction ledger is stored with distributed database, everyone on the system stores the ledger.



Retrieved from:Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview at Berkeley

2.1.1.5 Consensus (Proof-of-Work)

To prevent double spending, every transaction must be validated by the other peers. Bitcoin has anonymous identity, so people can have multiple accounts to take opportunities of cast vote. That is why Bitcoin validation protocol uses resources instead of cast votes. Peers use their CPU power to vote. They have voting power as much as used power. (System assumes majority of the network is honest)

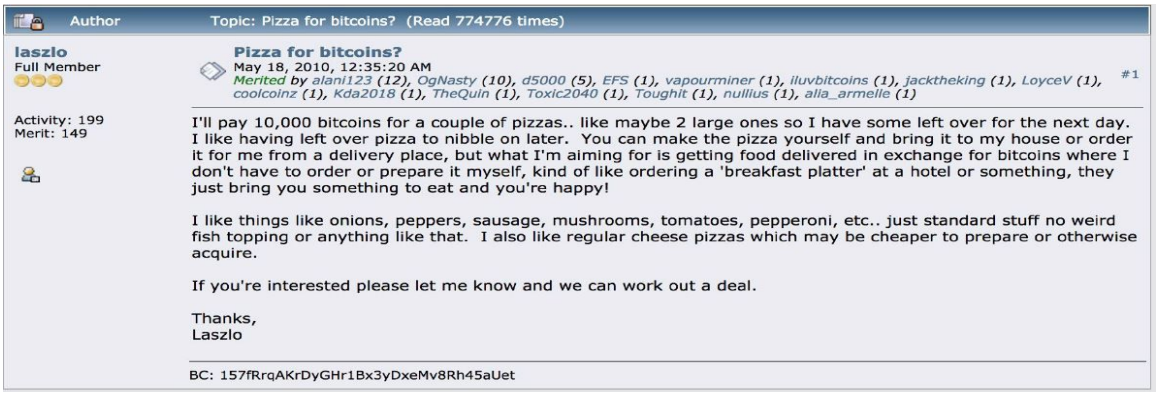
2.1.2 Some History of Bitcoin

2.1.2.1 Before Bitcoin

Before the Bitcoin, there are some early cryptocurrency attempts.
One of them is Digicash, it was developed by David Chaum at 1998 and it's transaction was similar to today's transaction which provides anonymity due to the it's cryptographic protocols. It was failed because of centralization.
Another one is Hashcash, it was designed for variety of functions, as well as minimizing email spam and preventing DDoS attacks.
Bit Gold, B-money were also early cryptocurrency attempts.

2.1.2.2 $74 million = 2 Pizzas

Bitcoin is the most valuable cryptocurrency today. Before the Bitcoin gets valued, there was a trade which a guy bought two pizzas for 10,000 Bitcoin, today it's value is ~$74 million.



Author | Topic: Pizza for bitcoins? (Read 774776 times)

laszlo
Full Member

Activity: 199
Merit: 149

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM #1
Merited by alani123 (12), OgNasty (10), d5000 (5), EFS (1), vapourminer (1), iluvbitcoins (1), jacktheking (1), LoyceV (1), coolcoinz (1), Kda2018 (1), TheQuin (1), Toxic2040 (1), Toughit (1), nullius (1), alia_armelle (1)

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

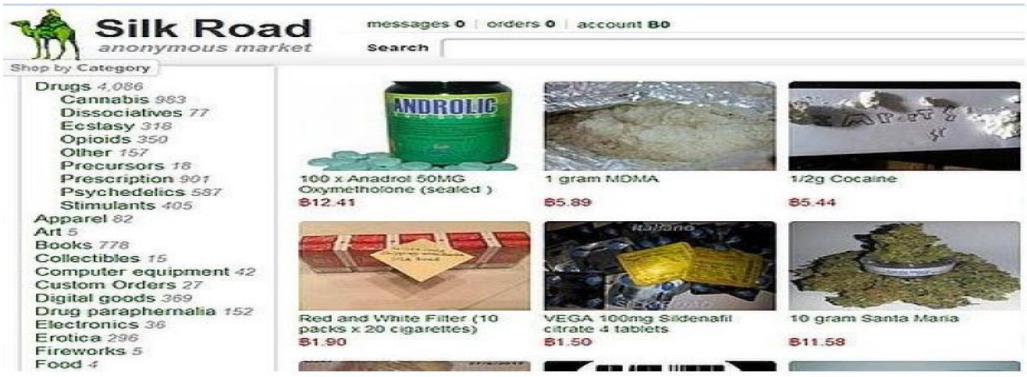
Retrieved from:Lecture 02 - Bitcoin to Blockchain History at Berkeley

2.1.2.3 Bitcoin Theft

Mt. Gox was the biggest online bitcoin exchange market. More than %70 of transactions were being occurred via Mt. Gox. In 2014, Mt. Gox lost 744,408 bitcoins in a theft, then Mt. Gox declared bankruptcy.

2.1.2.4 Bitcoin in Illegal Use

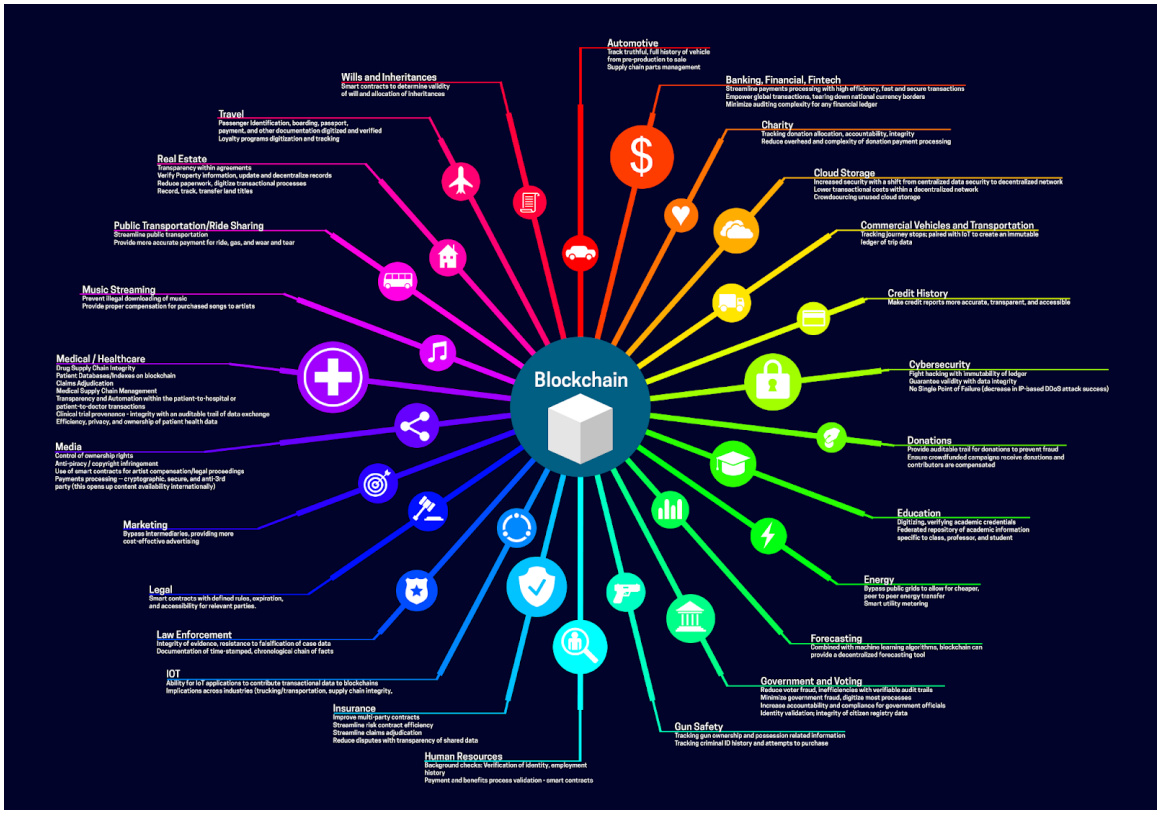
Due to Bitcoin anonymous protocol, it is used in the black market for illegal goods. Silk Road was one of them, it was sold goods for Bitcoin via Tor network. It was shut down by FBI with seizing $3.5m in Bitcoin.



Retrieved from:Lecture 02 - Bitcoin to Blockchain History at Berkeley

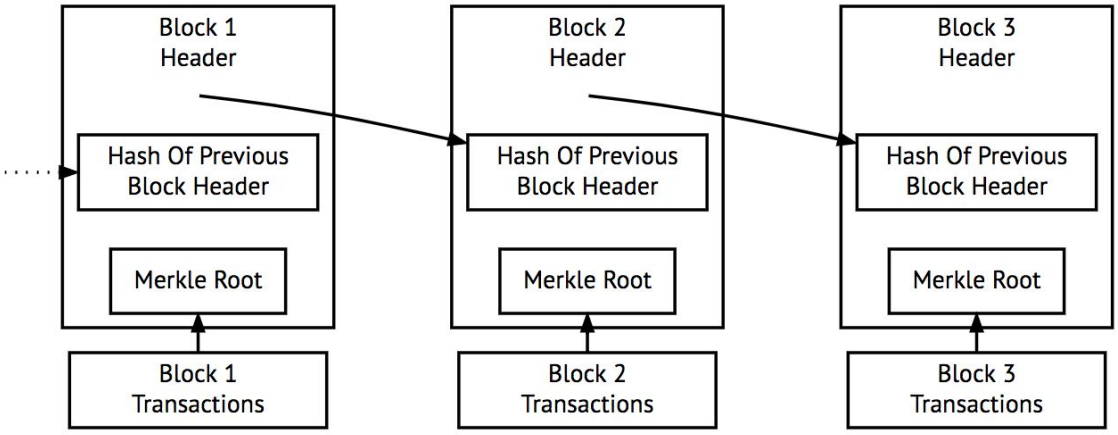
2.2 What is Blockchain

A **blockchain** is a distributed ledger that basically holds a list of records in semi-ordered manner. A copy of this list exists at every computer within the Blockchain network.(Blockchain at Berkeley, "Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview", 2018) In this project, we are interested in the technical details and use cases of this new technology.



("Blockchain use cases", 2018)

Blockchain could be public or private, it depends on the cryptocurrency, but in Bitcoin, the blockchain is public which means anyone can look at it.("How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes", 2018). In blockchain, every block has many transactions which contain key information like amount, sender, receiver (in our bitcoin case). In Bitcoin, blocks look like this:

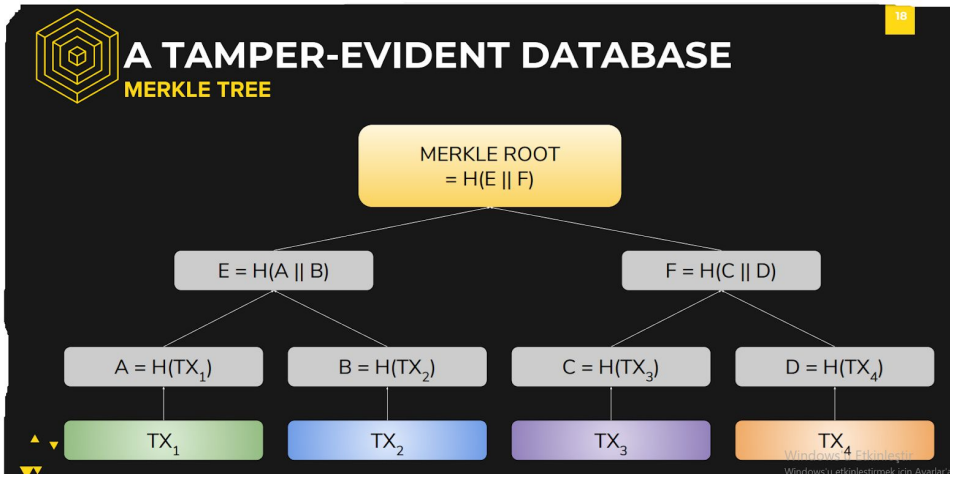


Simplified Bitcoin Block Chain

(Simplified Bitcoin Block Chain,Lecture 01 Bitcoin Protocol and Consensus,2018)

Every block has a header which holds “Merkle Root” and “Hash of previous block header” and every block has a list of transactions within its body.

In header, hash of previous header is there for making sure that block is not altered. When someone changes the previous block, its hash value changes which affects all the chain and makes the malicious activity visible to anyone. Merkle root is sort of a signature of all of the transaction in that block’s body part. Firstly, we hash all of the transaction ID’s. After that we pair them up (2 transactions are paired) and hash them again and again until there is only 1 hashed value left. That value is what we call “Merkle Root”.("Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview", 2018)



("Lecture 03 - Bitcoin Mechanics and Optimizations: A Technical Overview", 2018)

(Here TX1 is transaction1, TX2 is transaction 2, …, A is hash of transaction1, B is Hash of transaction2, …, E is hash of A and B and so on). Here, when someone changes a transaction it would change some hashes and it will result in a different Merkle root and which makes blockchain Tamper-evident. Finally the in order to explain “Nonce”. First we have too look at the idea of Partial Pre-image Hash Puzzle. We need to find a nonce that satisfies the following condition for that particular block to be valid:

```
H(prevBlockHash || merkleRoot || nonce) < target
```

("Lecture 03 - Bitcoin Mechanics and Optimizations: A Technical Overview", 2018)

Hash of the previous block, merkle root and nonce must be smaller than the target. Computers are continually tries to guess this value. They try random values at hash them together and check if it satisfies the condition, if not they try it again until target is reached (Blockchain at Berkeley, "Lecture 03 - Bitcoin Mechanics and Optimizations: A Technical Overview", 2018).

This idea is how “Proof of Work” idea works in the bitcoin. There are three characteristics that these hash puzzles have to have. First, they have to be computationally difficult. Because if proof of work requires little work, they could be easily achievable. Secondly, they have to be parameterizable. We want to use our 3 values to solve it and some specific “Nonce” is required. (Every nonce should create a unique output that may or may not satisfy the target. If satisfies block got written in the list.) and by changing the target we should be able to change the difficulty, because if network starts to verify blocks faster we want to increase its difficulty and maintain the same block time and vice versa. Finally they have to be easily verifiable by other people in network.

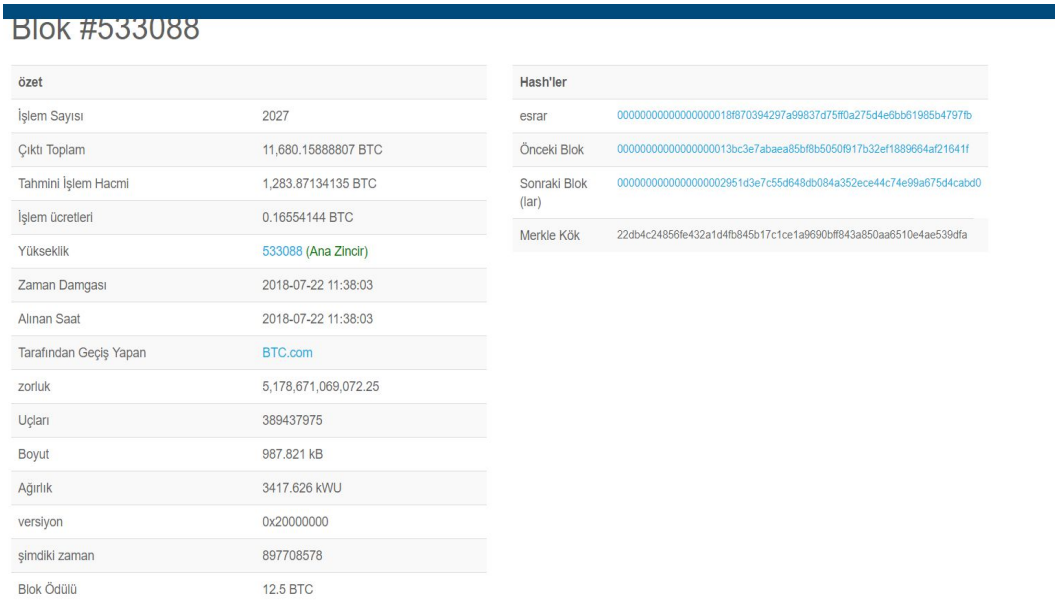
Merkle root and hash of previous block header and its “Nonce” creates a unique “Block hash” that will be used for next blocks. We can say that this system is safe and any changes within a block affects all the blocks that is coming afterwards which intervenes malicious activities.

2.3 Mining Process

We already looked at how blockchain is established and verified. We are also familiar with the idea of “Nonce”. So basically miners are people that are trying to find a “Nonce” that satisfies that given target. It could be assumed as throwing darts blindfolded. While you are blindfolded, throwing to any place is equally likely but if you throw faster, you can hit the target faster. In Bitcoin, difficulty is implemented as number of “leading zeros”. Miners are earning bitcoin by verifying the blocks.(Blockchain at Berkeley, "Lecture 03 - Bitcoin Mechanics and Optimizations: A Technical Overview", 2018)

2.4 Data Within The Block

Here is a typical blockchain block

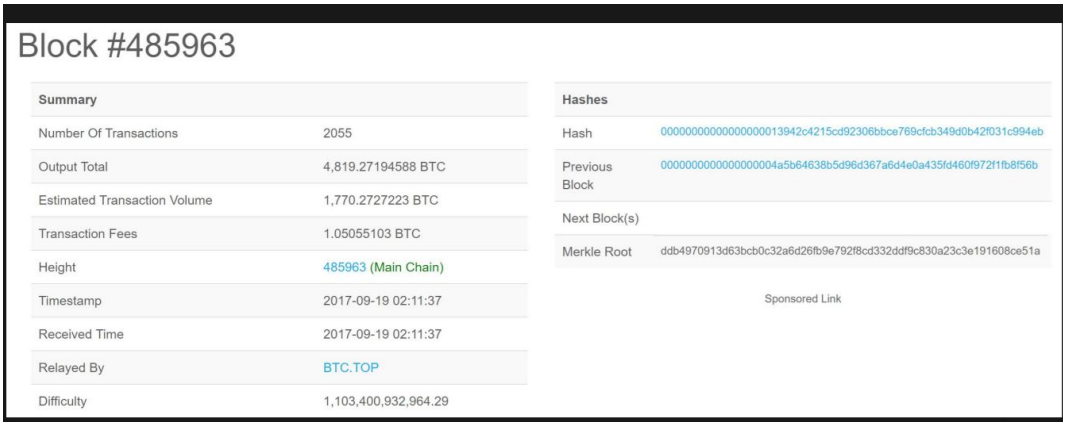


Blok #533088

özet	
İşlem Sayısı	2027
Çıktı Toplam	11,680.15888807 BTC
Tahmini İşlem Hacmi	1,283.87134135 BTC
İşlem ücretleri	0.16554144 BTC
Yükseklik	533088 (Ana Zincir)
Zaman Damgası	2018-07-22 11:38:03
Alınan Saat	2018-07-22 11:38:03
Tarafından Geçiş Yapan	BTC.com
zorluk	5,178,671,069,072.25
Uçları	389437975
Boyut	987.821 kB
Ağırlık	3417.626 kWU
versiyon	0x20000000
şimdiki zaman	897708578
Blok Ödülü	12.5 BTC

Hash'ler	
esrar	00000000000000000018f870394297a99837d75ff0a275d4e6bb61985b4797fb
Önceki Blok	00000000000000000013bc3e7abaea85bf8b5050f917b32ef1889664af21641f
Sonraki Blok (lar)	00000000000000000002951d3e7c55d648db084a352ece44c74e99a675d4cabd0
Merkle Kök	22db4c24856fe432a1d4fb845b17c1ce1a9690bff843a850aa6510e4ae539dfa

("Block #533088", 2018)



Block #485963

Summary	
Number Of Transactions	2055
Output Total	4,819.27194588 BTC
Estimated Transaction Volume	1,770.2727223 BTC
Transaction Fees	1.05055103 BTC
Height	485963 (Main Chain)
Timestamp	2017-09-19 02:11:37
Received Time	2017-09-19 02:11:37
Relayed By	BTC.TOP
Difficulty	1,103,400,932,964.29

Hashes	
Hash	00000000000000000013942c4215cd92306bbce769cfcb349d0b42f031c994eb
Previous Block	00000000000000000004a5b64638b5d96d367a6d4e0a435fd460f972f1fb8f56b
Next Block(s)	
Merkle Root	ddb4970913d63bcb0c32a6d26fb9e792f8cd332ddf9c830a23c3e191608ce51a

Sponsored Link

("Block #485963", 2017)

In the second block we can see number of transactions in it, total output of Bitcoins, transaction volume, transaction fees, height in the main chain, timestamp, received time, miner, difficulty, and hashes.

3 Ethereum

Ethereum is a decentralized platform that use smart contracts to run applications on a custom blockchain. This blockchain has powerful associated global connections that can share valuable items and contain ownership of possessions(Ethereum, 2015).

This features give opportunities to create markets, store given promises or record of charges, make action with funds based on instructions given in past and many different things that have not been think about yet.

Vitalik Buterin is a developer from Toronto who is the creator of Ethereum. He focused on the blockchain, crypto technologies and Bitcoin in 2011. Then, he created online news website Bitcoin Magazine in September 2011. After 2 years he came up with an idea of a platform that gives the opportunity to develop other decentralized application beyond the financial usage with the smart contract.(Hertig, 2017) Ethereum design based on the following 5 principles:

- **Simplicity**: Ethereum protocol should be as simple as possible to protect over data storage or time efficiency.
- **Universality**: Ethereum provides its own script language which developers can use to create contract or transaction type. Developers can build anything(...)
- **Modularity**: One of the principles of Ethereum is the modularity. Ethereum created as possible as modular and separable. This feature provides a possibility to make small modification without break integrity of the application.
- **Agility**: There is the opportunity to make the change on high-level constructs
- **Non-discrimination and Non-censorship:** As the philosophy of decentralized application, Ethereum protocols should prevent to attempt any restriction and any discrimination which come from central authorities.

3.1 Accounts

Accounts are objects that have 20 bytes addresses and able to interact with each other. There are two types of account which are external owned account and contract account. External owned accounts controlled by private keys, on the other hand, contract accounts controlled by contract code. External owned accounts can create signed transaction with its own private key then can send a message to any other external owned account or contract account. Ethereum accounts occurred by four states which are nonce, ether balance, hashed code and storage. External owned account’s nonce and contract

account's nonce are different from each other. when the account is an external owned account, nonce shows number of the sent transaction from address of the account. When the account is a contract account, the nonce shows the number of created contract by account.(Kasireddy, 2017) Storage is a Merkle tree which contains the storage content of this account. Hashed code change according to account type is external owned accounts or contract accounts as the nonce. The hashed code is a hash of EVM(Ethereum Virtual Machine) code of this account. If code belongs the contract code, it is hashed and stored code. If code belongs the external owned accounts, the code is a hashed empty string.

3.2 Transaction and Messages

Basically, transactions are data package that generated and signed by external owned accounts and includes a message, then submitted to the blockchain.All transactions contain:

- Nonce: count of the number of transactions sent by the sender.
- The recipient of the message
- The address of the sender
- The amount of the ether to transfer
- Optional data field
- The maximum amount of the gas that the sender will pay to execute the transfer
- Gas price

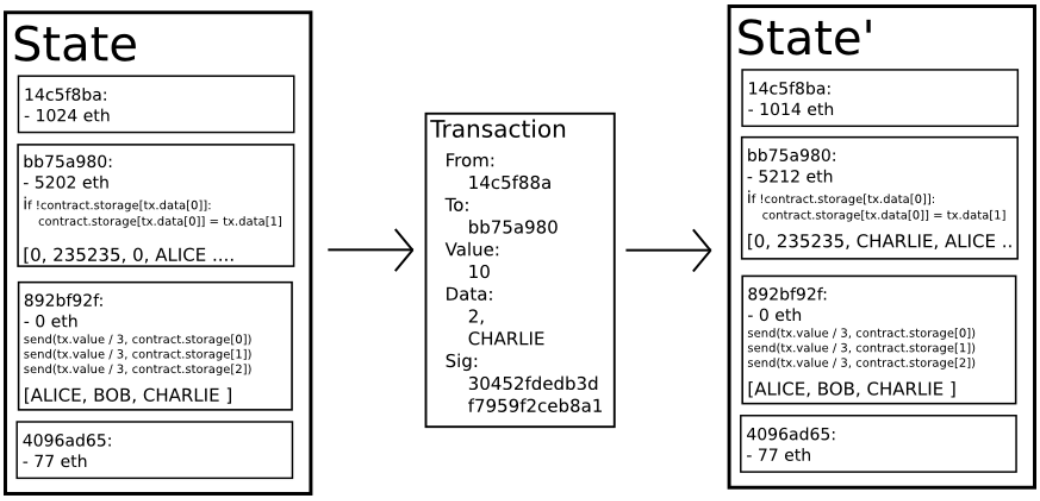


Figure 1. Ethereum state transition function (Ethereum,2015).

3.3 **Transaction Execution**

Transactions must satisfy some requirements to be executed. These includes:

- Transaction signature must be valid.
- Transaction nonce must be valid.
- The gas limit must be enough to execute a transaction.
- Sender's account must have enough ether to pay an upfront cost of the transaction. Upfront cost includes gas price x gas limit + transferred value from a sender to the recipient.

3.4 **Smart Contracts**

Smart contracts are the self-processing digital agreements between two people which written into lines of code. The code is placed and process on the distributed and decentralized blockchain network. Smart contracts give the opportunity to create the reliable environment that can make trusted transactions without the need for any central authority.(Investopedia, 2018) Ethereum gives chance developers to program their own contract with using Ethereum own script language which called Solidity.

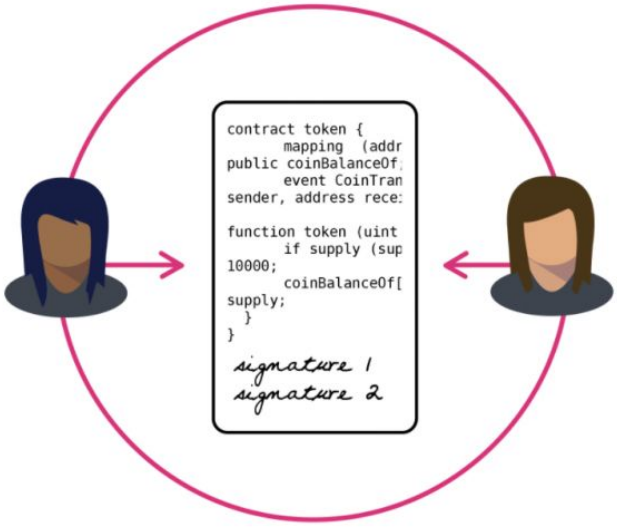


Figure 1. Smart contract (Coindesk, n.d.)

3.5 **Proof of Stake**

Proof of Stake is the consensus protocols as an alternative to proof of work, to use consensus on which block will be the next in blockchain. Generally proof of stake algorithm works as follows. Creator of next block selected by the randomized system.According to how much cryptocurrency account have or how long account has been holding that particular currency rather than computational power as proof of work system. The randomized system prevents the manipulations of blockchain otherwise, individuals who have the most amount of money in own account can manipulate the system(Ethereum, 2015).Possible advantages of proof of stake against proof of work are that:

- It reduces energy consumption while adding the new block on the blockchain.
- Because of using less energy to mining, there is no need to create many new coins in order to encourage miner to continue mining process.
- Proof of stake more secure against %51 attack than the proof of work.

3.6 Implementation of cryptocurrency within the campus

3.6.1 Puregold and the idea behind

One of the main goals of the project was to implement a cryptocurrency for in-campus usage to raise awareness about blockchain. In order to do that team made a research on popular uses of blockchain. As stated in previous sections Bitcoin and Etherium were among them.

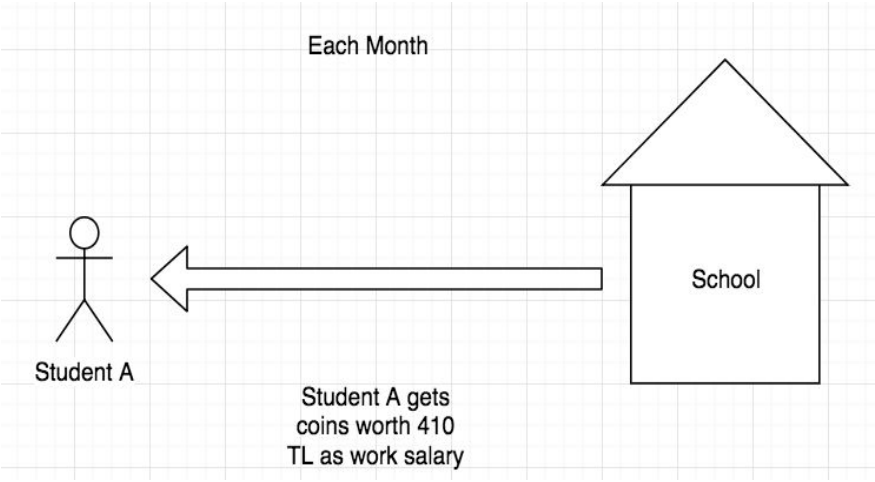
Team tried to come up with a design idea in order to implement a cryptocurrency which is mainly aimed to work on campus. To do this, team looked for design ideas among popular cryptocurrencies. For example, Bitcoin inherits a reward system for users. However, to implement a similar system for in-campus usage, there needs to exists a consistent trade among students and staff.

However, teams intention was to design a system for Sabancı University. Sabancı University campus life lacks these kind of trades between students. Teams main focus was students because the majority of the population in campus is students.

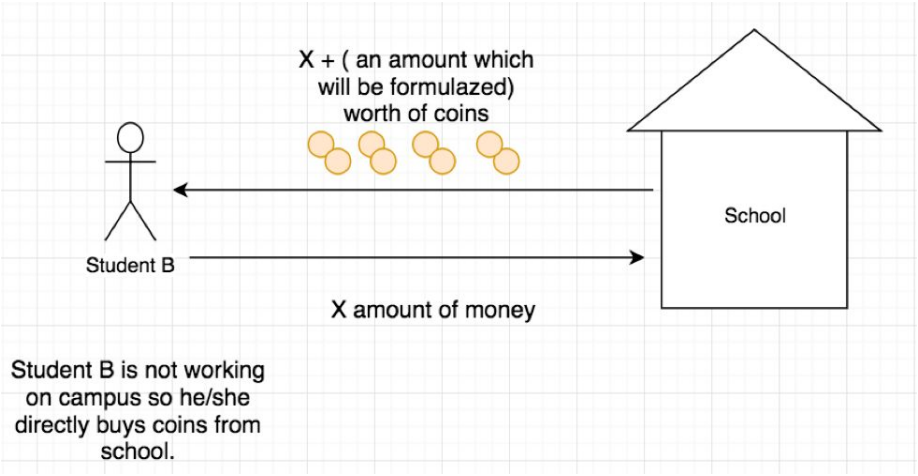
At that point team and supervisor decided to propose a "discount" idea on the design in order to potentially increase the usage and interest towards the concept. In addition, team and supervisor decided to name the coin "Puregold" due to this Project being a PURE Project.

The design goes likes this; There exists a quite high number of students who also work in campus. Such as equipment operator, library staff, academic support program and etc. And these students get paid each month accordingly.

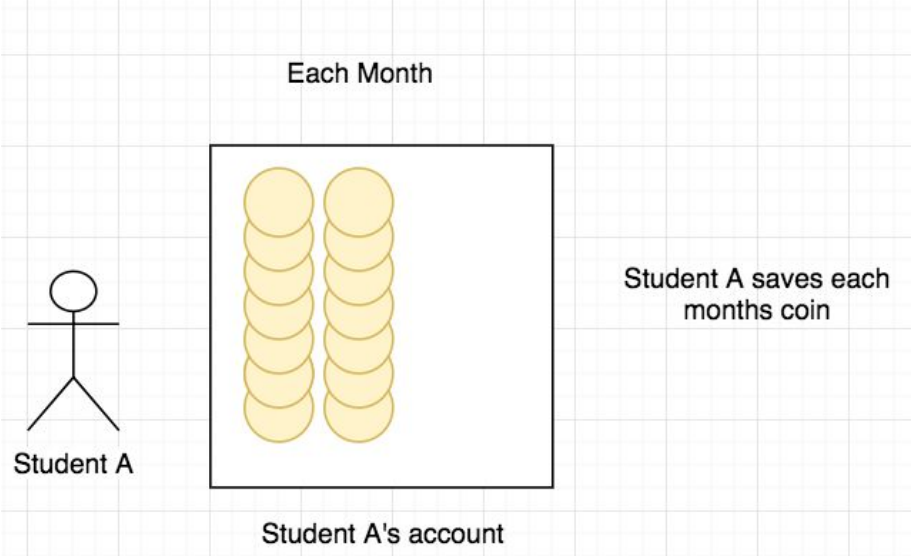
A portion of the work salary is given as coins to everyone who gets paid by school. In this way, the designed cryptocurrency enters the flow cycle in campus. The ones who do not work in campus can also directly purchase the coins.



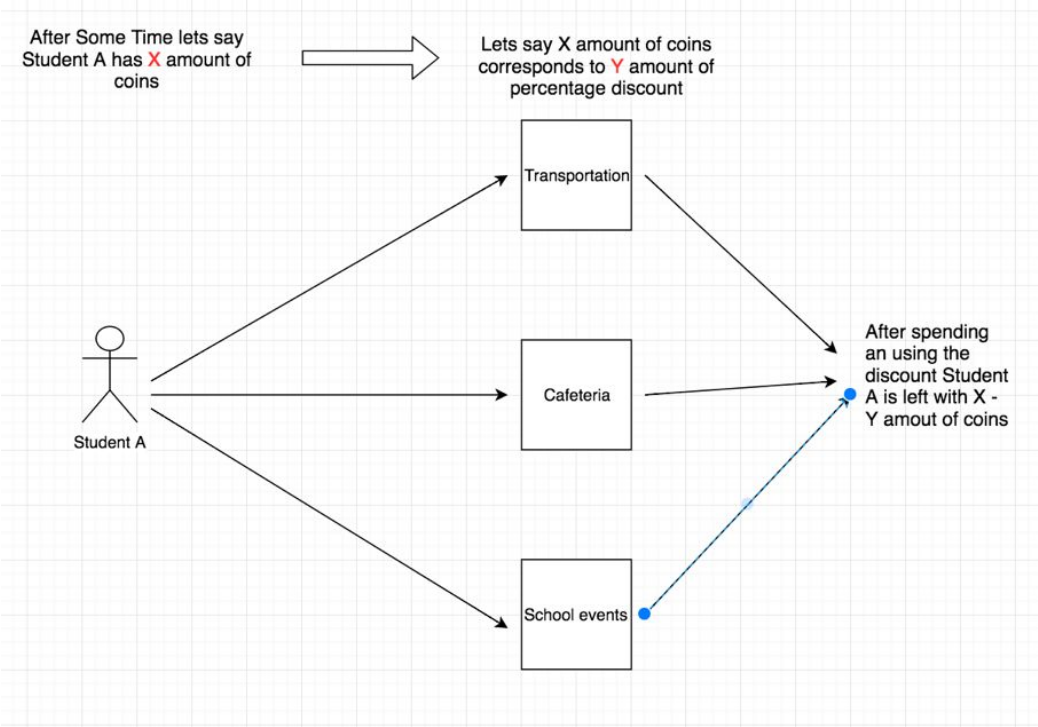
Or if the student is not working in campus:



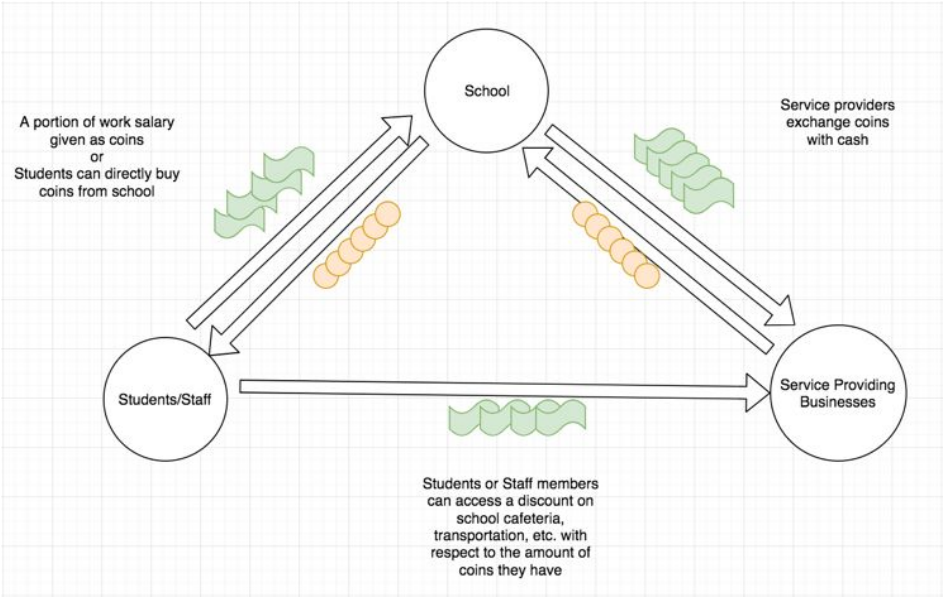
Then, the amount of coins that a student or staff have corresponds to discount value. By each months salary, coins stack up and correspond to a greater discount value. Of course this discount value is capped at some limit.



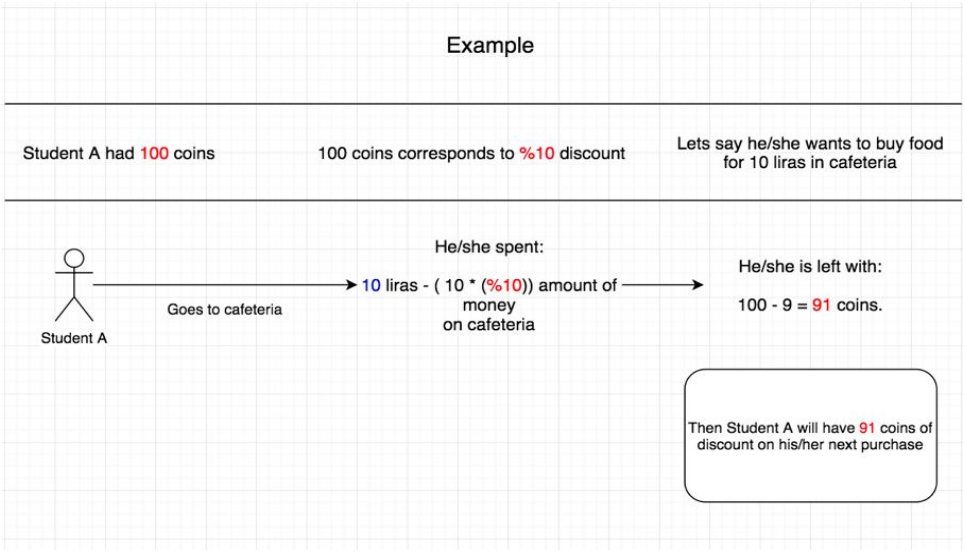
Then this discount value that student or staff obtained through having coins, will be usable for their next in-campus purchases.



After the purchases, coins are collected by service providing businesses in campus. Then these businesses such as cafeteria and transportation company will exchange the collected coins with money with school in order to complete the cycle.
Here is a diagram to show whole flow of the designed coin system;



And also there is a math behind the system which corresponds to the discount values calculation before and after the purchase. Here is an example case shown in a diagram which explains the mathematics behind the idea:

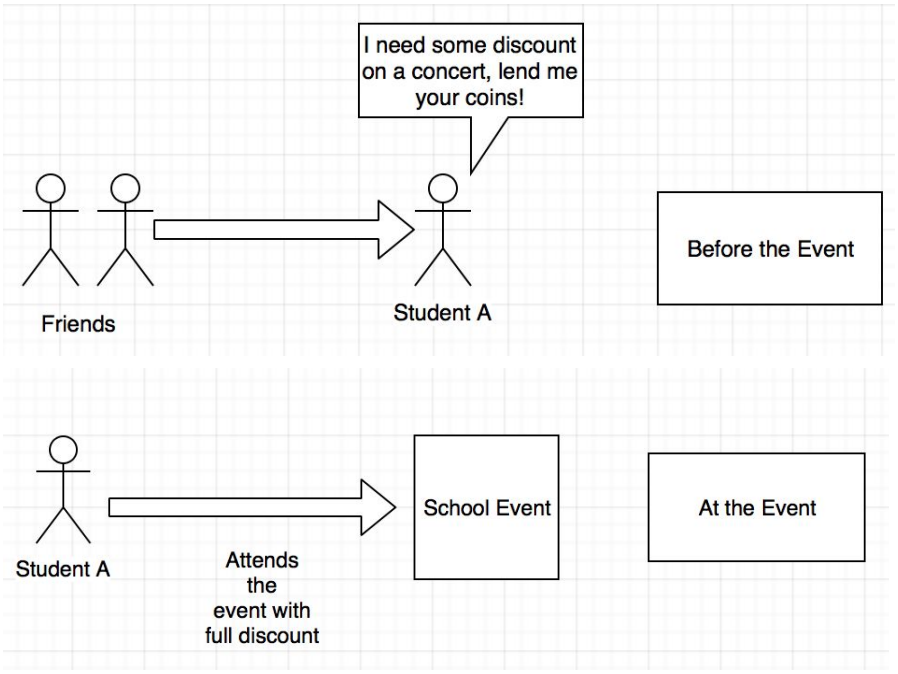


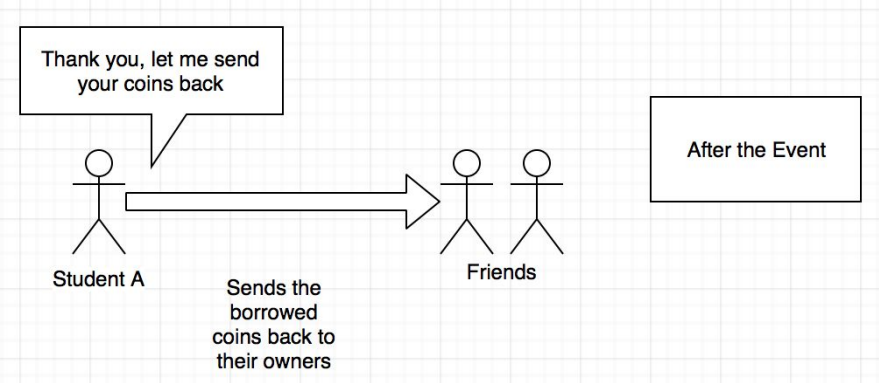
3.6.2 Abuse Cases

As all cryptocurrencies have potential abuse cases such as double spending, Team also spent time on to figure out what might be the possible abuse cases for Puregold as well.

3.6.2.1 Potential Abuse Cases

1) Short term coin transfer among students to abuse the discount on school events or purchases.



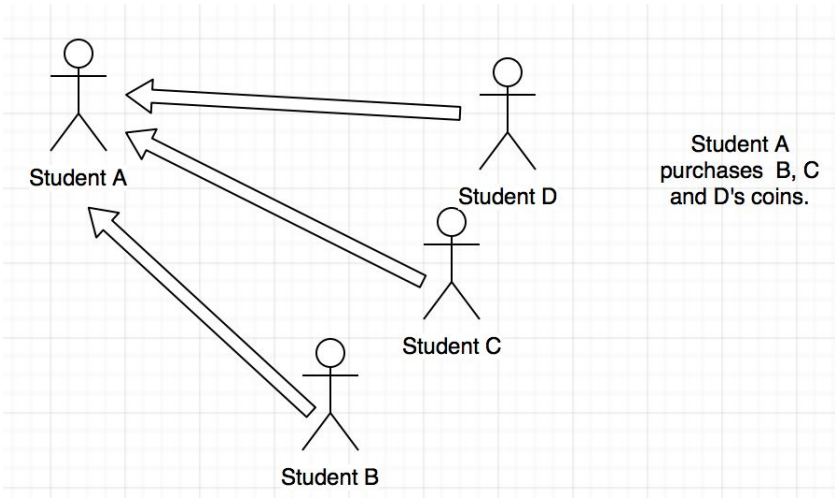


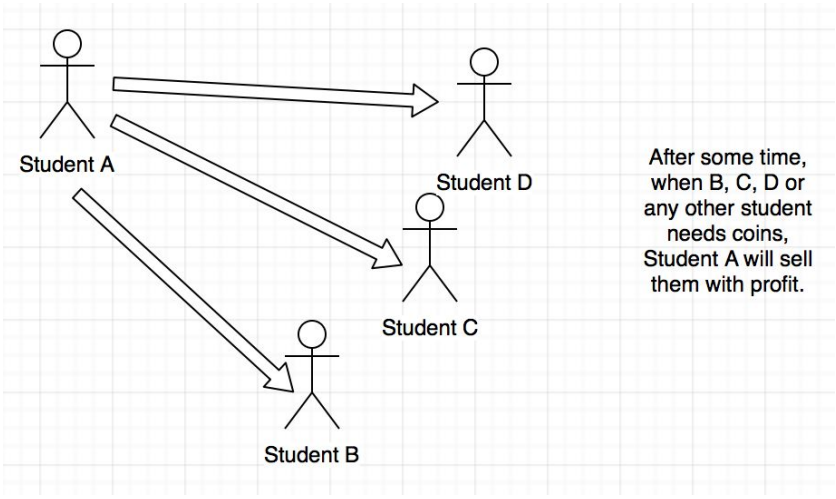
Possible solutions:

- A transaction fee will most likely to avoid this problem. Assuming Student A is not stealing, he/she will give the borrowed coins back, at this point a transaction fee with respect to the amount of coins being transferred will solve the case.

- A time limitation for transactions will also help to avoid this potential abuse case. Adding timestamps to the transactions. Say X amount of time needs to pass in order to use the coins which was obtained from a student to student transaction.

2) Some can use coins as a black market in order to make profit





Possible solutions:

- Setting a limit for coins at the student side. Meaning, a student will at most have X amount of coins (which corresponds to maximum discount). So no user can stack coins later to make profit.

4 Future Work and Further Studies

Team and supervisor concluded that, to implement and run this system in real life there are few things that should be done;

- Interview the service providing businesses in campus to understand their standing on the subject to know whether they would choose to use Puregold or not to choose.
- Considerable amount of coding needs to be done in order to implement both Puregold and the system that runs it in campus network.
- Interview also the students to know whether if they would like to use cryptocurrency in in-campus purchases.

- Propose the idea to Sabanci University administration in order to get their idea about the system.

The work that had been done for Puregold by the team did not match these conditions in the given time. That is why Puregold is currently an idea to begin with. However, it is open to development and execution for future works and projects. Also, the design itself is flexible in the sense that it could be executed in any campus life since all of them are quite similar. So if one administration would reject, it can be proposed to an another one.

Overall, this projects aim was to explore blockchain technologies and come up with a similar idea which may work in campus to raise awareness and encourage people to learn about blockchain technologies. In that sense, Puregold quite fits the needs for future studies and improvements.

References

Brin, S., Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. In: Seventh International World-Wide Web Conference (WWW 1998), April 14-18, 1998, Brisbane, Australia.

Einstein, A., Podolsky, B., Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47 (10), 777-780. doi: 10.1103/PhysRev.47.777.

Hofstadter, D. R. (1979). *Gödel, Escher, Bach: An Eternal Golden Braid*. New York, NY: Basic Books Inc.

N., G., B., & S. (n.d.). *Blockchain at Berkeley*. Lecture presented at Blockchain at Berkeley, Berkeley.

Blockchain use cases [Digital image]. (n.d.). Retrieved from https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99

[Simplified Bitcoin Blockchain]. (n.d.).
Retrieved from Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview

How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes. (2018). Retrieved 2018.

Lecture 03 - Bitcoin Mechanics and Optimizations: A Technical Overview. (2018). Lecture, Berkeley.

Lecture 01 - Bitcoin Protocol and Consensus A High Level Overview. (2018). Lecture, Berkeley.

[Slide that retrieved from "Lecture 03 - Bitcoin Mechanics and Optimizations: A Technical Overview"]. (2018). Retrieved 2018.

Block #533088. (n.d.). Retrieved July 20, 2018, from https://www.blockchain.com/btc/block/000000000000000000018f870394297a99837d75ff0a275d4e6bb61985b4797fb

Your Bibliography: Kasireddy, P. (2017). *How does Ethereum work, anyway?*. [online] Medium. Available at: https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369 [Accessed 7 Aug. 2018].

Ethereum. (n.d.). ethereum/wiki. Retrieved August 7, 2018, from https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-proof-of-stake

Ethereum. (2015, July 30). ethereum/wiki. Retrieved August 7, 2018, from https://github.com/ethereum/wiki/wiki/White-Paper

Hertig. (2017, March 30). Who Created Ethereum? Retrieved from https://www.coindesk.com/information/who-created-ethereum/

Ethereum. (2015). *Ethereum state transition function* [diagram]. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper

Coindesk. (n.d.). *smart contract*. Retrieved from https://media.coindesk.com/uploads/2017/03/Screen-Shot-2017-03-28-at-5.43.08-PM-728x539.png