# 1. Novel Idea

The paper presents a new type of decentralized electronic cash system called Bitcoin. It allows payments to be sent online, directly from one party to another and doesn’t require third parties to prevent double-spending problems.[1]

# 2. Main Result(s)

The main result of this paper is that it theoretically proves the feasibility of the Bitcoin system. It analyzes the structure of the system through ten sections: describe the transactions process, use a timestamp server to prevent double-spending, show the proof-of-work, demonstrate the construction of the network, use incentive as transaction fees in order to prevent inflation and help nodes to stay honest, prove storage will not be a problem for the system, discuss the simplified payment verification, demonstrate how combining and splitting value work, keep public keys anonymous in order to protect privacy and show calculation that the system has very low probability being changed.[1]

# 3. Impact

These results are important not only because it proves the feasibility of the construction of the Bitcoin, but also it is a practical implementation of blockchain computing. The invention of the Bitcoin established a new cash payment system that is inflation free, highly privacy, unsupervised by the government, extremely safe and independent.

The key technology of Bitcoin is a new invention on computer systems: blockchain computing. It has five major technical elements: distributed databases that no single party controls and everyone has access to the entire database and whole history, peer-to-peer transmission that make communication only between nodes and each node stores and forwards information to all other nodes, transparency with pseudonymity that keep payment visible and anonymous, irreversibility of records that keep the accounts are updated but unalterable, computational logic that algorithms and rules can be used to trigger transactions automatically.[2]

The invention of blockchain computing has profound impact on the practice of computer systems. It allows information to reside on multiple systems, even millions of them, simultaneously.[3] Which means any information such as data, identities, currency, communication, calculation and etc is eligible for using this technology to implement practical applications. Therefore it is a game changer for the old practical computer systems, for example, customers no longer need to pay fees to the banks, insurance companies, property companies and traders for their integrity[3] because Bitcoin can replace the old payment system.

In conclusion, the results of the paper have great impact on the practice of computer systems, and the prospect of blockchain computing has great potential.

# 4. Evidence

For transactions, the author uses a figure to demonstrate the structure of the electronic coin and payment process: the electronic coin itself is a chain of digital signatures, to make payment, digitally sign a hash of the previous transaction and the public key of the next owner and add them to the end of the coin. Payee can verify the signatures to confirm the chain of ownership.[1]

For timestamp server, the author uses a figure to demonstrate the implementation of timestamp server: take a hash of a block of items to be timestamped and widely publish it[1] It is the solution of the problem raised by the end of the transactions section: double-spending.

For proof-of-work, the author uses a figure to demonstrate the process of distributed timestamp server implementation: increment a nonce in the block until a value is found that gives the block’s hash the required zero bits.[1] The author also uses a moving average as the reason that the proof-of-work difficulty is dynamic in order to compensate for increasing hardware speed and varying interest in running nodes over time.[1]

For network, the author uses a step list to demonstrate the steps to run the network, indicates that nodes always consider the longest chain to be the correct one and keep working on extending it and new transaction broadcasts do not have to reach all nodes.[1]

For incentive, the author uses empirical analysis to explain the result: by convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. The incentive can also be funded with transaction fees in order to be completely inflation free, and the incentive may help encourage nodes to stay honeset.[1]

For reclaiming disk space, the author uses a figure and mathematical calculation and Moores’ Law prediction to support his result: storage should not be a problem even if the block headers must be kept in memory.[1]

For simplified payment verification, the author uses a figure to demonstrate the payment verification without running a full network node. However, the author uses empirical analysis to remind that: if the network is overpowered by an attacker, the internet is vulnerable, so businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.[1]

For combining and splitting value, the author uses a figure to demonstrate the process of combining and splitting value: transactions contain multiple inputs and output.[1]

For privacy, the author uses a figure to compare the traditional privacy model and new privacy model, in order to support the result: the public can see the sending process, but can’t link the transaction to anyone.[1]

For calculations, the author uses mathematical probability calculation to show the probability of an attacker trying to change one of his own transactions to take back money he recently spent[1], the result is that the probability is very low, therefore the system is secure.

# 5. Prior Work

The establishment of Bitcoin builds upon both theoretical and practical outcomes previously published.

The theoretical outcome is b-money, two protocols introduced in the paper: one is impractical due to heavy use of a synchronous and unjammable anonymous broadcast channel[4], one is more practical. The first protocol introduces that all participants maintain a part of the money database, the transfer of money is a broadcast process. The second protocol is that money is kept by servers instead of everyone, the servers are linked by a Usenet-style broadcast channel. The translation process is the same as the first protocol, but the verification is a randomly selected subset of the servers. The b-money is the theoretical model of an untraceable pseudonymous entity, the Bitcoin implements the idea and solves trust and double-spending problems.

One of the practical outcomes is Hashcash, it introduces a hashcash CPU cost-function that computes a token which can be used as a proof-of-work.[5] In this paper, the author uses a similar proof-of-work system to support his research.

Another practical outcome is timestamping. Timestamp is a digital record of time when the event occurred. It was a well-developed and widely-used technology. From the explanations and references in the paper, the author uses this practical result to solve the double-spending problem by designing a working timestamp server.

The last practical outcome is the use of probability theory. The author uses a probability model introduced by William Feller[6] to calculate the chance of an attacker trying to change one of his own transactions to take back money he recently spent[1], in order to prove the safety of the Bitcoin.

# 6. Competitive work

These results are the consummations to the prior works and the fundamentals of the contemporary works. Based on the prior work results, the author introduces a theoretically functional peer-to-peer electronic cash system. Furthermore, by using practical technologies such as timestamping, proof-and-work and probability theory, the author solves the problem that exists in b-money and proves the feasibility of Bitcoin.

The reason these results are the fundamentals of contemporary works is that most modern crypto currencies are developed and implemented based on these results. For example, the most fundamental technical difference between Bitcoin and Litecoin are the different cryptographic algorithms that they employ. Bitcoin makes use of the longstanding SHA-256 algorithm, whereas Litecoin makes use of a comparatively new algorithm known as Scrypt.[7], Since these results are first published and Bitcoin is the first crypto currency, they are the basis of contemporary peer-to-peer electronic cash systems.

# 7. Reproducibility

Yes, these findings can be reproduced.

The author uses figures in transactions, timestamp server, proof-of-work, reclaiming disk space, simplified payment verification, combining and splitting value and privacy sections to show the structure of the corresponding part of the system. Plus, with the explanations surrounded, such as “by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin”, “by taking a hash of a block of items to be timestamped and widely publishing the hash”, “only needs to keep a copy of the block headers of the longest proof-of-work chain”[1], 6 steps in network construction and etc are detailed enough to reproduce the results. Although they are not programming languages, these steps can be considered as pseudo code, which are feasible for algorithm design and implementation.

# 8. Question

How to judge the value of Bitcoin?

It is common knowledge that the production and distribution of the currency is based on the government's integrity, the use of currency links to real life products which the goal is to exchange for entities. The production and distribution of Bitcoin is based on CPU power, but we can’t just simply link the value of Bitcoin to CPU power - electricity price. As long as the government denies the legitimacy, Bitcoin is equivalent to nothing realistic but a set of virtual data.

On the other hand, it is a type of currency that can be controlled: those who have more resources in real life have more power and energy to produce more bitcoin. Since the total number of Bitcoins is a fixed number - 21 million[8], the situation may come true as a small number of people own the most Bitcoin resources and the Bitcoin market is under control. Therefore its value can be theoretically manipulated.

# 9. Criticism

The invention of Bitcoin provides an untraceable payment method which can be used in criminal or terror activities. Due to its anonymity, law enforcement is not able to identify the criminals, terrorist or terror groups, which is a huge security breach for all countries in the world. It threatens society order and nation security. According to the research, even a terrorist organization locked out of the traditional financial system, they can use crypto currency like Bitcoin to raise money: Terrorists have been slow to join other criminal elements that have been drawn to Bitcoin and have used it for everything from drug purchases to money laundering[9]. Therefore, this work is a double sided sword, the technology results can both benefit and threaten human civilization.

# 10. Ideas for further work

Based on the features of these results, I think this system can be used in instant messaging.

For example, an anonymous communication community. Everyone uses their CPU power as costs to create their block, able to embed messages into the block and broadcast it to everyone else in the network. All members have access to read all messages including message history and post theirs simultaneously.

Another example is company private blockchains. Similar to the previous scene, as long as the members in the communication network are trustable, the communication only visible to all members inside the network, while the network is under control by the group. The members can add their identification to the message for other members to recognize, otherwise they stay anonymous.

# 11. References

1. Satoshi Nakamoto. “Bitcoin:‌ ‌A‌ ‌Peer-to-Peer‌ ‌Electronic‌ ‌Cash‌‌ System”, October 31, 2008.

2. Marco Iansiti and Karim R. Lakhani. “The Truth About Blockchain”. https://hbr.org/2017/01/the-truth-about-blockchain. January–February 2017.

3. Richard Kestenbaum. “Why Bitcoin Is Important For Your Business”. https://www.forbes.com/sites/richardkestenbaum/2017/03/14/why-bitcoin-is-important-for-your-business/#593f2d0541b5. 2017.

4. W. Dai, “B-money”. http://www.weidai.com/bmoney.txt, 1998.

5. Adam Back. “Hashcash - A Denial of Service Counter-Measure”. 1st August 2002.

6. W. Feller. “An introduction to probability theory and its applications”. 1957.

7. Jason Fernando.“Bitcoin vs. Litecoin: What's the Difference?”. https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp. Jun 25, 2019.

8. Buybitcoinworldwide. “Total Number of Bitcoins”. https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/. May 18,2020.

9. Homeland Security News Wire. “Terrorists Turn to Bitcoin for Funding, and They’re Learning Fast”. http://www.homelandsecuritynewswire.com/dr20190819-terrorists-turn-to-bitcoin-for-funding-and-they-re-learning-fast. 19 August 2019.