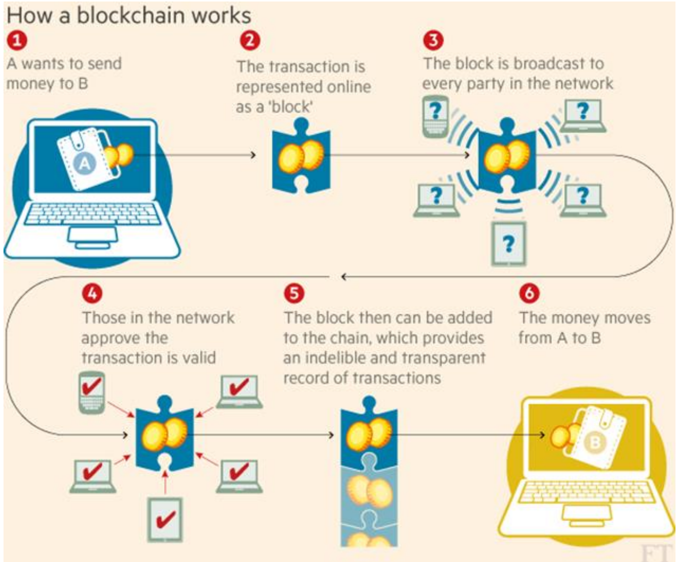
BRANDON UNIVERSITY

September 2018 – Issue 2(1)

RESEARCH CONNECTION

The future of blockchain technology

By Gautam Srivastava, Ph.D., Ashutosh Dhar Dwivedi, Ph.D. candidate, & Rajani Singh. Ph.D. candidate


How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Source: The Financial Times.

Why this research is important

With most of, if not all, public and private documentation moving into a digital form, new and innovative ways to store, share, and protect that data becomes of the utmost importance. Bitcoin started to emerge in 2009, but only recently it became a water cooler discussion topic with its value skyrocketing. The technology behind Bitcoin and other cryptocurrencies known as blockchain has been viewed as the future of information sharing. Different ways of using blockchain technology in a multitude of areas are being heavily researched; sometimes behind the scenes as to not give any legitimacy to cryptocurrency by banks and governments who rely on physical currencies to run the world.

> What you need to know
>
> The blockchain is the core mechanism for cryptocurrencies like Bitcoin. Blockchain technology can be regarded as a public ledger, in which all committed transactions are stored in a chain of blocks. This technology has far-reaching possibilities of applications beyond finance in areas such as healthcare, voting systems, and civil document management to name just a few.

How the research was conducted

The beginnings of any computer science or mathematical research are always based on strong theoretical, provable results. Therefore, most of this preliminary research on blockchain technology was done ensuring that the technology is robust and technically sound.

We introduced a more advanced blockchain voting management system utilizing a Directed Acyclic Graph of blocks—aka **blockDAG**—a generalization of blockchains which better suits a setup of fast or large blocks. Our system uses a repetitive process on the **blockDAG** to distinguish between blocks mined properly by trustworthy miners and those mined by noncooperating miners that deviated from the mining protocol.

What the researchers found

To date, we have explored the possibilities of implementing blockchain technology in voting systems. One of the biggest problems plaguing society today is that of fraudulent elections. The world's largest democracies still suffer from flawed electoral systems. In current voting systems, we see problems with vote rigging, hacking of the EVM (Electronic Voting Machine), election manipulation, and polling booth capturing. We have proposed a novel voting model, which can resolve these issues. Using blockchain technology, we try to alleviate known problems in voting systems. Furthermore, the advantage of using our model is that it is compatible with all voting schemes. So, one can implement our model using any voting scheme depending on the requirement of the different type of elections.

We have also explored the on-going "GAME" that exists between the miners in Bitcoin. Miners in bitcoin receive reward payments for confirmation of transactions, thereby making the mining of bitcoins a competitive activity. We have found provable results stating that it is better for miners to work together to mine bitcoins rather than against each other. These findings are not only in the best interests of the miners but for the currency itself.

How this research can be used

We see research in blockchain technology taking over many public services. Since the blockchain is secure, decentralized, and can be easy to use, it can have far-reaching uses in all facets of public administration. To date, we have seen certain countries adopt blockchain technology for some of their services. A quick top ten uses: (1) money transfers, (2) supply chains, (3) loyalty rewards programs, (4) digital IDs, (5) copyright protection, (6) digital voting, (7) title transfers, (8) tax regulation, (9) medical recordkeeping, and (10) wills or inheritances.

About the researchers

Dr. Gautam Srivastava is an Associate Professor of Mathematics and Computer Science at Brandon University. Ashutosh Dhar Dwivedi (Polish Academy of Sciences), and Rajani Singh (University of Warsaw) are Ph.D. students. srivastavag@brandonu.ca

Keywords

Blockchains; bitcoin; cryptography; hash functions; directed graphs

Publications based on this research

Dwivedi, A. D., Singh, R., & Srivastava, G. (2018, forthcoming). PHANTOM protocol as the new Crypto-democracy. *Proceedings of the International Conference on Computer Information Systems and Industrial Management Applications* (CISIM).

Srivastava, G., Dwivedi, A. D., & Singh, R. (2018). Crypto-democracy: A decentralized voting scheme using blockchain technology. *Proceedings of the International Conference on Security and Cryptography* (SECRYPT).

Dwivedi, A. D., Singh, R., & Srivastava, G. (2018). A democratic future using a decentralized blockchain voting scheme. *Proceedings of the 41st International Central European Conference on Cryptography* (CECC).

Acknowledgements

Research was supported by BURC during the early stages of the project.

Research Connection is a periodical publication intended to provide information about the impact of Brandon University's academic research and expertise on public policy, social programming, and professional practice. This summary is supported by the Office of Research Services and by the Centre for Aboriginal and Rural Education Studies, Faculty of Education.

Editor: Christiane Ramsey Ramseyc@Brandonu.ca

http://www.brandonu.ca/research-connection