Facilitating the Decentralised Exchange of Cryptocurrencies in an Order-Driven Market

KING'S College LONDON

2nd conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 28-30 Sep 2020

Moritz Platt (*Presenter*)*, Francesco Pierangeli*, Giacomo Livan, Simone Righi****

*King's College London, **University College London

Agenda

1. **Centralised Exchanges *(CEX)* vs. Decentralised Exchanges *(DEX)***—Two different paradigms creating different risk profiles for traders

2. **Protocol**—Combining centralised and decentralised elements and the need for performance scoring

3. **Future Work**—Addressing the trade-off between anonymity and reliability in a decentralised environment via a zero-knowledge protocol

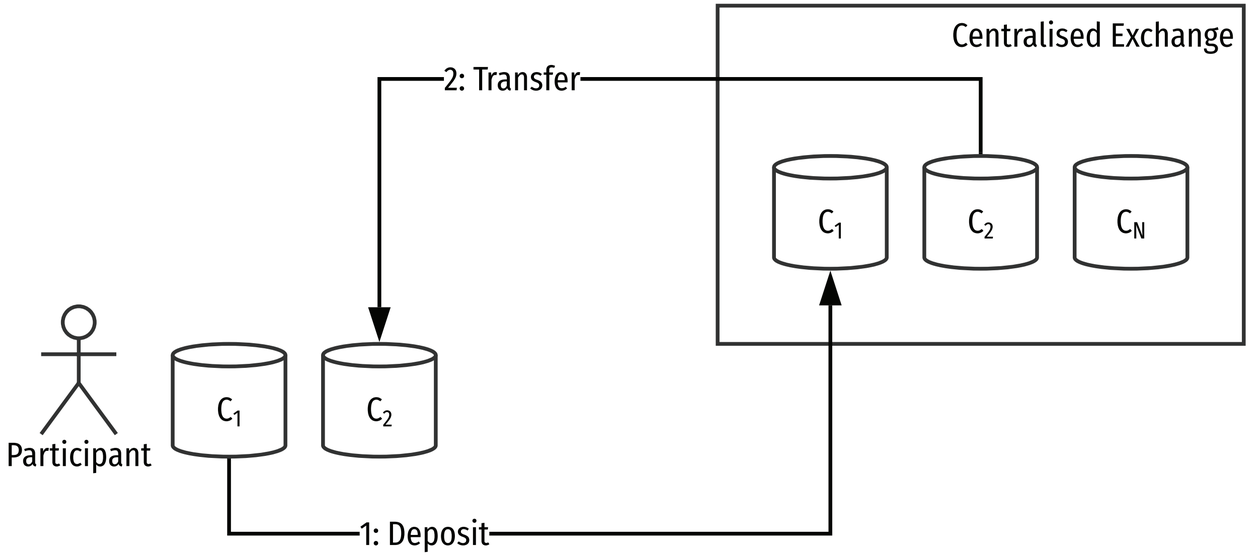
CEX by Trade Volume

	Name	Volume (24h)	Volume (7d)	Volume (30d)	No. Markets
1	BKEX	$3bn	$18.3bn	$74bn	100
2	Fatbtc	$2.8bn	$16.1bn	$66bn	114
3	BiKi	$2.4bn	$13.5bn	$57bn	92
4	BitForex	$2.4bn	$15.1bn	$60bn	153

USD rounded, CoinMarketCap (2019)

- All commercially relevant exchanges on the market today operate in a centralised manner
- Centralised exchanges provide market-making capabilities by holding a reserve of crypto-currencies, standing ready to buy currency and to sell
- Well understood model based on the same principles as foreign exchange spot trading of fiat currencies

Anatomy of a *CEX*



- Participants deposit currency into exchange account
- Exchange pays out funds at agreed rate to recipient account
- Business model reliant on fees and bid-ask-spread (Bundi and Wildi, 2019)

Risk of Misappropriation of Funds in Transit in *CEX*

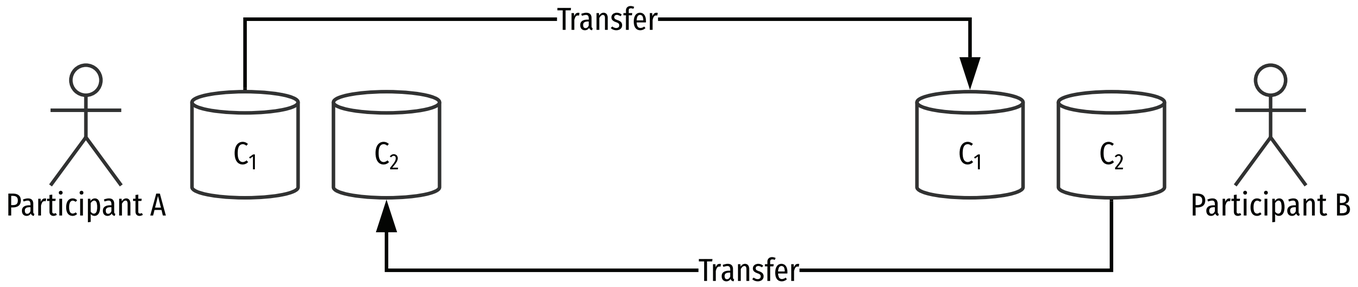
Chohan (2018) outlines collates high-profile incidents:

Year	Exchange	Impact
2011	Mt. Gox	$8m
	Bitomat	$220k
	MyBitcoin	$800k
2012	Bitcoinica	$460k
	Bitcoin Savings and Trust	$5.6m
	Bitfloor	$250k

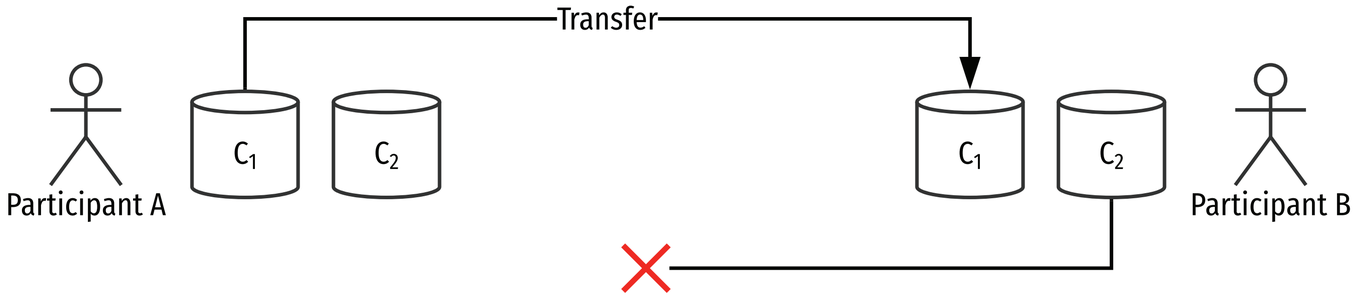
Year	Exchange	Impact
2012	Bitfloor	$250k
2013	Instawallet	$4.6m
	Inputs.io	$730k
	Global Bond Limited	$5m
2014	Mt. Gox	$390m
2015	Bitstamp	$5.1m

USD rounded

Naïve *DEX*

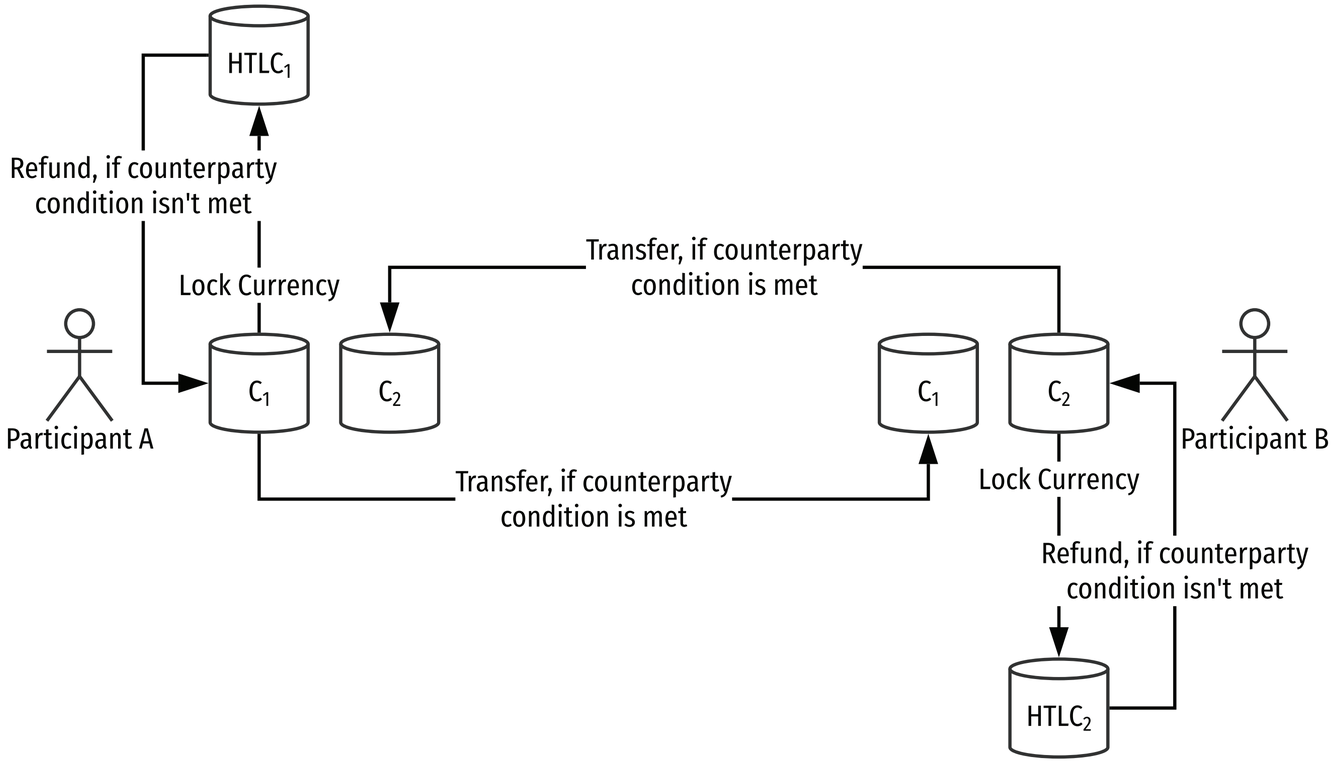


- *A* transfers a previously agreed amount of C_1 to *B* who in turn transfers a previously agreed amount of C_2 back to *A*
- Transactionality of transfers is key



Transactional *DEX*

- The prevalent paradigm utilised to enable ‘atomic’ swaps between different cryptocurrencies are ‘Hashed Time-Locked Contracts’ (HTLC)
- Most commercially relevant cryptocurrencies can be connected via HTLC (Griffith, 2019)



Exchange Paradigms

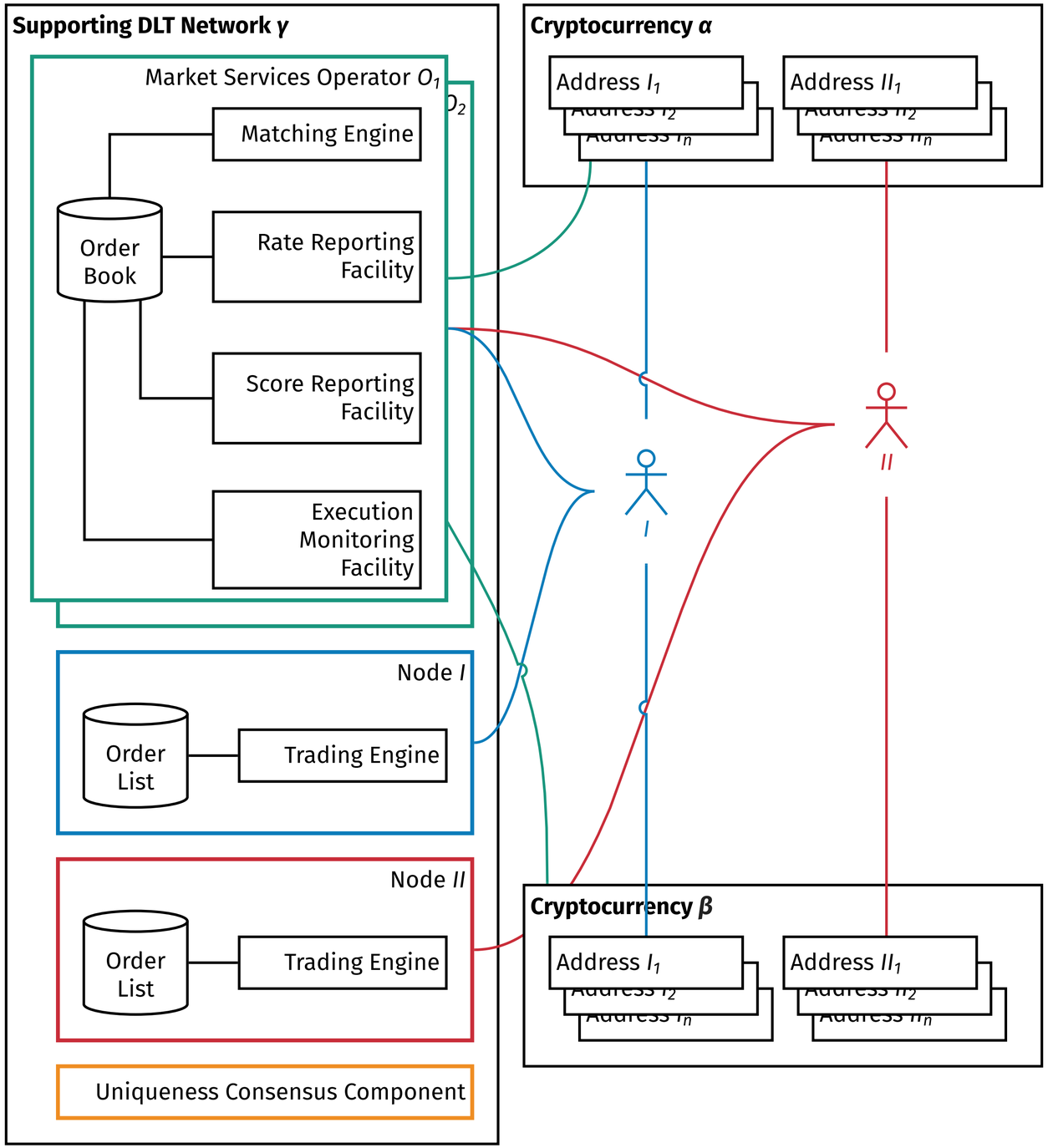
Within paradigms, different aspects are beneficial to traders:

Aspect	CEX	DEX
Risk of misappropriation of funds in transit	High	**None**
Exclusion of participants	Feasible	**Unfeasible**
Direct trading costs	Prevalent	**None**
Trading partner discovery	**Trivial**	Complex
Exchange rate transparency	**Transparent**	Opaque
Opportunity costs due to tied capital	**Low**	High

Protocol Implementation

- Multi-stage protocol that facilitates HTLC-based decentralised exchanges
- Designed to alleviate the downsides of decentralised exchanges:
  - Complicated trading partner discovery
  - Opaque exchange rates
  - Opportunity costs incurred from failed trades
- Introduces a ‘supporting distributed ledger’ to facilitate trades
- Supporting ledger is not involved in the actual execution of trades, thus maintaining the advantages of decentralised exchanges
  - No risk of misappropriation of funds in transit
  - No direct trading costs
  - Censorship resistancy

System Design



Conclusion

- We show how combining centralised elements with decentralised technology can ease trading partner discovery, thus lowering the friction during the preliminary phase of a trade
- We show how performance scoring can lower opportunity costs by reducing the risk of trades falling through

Future Work

- Performance scoring is the main driver for centralisation
- Can we do better, i.e. make performance scoring work in a decentralised fashion?
- Zero-knowledge proofs for successful/failed trade volumes?

Bibliography

Black, Matthew, and TingWei Liu and Liquality Team. 2018. 'Hashed Time-Locked Contracts.' EIP 1630. https://github.com/matthewjablack/EIPs/blob/EIP-1630/EIPS/eip-1630.md.

Bolici, Francesco, and Sara Della Rosa. 2016. 'Mt. Gox Is Dead, Long Live Bitcoin!' In *Empowering Organizations*, edited by Teresina Torre, Alessio Maria Braccini, and Riccardo Spinelli, 285–96. Cham: Springer International Publishing.

Bowe, Sean, and Daira Hopwood. 2017. 'Hashed Time-Locked Contract transactions.' BIP 199. https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki.

Bundi, Nils, and Marc Wildi. 2019. 'Bitcoin and Market-(in)efficiency: A Systematic Time Series Approach.' *Digital Finance*, March. https://doi.org/10.1007/s42521-019-00004-z.

Chiarella, Carl, and Giulia Iori. 2002. 'A Simulation Analysis of the Microstructure of Double Auction Markets.' *Quantitative Finance* 2 (5): 346–53. https://doi.org/10.1088/1469-7688/2/5/303.

Chohan, Usman. 2018. 'The Problems of Cryptocurrency Thefts and Exchange Shutdowns.' *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3131702.

CoinMarketCap. 2019. 'Top 100 Cryptocurrency Exchanges by Trade Volume.' November 2019. https://coinmarketcap.com/exchanges/coinbene/.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2019. 'Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges.' http://arxiv.org/abs/1904.05234.

Deng, Liping, Huan Chen, Jing Zeng, and Liang-Jie Zhang. 2018. 'Research on Cross-Chain Technology Based on Sidechain and Hash-Locking.' In *Edge Computing – Edge 2018*, edited by Shijun Liu, Bedir Tekinerdogan, Mikio Aoyama, and Liang-Jie Zhang, 144–51. Cham: Springer International Publishing.

Franke, Jürgen, Wolfgang Karl Härdle, and Christian Matthias Hafner. 2019. 'Financial Econometrics of Cryptocurrencies.' In *Statistics of Financial Markets: An Introduction*, 545–68. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-13751-9_23.

Gandal, Neil, and Hanna Halaburda. 2014. 'Competition in the Cryptocurrency Market.' Working Papers 14-17. NET Institute. https://EconPapers.repec.org/RePEc:net:wpaper:1417.

Griffith, Trey. 2019. 'Atomic Swap Readiness.' June 2019. https://swapready.net/.

Herlihy, Maurice. 2018. 'Atomic Cross-Chain Swaps.' In *Proceedings of the 2018 Acm Symposium on Principles of Distributed Computing*, 245–54. PODC '18. New York, NY, USA: ACM. https://doi.org/10.1145/3212734.3212736.

Herlihy, Maurice, Barbara Liskov, and Liuba Shrira. 2019. 'Cross-Chain Deals and Adversarial Commerce.' *Proc. VLDB Endow.* 13 (2): 100–113. https://doi.org/10.14778/3364324.3364326.

'IDEX: A Real-Time and High-Throughput Ethereum Smart Contract Exchange.' 2019. Aurora Labs. https://idex.market/static/IDEX-Whitepaper-V0.7.6.pdf.

Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982. 'The Byzantine Generals Problem.' *ACM Trans. Program. Lang. Syst.* 4 (3): 382–401. https://doi.org/10.1145/357172.357176.

Lin, Lindsay X. 2019. 'Deconstructing Decentralized Exchanges.' *Stanford Journal of Blockchain Law & Policy*, January, 58–77. https://stanford-jblp.pubpub.org/pub/deconstructing-dex.

Miraz, Mahdi H., and David C. Donald. 2019. 'Atomic Cross-Chain Swaps: Development, Trajectory and Potential of Non-Monetary Digital Token Swap Facilities.' *Annals of Emerging Technologies in Computing* 3 (1): 42–50. https://doi.org/10.2139/ssrn.3312624.

Moore, Tyler, and Nicolas Christin. 2013. 'Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk.' In *Financial Cryptography and Data Security*, edited by Ahmad-Reza Sadeghi, 25–33. Berlin, Heidelberg: Springer Berlin Heidelberg.

Nakamoto, Satoshi. 2008. 'Bitcoin: A peer-to-peer electronic cash system.' http://www.bitcoin.org/bitcoin.pdf.

Oved, Michael, and Don Mosites. 2017. 'Swap: A Peer-to-Peer Protocol for Trading Ethereum Tokens.' AirSwap. https://swap.tech/whitepaper/.

Schwartz, Robert A., and Lin Peng. 2013. 'Market Makers.' In *Encyclopedia of Finance*, edited by Cheng-Few Lee and Alice C. Lee, 487–89. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4614-5360-4_38.

Sexer, Nathan. 2018. 'State of Decentralized Exchanges, 2018.' January 2018. https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79.

Victor, Friedhelm, and Bianca Katharina Lüders. 2019. 'Measuring Ethereum-Based ERC20 Token Networks.' In *Financial Cryptography and Data Security*, edited by Ian Goldberg and Tyler Moore, 113–29. Cham: Springer International Publishing.

Vogelsteller, Fabian, and Vitalik Buterin. 2015. ‘ERC-20 Token Standard.’ EIP 20. https://eips.ethereum.org/EIPS/eip-20.

Warren, Will, and Amir Bandeali. 2017. ‘0x: An open protocol for decentralized exchange on the Ethereum blockchain.’ 0x. https://github.com/0xProject/whitepaper/blob/master/0x_white_paper.pdf.

Wilmoth, Josiah. 2018. ‘Decentralized[?] Ethereum Exchange IDEX Waves Goodbye to New York Traders.’ October 2018. https://www.ccn.com/decentralized-ethereum-exchange-idex-waves-goodbye-to-new-york-traders/.

Zamyatin, Alexei, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William J. Knottenbelt. 2018. ‘XCLAIM: Trustless, Interoperable Cryptocurrency-Backed Assets.’ Cryptology ePrint Archive, Report 2018/643. https://eprint.iacr.org/2018/643.

Zie, Jean-Yves, Jean-Christophe Deneuville, Jérémy Briffaut, and Benjamin Nguyen. 2019. ‘Extending Atomic Cross-Chain Swaps.’ In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, edited by Cristina Pérez-Solà, Guillermo Navarro-Arribas, Alex Biryukov, and Joaquin Garcia-Alfaro, 219–29. Cham: Springer International Publishing.*ional Convention on Information and Communication Technology, Electronics and Microelectronics (Mipro)*, 1545–50. https://doi.org/10.23919/MIPRO.2018.8400278.