UNIVERSAL DIGITAL COIN

New Payment System for the Digital Era

(A brief outline of UDC's platform and vision)

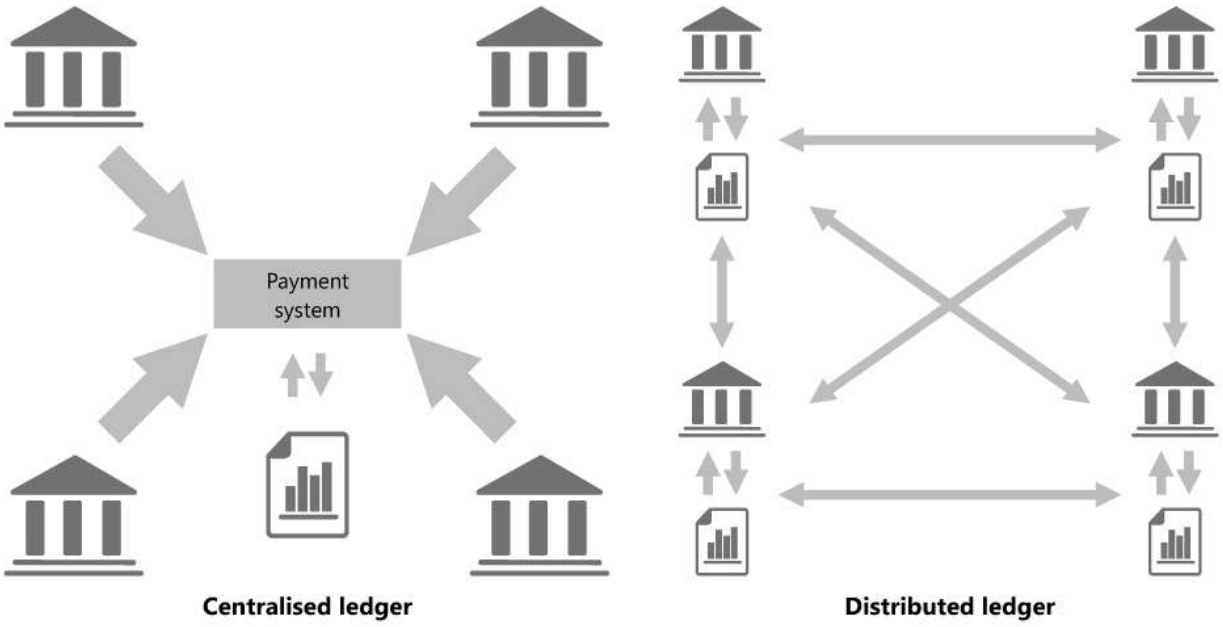
S.no	Content	Page
1	Abstract	4
1.1 1.2	About Universal Digital Coin? Global Network	4 5
2	FEATURES	6
3	Test Schedule	7
3.1 3.2	Equipment utilised Methodology	7 7
4	Mission	9
5	Proof-of-Work	11
6	Simplified Payment Verification	12

7	Decentralized Banking	13
8	Payment Service	15
9	The Peer-to-peer client	16
10	Market size and growth of Economy	17
11	Current Progress and Development	20
11.1 11.2	Development Acknowledgements	20 20
12	Summary	21
13	Conclusion	23
14	Reference	25

1. Abstract:

1.1. About Universal Digital Coin?

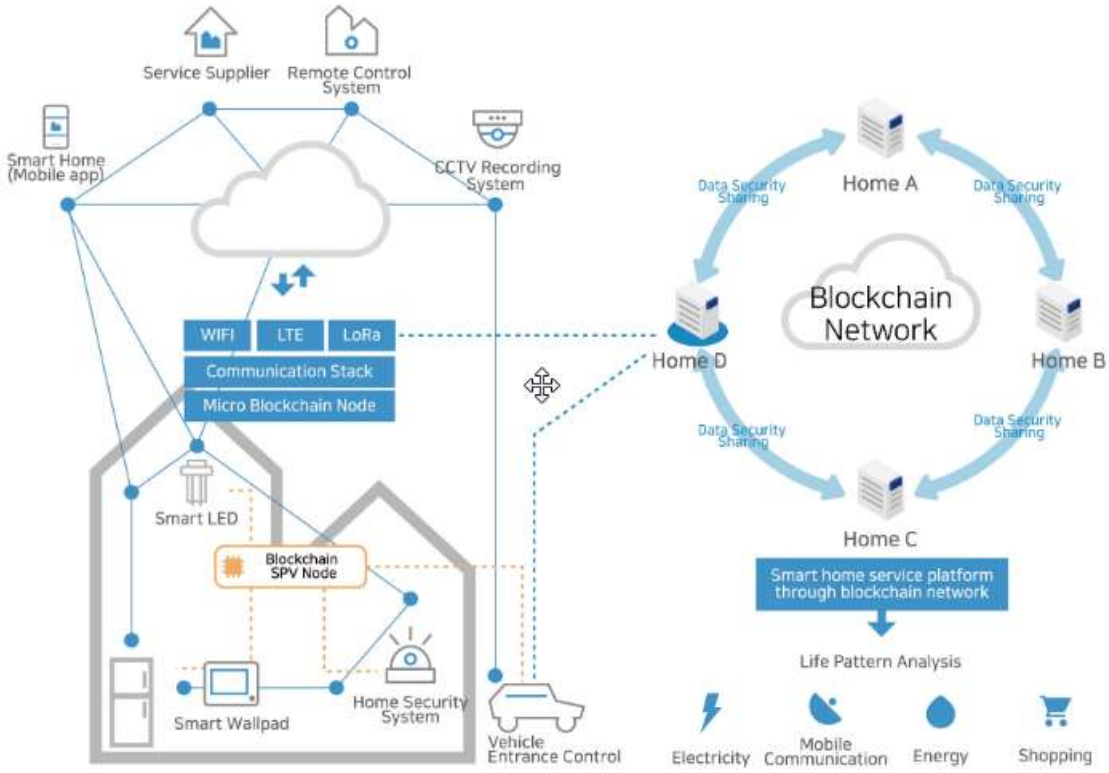
- UNIVERSAL DIGITAL COIN IS A PEER-TO-PEER INTERNET CURRENCY THAT ENABLES INSTANT, NEAR-ZERO COST PAYMENTS TO ANYONE IN THE WORLD. UNIVERSAL DIGITAL COIN IS AN OPEN SOURCE, GLOBAL PAYMENT NETWORK THAT IS FULLY DECENTRALIZED WITHOUT ANY CENTRAL AUTHORITIES. MATHEMATICS SECURES THE NETWORK AND EMPOWERS INDIVIDUALS TO CONTROL THEIR OWN FINANCES. UNIVERSAL DIGITAL COIN FEATURES FASTER TRANSACTION CONFIRMATION TIMES AND IMPROVED STORAGE EFFICIENCY THAN THE LEADING MATH-BASED CURRENCY. WITH SUBSTANTIAL INDUSTRY SUPPORT, TRADE VOLUME AND LIQUIDITY. UNIVERSAL DIGITAL COIN IS DEVELOPED USING SCRYPT ALGORITHM BY WHICH A CRYPTO CURRENCY BLOCK CHAIN NETWORK AIMS TO ACHIEVE DISTRIBUTED CONSENSUS.



- UNIVERSAL DIGITAL COIN IS A FREE OPEN SOURCE PROJECT, WITH THE GOAL OF PROVIDING A LONG-TERM ENERGY-EFFICIENT SCRYPT-BASED CRYPTO-CURRENCY. ANYONE CAN SEND OR RECEIVE ANY AMOUNT OF MONEY WITH ANYONE ELSE, ANYWHERE ON THE PLANET, CONVENIENTLY AND WITHOUT RESTRICTION

1.2. Global Network:

- UNIVERSAL DIGITAL COIN IS DIGITAL CURRENCY FOR A CONNECTED WORLD. WITH UNIVERSAL DIGITAL COIN, YOU ARE YOUR OWN BANK. UNIVERSAL DIGITAL COIN IS A PLATFORM THAT CONNECTS BANKS, PAYMENTS SYSTEMS, AND PEOPLE. INTEGRATE TO MOVE MONEY QUICKLY, RELIABLY, AND AT ALMOST NO COST.



2. FEATURES:

Ultra-Fast Transactions-

- Transaction speeds are ultra-fast compared to other coins. Simple Payment Verification (SPV) technology allows average transaction confirmation times to drop to ~10 seconds.

Decentralized-

- UNIVERSAL DIGITAL COIN IS A DECENTRALIZED CURRENCY BASED ON AN OPEN-SOURCE PLATFORM. THERE IS NO CENTRAL CONTROL OVER THE COIN.

Safe-

- Universal Digital Coin uses multiple anonymity-centric networks such as Tor and I2P. The IP addresses of the users are obfuscated and the transactions are completely untraceable.

Secure & Simple-

- World's most robust block chain technology. Real-time traceability of funds. Easy to use, no hassles. Transact in seconds. Get confirmed in minutes. To ensure that no third-party can execute a fraudulent trade between users, the trade method of the exchange smart contract will only accept orders signed by a private key held by the matching engine.

3. Test Schedule:

- For validation of the testing there is a record below of the equipment utilised along with the operating system and the scenario it relates to. The methodology covers the approach to setting up the artefacts in preparation for the forensic tool. The actions taken will assist drawing conclusions from the test results through verification of artefacts and related timestamps.

3.1. Equipment utilised-

- The following equipment that was used for the analysis is as follows: Scenario 1 - Clean Windows 8 SP1 Professional 64 bit laptop Scenario 2 - Used Windows 7 SP1 Professional 64 bit laptop – running Universal Digital Coin but not mining Scenario 3 - Used Windows 7 SP1 Professional 32 bit laptop – having already purchased Universal Digital Coin through P2P site https://universaldigitalcoin.com/

3.2. Methodology -

- The methodology was to act as a normal user would do so that artefacts would be created to test the forensic tool. It is difficult to define a normal user as everyone is different. However, by using the three scenarios one would be able to obtain slightly different results.

- Scenario 1 – The methodology was to test what results Tor would hide in terms of forensic analysis of a user's behaviour. The user would simply download and install the Tor browser. They would then activate the program and browse for virtual currency websites. Originally it was planned to use the Silk Road website but the site was subsequently taken down by law enforcement.

Given the nature of Tor and the obvious interest of law enforcement in its use testing was limited to ensure just basic searches were performed.

- Scenario 2 – The original methodology was to have a user who mined virtual currency. However, this was more involved and required greater processing power so the methodology was changed to a user who is partaking in the peer-to-peer network of a virtual currency.

- Scenario 3 – Our final user is our most active. One wanted to create the majority of "noise" in terms of forensic artefacts. To do this, real transactions were carried out on genuine sites on the internet. Physical currency was changed into virtual currency. The methodology being that the transactions would be identifiable forensically and allow a forensic investigator to trace transactions made.

4. Mission:

- Our Mission is to provide this world a better decentralised system eliminating the current issues of transparency, corruption and economy unevenness.

- Being pioneer for Blockchain solutions we continuously aim for providing best-of-breed business solutions leveraging the Blockchain technology. As an innovation oriented company made with striving excellence in relationship with our partners, clients and employees we are targeting to emerge as a global leader in bridging the gap between business difficulties and Blockchain's ability to solve these issues.

- UDC aims to solve some of the biggest problems in the world of crypto currencies – including price volatility, fixed coin supply, and lack of real world uses for digital currencies.

- We intend to grow UDC Platform as a unified market, without boundaries and restrictions. We believe that UDC Platform has the potential to become a true legacy system - the fundamental pillar of a new economic and financial era.

Figure 4.2, what is block chain

- Our ultimate goal is to inspire hundreds of millions of users to join us, and build a self-supportive, decentralized ecosystem, which supports a better world. We stand for the fair distribution of goods and money, and our plan is simple - to improve the ways businesses and individuals connect, by leveraging Smartphone technology to create an unparalleled, self-supporting global system.

5. Proof-of-Work:

- To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hash cash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

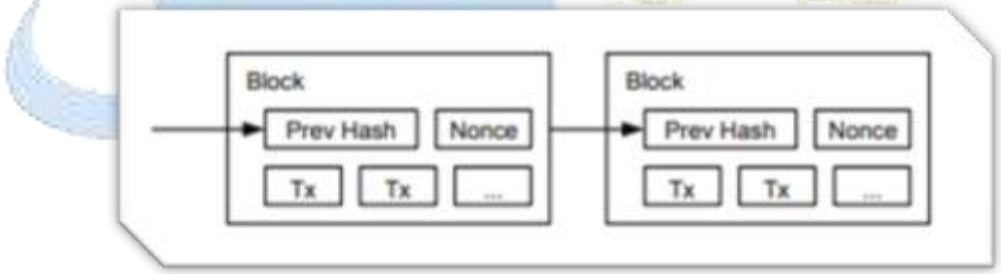


Figure 5.1, Explains Proof-of-work

- The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote.

6. Simplified Payment Verification (SPV):

- It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's time stamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

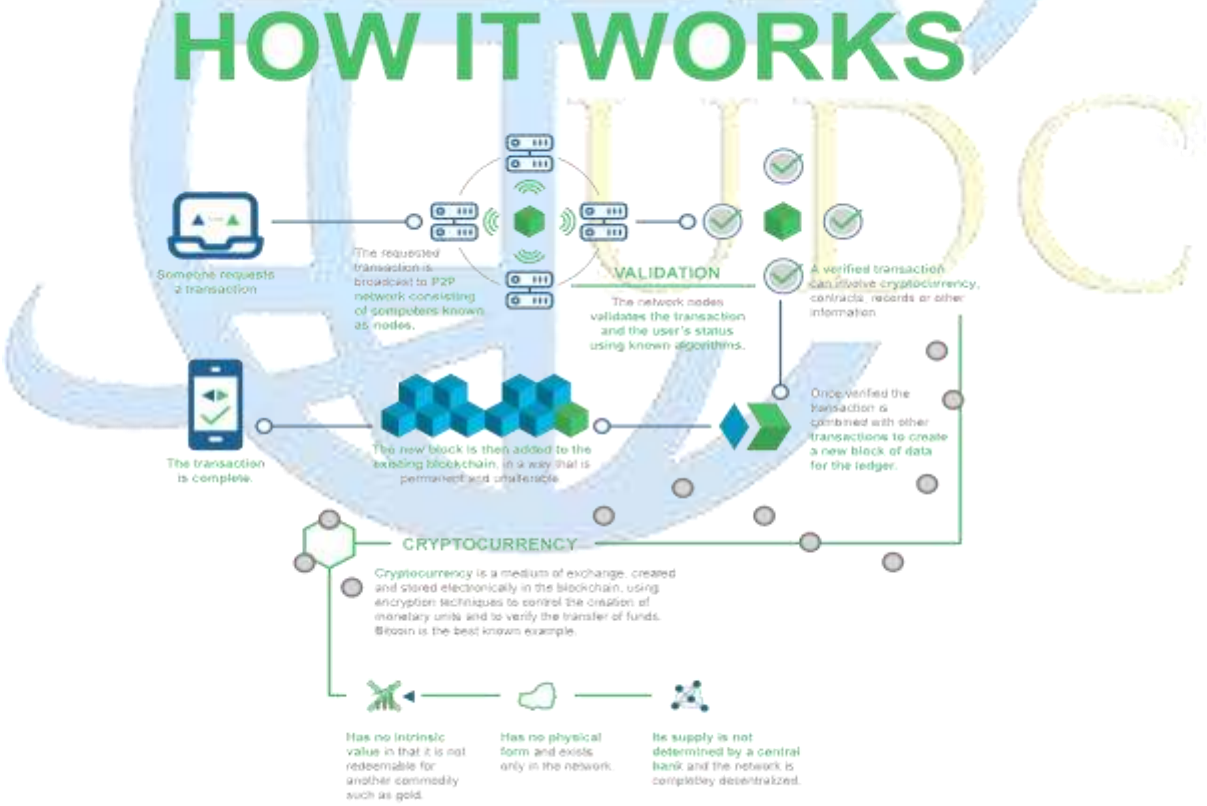


Figure.6.1, Explains how transaction worked

7. Decentralized Banking:

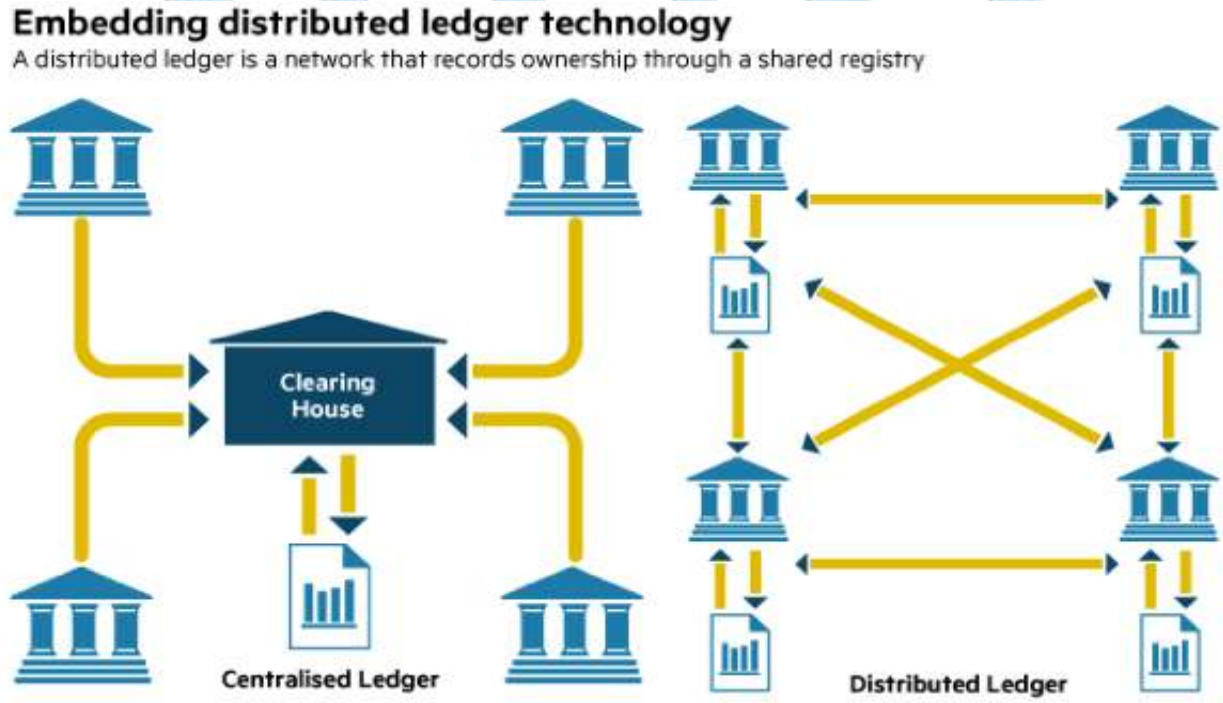
- Beyond enabling decentralized exchange, UDC offers a long term vision of decentralized banking: a smart contract based funds management service for assets on the block chain. As with traditional banking, this management service would be designed to provide both fund security and investment opportunities. For example, this funds management smart contract can provide advanced security features through a dual key system consisting of frequent use key and large funds key. A user moving funds in UDC with the frequent key would be limited to a daily amount, and to trade above this threshold would need to provide their large funds key.

Comparison	The Centralized Bank	The Decentralized Bank
Definition	Power and authority for planning and decisions rest with top management organized around a hierarchical structure.	Power and authority (with accountability) should be close to the employee and customer.
Decision Making	Rests with senior management	Rests with local markets
Largest Risks	Inflexibility	Inconsistency
Biggest Advantage	Control	Resiliance
Other Advantages	Consistent Customer Experience	Market specific pricing, marketing and product design

- If a frequent use key is compromised the user can lock their account using both keys and transfer the funds to a new account. Following the success of core exchange features, we envision this smart contract will integrate with and manage other UDC services, such as peer-to-peer lending or indexed investment accounts.

8. Payment Service:

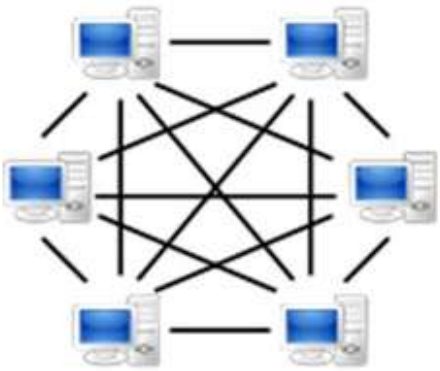
- The UDC payment service allows UDC smart contracts to interact with assets that live outside of the UDC virtual machine. For example, a user might use the payment service to make transactions across chains, sending ETH to a UDC smart contract that then distributes it among their friends' UDC addresses. In the future, the payment service will support assets on other block chains or non-digital assets such as USD, serving as a gateway for the trade of off-chain assets on UDC.



- In the near term, however, the payment service is designed to provide a similar function for global assets on the UDC block chain. More broadly, the payment service provides a starting point for reasoning about how a decentralized exchange can interact with assets on other chains.

9. The Peer-to-peer client:

- The UDC's peer-to-peer client (P2P) is the software which connects the user to the network to facilitate a transaction between two individuals without an exchange. All transactions are processed by each client. When you open your P2P program it updates itself from the network with all the transactions that make up the currency ledger. The client is also used to send and receive payments. Haid discusses the use of Tor and virtual private networks for anonymity by those seeking to hide their identity. Virtual currencies have publicly available ledgers known to all the peer-to-peer participants. Therefore an audit trail of transactions should be possible to retrieve forensically from various sources. Anonymity will continue to be an issue until such time that physical identity can be tied to transactions.

A **server** based network	A **peer-to-peer** based network.
	

10. Market size and growth of Economy:

- Since the 21st century, Economy all over the world keeps growing at a rate of 5.6% on annual average. Among them, output value of the American Economy tops the list. In some developing countries such as India, China and Brazil, etc., Economy is making progress strongly and annual average increases in these countries all exceed 10%. The reason why the Economy can leap forward at full speed today is that a complete set of comprehensive recreation system cantering around life style, gambling and game playing has been established for it as its foundation. The above aspects have been always the “cash cow” of the Economy and their integration with network releases the giant potential of entertainment to a greater extent.

- At present, the annual scale of global Economy market has reached thousands of billions. Internet Revolution makes it possible for entertainment experience to be globalized for the first time so as to generate numbers of Economy giants at a level of trillions on the world

- With the renovation and development of global internet technology and the awakening of consumers’ self-awareness, industries falling into the category of life style are rising quickly. The 2016 Global Social Media Study Summary indicates that among nearly 7.4 billion of the global population, the number of active users of social media has reached 2.307 billion; overlord status f traditional social applications such as Facebook, etc. has been shaken to a certain degree; and, young users tend to have more diversified application selections .

- Throughout the world, values for applications of life style, including Tinder and Instagram, etc., have been estimated to break through ten billions of dollars and are forging recreational life of human beings in an unprecedented manner.

- In this process, broad business development opportunities are raised. Match Group, the largest online dating group of American, went public on November 19, 2015. On that day, it raised $ 0.536 billion and its aggregate market value exceeded $ 3.4 billion. Moreover, multiple well-known social apps are owned by it, such as Tinder and OkCupid, etc.

- Likewise, the Asia-Pacific market is booming and the development of life style apps is especially spectacular in the Asian region, particularly China. Currently, utilization frequencies of social networking software such as WeChat and QQ, etc. have ranked Top among social software on the world. Emerging diversified social apps spring up one after another in a rising tendency.

- Taking social broadcaster software industry in China for example, Momo as a benchmarking listed company in Chinese broadcasting industry has been established for five years and its market value has arrived at $ 8 billion. Up to now, the average rate of increase in each quarter remains at 50% and above . Other companies closely following it are YY (market value: $ 4 billion) and Inke (market value: 7 billion RMB), etc. successively. All of them are growing rapidly. In China, it can be said that “A Battle among Thousands of Broadcasting Companies” has been put on the stage, which attracts ten billions of venture capital funds.

- Clearly, not only are lifestyle apps becoming an indispensable part of users’ life around the world, but considerable gains can be generated commercially as they are featured with high gross margins, large flow and impressive interactions and penetration

11. Current Progress and Development:

Here we describe the current state of development on UDC.

11.1 Development-

- We have completed and deployed smart contract prototypes for trading and withdrawal features on the exchange. Development of the matching engine has begun and a full prototype will be available in early 2018. We have also released an alpha version of the UDC web extension, which will connect with the exchange for asset conversion, and begun work on the trading user interface. We have created and shared template code with our banking partners that will allow them to interface with the UDC extension to buy crypto currencies and send them to a user's account.

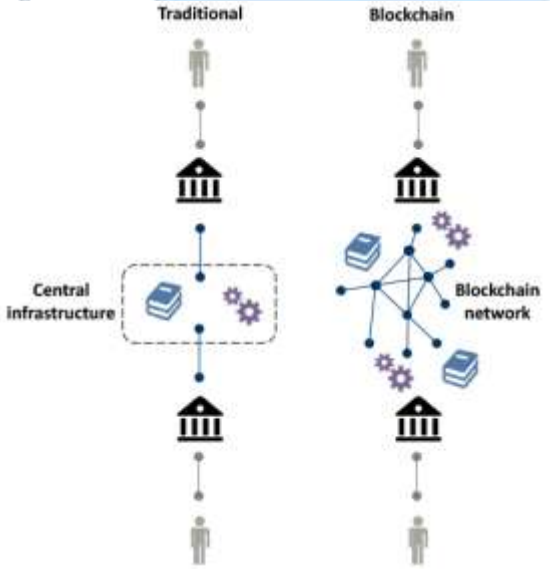
11.2 Acknowledgements-

- UDC Labs would like to acknowledge all of the people involved in the development of the UDC Protocol consensus algorithm. Specifically, UDC is a crypto currency platform with ambitious goals - to promote the widespread use, availability, and accessibility of crypto currency, in order to promote a more stable and connected global economy. We hope you'll stay tuned for the big changes ahead - and support us as we strive for greatness.

12. Summary:

- Our results confirm that the use of Tor can present problems for forensic artifacts to be found in terms of activity. This was demonstrated in our first scenario on Windows 8. From a forensic perspective live memory analysis would be a next interesting area to investigate Tor. Our results can prove forensically that someone used a web browser to search for Tor and download the Tor browser bundle.

- A user then used Tor on the machine. Once the user was running the Tor browser the tool was unable to identify what actions were taken and proved in our search (event 21). Virtual currency artifacts from the peer-to-peer UDC install demonstrated the download of UDC onto a machine and presence of crypto currency artifacts. However, other than that, to explore this further the key files of interest to a forensic investigator would be the wallet.dat and peers.dat. Peers.dat contains connection information.



	Purpose	In Traditional networks	In Blockchain networks
Front-end	Interaction with end-user (untouched by blockchain technology)	Not affected: remains the same	
Messaging	Technical connectivity with the network	Through central infrastructure	Peer-to-peer
Processing	Execution of transactions	• Centrally • Batch or per trx	• Decentral • In 'blocks'
Ledger	Keeps track of participants' balances	• Central • Closed (one trusted party)	• Decentral • Public

- This may assist in an investigation in terms of network connections to and from a machine participating on a peer-to-peer currency network. The third test where four transactions, (two processed, two cancelled) have created a host of artifacts shows that cloud forensics is just as important to corroborate the tools findings. UDC and the open nature of transactions have allowed us to draw together transaction data from the forensic tool. This matches the actions taken. The key artifacts for an investigator would appear to be login web page URLs which contain user IDs in relation to the website UniversalDigitalCoin.com. They merely demonstrate a possible intent to buy and need verifying with other artifacts.

13. Conclusion:

- We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination.

- They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

- In conclusion, an investigator would be interested in the artefacts, the online exchange website, the user's transactions through the online exchange and their UDC balance if one exists. Wallet.dat in this case was not used or taken off line, for example on removable media, encrypted. Interestingly if the user removes the UDC application wallet.dat and peers.dat remain on the machine. Technology offers the use of crypto currencies in a variety of ways in terms of purchasing and selling. The tools that exist would allow a user to do the following.

A user who wishes to remain anonymous could take the following actions:

Download Tor onto a USB device.

Connect the USB device to a workstation of choice anywhere.

3. Browse to a crypto currency exchange and agree to meet in person and purchase for cash.

4. Connect the USB device to a different workstation of choice anywhere.

5. Browse to the crypto currency exchange and download currency to wallet.dat on the USB device.

6. Print the details of the private key of the wallet.

7. Lock the USB away or distribute the USB to others.

8. Repeat step 1 with a new USB device.

14. References:

[1] Coinmarketcap.com. http://coinmarketcap.com, 2017.

[2] Etherdelta. https://etherdelta.com/, Accessed 2017.

[3] EtherOpt. https://github.com/etheropt, Accessed 2017.

[4] Maker Market. https://oasisdex.com, Accessed 2017.

[5] NEO White Paper: Superconducting Exchange. https://github.com/neo-project/ docs/blob/e01d268426a8b5f9b3676cfd03d0b8b83d7711a1/en-us/white-paper. md#highly-scalable-architecture-design, Accessed 2017.

[6] Raiden Network. https://raiden.network, Accessed 2017.

[7] Why we are building Cardano. https://whycardano.com, Accessed 2017.

[8] Bitcoin Developer Guide: Proof of Work. https://bitcoin.com/en/developer-guide# proof-of-work, Accessed 2017, Archived at https://www.webcitation.com/ 6v7DUj9JJ on November 20th, 2017.

[9] Bitcoin Developer Guide: Simplified Payment Verification. https://bitcoin.com/en/ developer-guide#simplified-payment-verification-spv, Accessed 2017, Archived at https://www.webcitation.com/6v7DUj9JJ on November 20th, 2017.

[10] Bitcoin Developer Guide: UTXO. https://bitcoin.com/en/developer-guide# term-utxo, Accessed 2017, Archived at https://www.webcitation.com/6v7DUj9JJ on November 20th, 2017.

[11] The Cost of Decentralization in 0x and EtherDelta. http://hackingdistributed.com/ 2017/08/13/cost-of-decent/, Accessed 2017, Archived at http://www.webcitation. org/6v7Ff8r7D on November 20th, 2017.

[12] Ethereum Wiki: Design Rationale. https://github.com/ethereum/wiki/wiki/ Design-Rationale#accounts-and-not-utxos, Accessed 2017, Archived at http://www. webcitation.com/6v7FswqI2 on November 20th, 2017.

[13] NEO NEP-5: Token Standard. https://github.com/neo-project/proposals/blob/ master/nep-5.mediawiki, Accessed 2017, Archived at http://www.webcitation.com/ 6v7FuuPv2 on November 20th, 2017.

[14]Open SSL. http://www.openssl.com/source/

[15]Miniupn. http://miniupnp.tuxfamily.com/files/

[16] Ethereum Wiki: Proof of Stake. https://github.com/ethereum/wiki/wiki/ Proof-of-Stake-FAQ, Accessed 2017, Archived at http://www.webcitation.com/ 6v7G0YAQH on November 20th, 2017. 10

[17] Oracle. Inc. http://www.oracle.com/technology/

[18]Boost.com. http://www.boost.com/users/download/

[19] Reconstructing Smart Contracts, Part II: Scalability. https://themerkle.com/reconstructingsmart-contracts-part-ii-parallel-universes-and-unlimited-scalability/, Accessed 2017, Archived at http://www.webcitation.com/6v7FxFbHA on November 20th, 2017.