EOT - "The Encryption of Things"

4 July 2017

Introduction to Blockchain:

What is a blockchain? - From Wikipedia

A blockchain[1][2][3] – originally block chain[4][5] – is a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block.[6] A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. Functionally, a blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically."[7]

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.[8] This makes blockchains potentially suitable for the recording of events, medical records,[9][10] and other records managementactivities, identity management,[11][12][13] transaction processing, and documenting provenance.

The first blockchain was conceptualised by Satoshi Nakamoto in 2008 and implemented the following year as a core component of the digital currency bitcoin, where it serves as the public ledger for all transactions.[1] The invention of the blockchain for bitcoin made it the first digital currency to solve the double spending problem, without the use of a trusted authority or central server. The bitcoin design has been the inspiration for other applications.[1][3]

What is Bitcoin? - From Wikipedia

Bitcoin is a cryptocurrency and a digital payment system[13]:3 invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto.[14] It was released as open-source software in 2009.[15]

The system is peer-to-peer, and transactions take place between users directly, without an intermediary.[13]:4 These transactions are verified by network nodes and recorded in a public distributed ledger called a *blockchain*. Since the system works without a central repository or single administrator, bitcoin is called the first decentralized digital currency.[13]:1[16]

Besides being created as a reward for mining, bitcoin can be exchanged for other currencies,[17] products, and services in legal or black markets.[18][19]

As of February 2015, over 100,000 merchants and vendors accepted bitcoin as payment.[20] According to research produced by Cambridge University in 2017, there are 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin.[21]

The underlying principles of Bitcoin and the Blockchain

Anonymity – all Bitcoin transactions are only between cryptographical pseudonyms without the need to have their true identity of the transacting parties revealed.

Security – all confirmed Bitcoin transactions are with mathematical certainty irreversible, all bitcoins are with mathematical certainty non-counterfeitable

Decentralization – Bitcoin has no central authority and is voluntarily run by consenting autonomous peers in a peer to peer network

Finiteness – unlike the infinite supply of fiat currencies the total supply of bitcoins to ever exist is forever arbitrarily limited and fixed

Tangibility – issuing new Bitcoins requires labor in the form of finding a specific number by solving a cryptographic math problem

Transparency – all Bitcoin transactions are public and forever stored in the blockchain for anyone to see

Integrity – all bitcoins are counted equally(are fungible), virtually can't be frozen or blocked from being spent

Practicality – Bitcoin works anywhere, for anyone, non-stop, and the protocol allows for many practical layers on top, just like email
Rationalism – the Bitcoin software is written under the MIT open source license and is not a logically inconsistent intellectual property of anyone but merely organized information everyone can use as they wish

For furthere reference the full Satoshi Whitepaper is here: - https://bit-media.org/wp-content/uploads/2017/06/bitcoin-paper.pdf

Encryption - from Wikipedia

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended

information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

In our modern world encryption has become a powerful to ensure privacy and security of communication. Cryptography linked to blockchain technology is one of the most exciting developments of modern times.

The Internet of things

The **Internet of things** (**IoT**) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.[1][2][3] In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[3] and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks".[4] The IoT allows objects to be sensed or controlled remotely across existing network infrastructure,[5] creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.[6][7][8][9][10][11] When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020.[12]

In recent times more and more of these devices have become prone to hacking and in need of security solutions thus the need for encryption.

Introducing the “Encryption of Things” [EOT]

The huge surge in devices attached to the internet [see estimate above of 30 billions objects attached to the internet by 2020] constant hacking and cyber attacks have increased not only the demand but the necessity of secure solutions.

Applications of EOT can be explained by a few examples.

Secure messaging

To make messages truly secure we need a process whereby a cryptography can be applied to encrypt transaction. An example would be where a cryptocurrency transaction is used to create public and private encryption keys for such a message, The message will then be transmitted via a blockchain from the sender to the receiver. The messages could be in the form of chat messages, emails and would be able to handle attachments. Confirmation by the nodes on the blockchain will confirm the validity of the sender and receiver and the encryption will ensure privacy of the message.

Secure calling

Secure calling is a process whereby the caller and the recipient of the call are identified and linked via a blockchain enabled cryptocurrency transfer, again creating public and private encryption keys making the call truly private.

Secure media storage

To safely and securely store media a process is required where 1.) Access to the media is encrypted via public and private keys of the person wanting to store the media. 2.) The media itself needs to be encrypted with a set of encryption keys and 3.) Media storage costs need to be paid via cryptocurrency

Secure browsing

To browse the internet securely we need to create a process of verification whereby nodes on the blockchain can verify websites as “safe”. Furthermore the entire process needs to be encrypted as well.

Verification

This is one of the most important uses of a blockchain, we can verify websites as in the example above but also various other things such as identity [important in KYC and AML procedures] , title and ownership [such as land registries or stock ownership], date stamps [example would be in the case of intellectual property disputes] and source of products [as with the verification of source of agricultural or other products. These are just a few examples. All of this data needs to be encrypted as well.

“Smart home” security

What is a “smart home?”

Home automation or smart home[1] (also known as domotics[2]) is building automation for the home. It involves the control and automation of lighting, heating (such as smart thermostats), ventilation, air conditioning (HVAC), and security, as well as home appliances such as washer/dryers, ovens or refrigerators/freezers. Wi-Fi is often used for remote monitoring and control. Home devices, when remotely monitored and controlled via the Internet, are an important constituent of the Internet of Things. Modern systems generally consist of switches and sensors connected to a central hub sometimes called a "gateway" from which the system is controlled with a user interface that is interacted either with a wall-mounted terminal, mobile phone software, tablet computer or a web interface, often but not always via Internet cloud services. - source Wikipedia

As we can see all these devices are linked and controlled via the internet thus creating security issued. Blockchain technology and encryption can mitigate many of these risks.

Secure banking and Fintech

New financial technologies in the fields of banking, insurance, investments and other financial services applications are playing a major part in our lives. We use our smartphones to pay for goods and services, transfer money and to do online banking. The need for security in this field is imperative and a major role is to be played by blockchain technology and encryption.

EOT in the future

The examples we mentioned above are only “scratching the surface” of where these technologies are applicable and who knows what will be invented in future. Google, Apple and Uber are all testing cars that drive themselves. A major issue with this technology is again the security aspect and the need to protect against hacking and who want’s to get into a spaceship to Mars that might be hacked or hijacked by ransomware?

So the future for the “Encryption of Things” - EOT, looks very interesting indeed and the role of cryptocurrencies in this will be major.

EOT - Coins - A cryptocurrency for the Future

As clearly indicated above, cryptocurrencies will play a major role in the future of the encryption of things and there is a definite need for a cryptocurrency that can fill this gap, thus the introduction of the EOT - Coin.

As we know Bitcoin is the first cryptocurrency and has now been proven as a currency as well as for its security aspects. There are however a few issues with using Bitcoin “ as is” for the

encryption of things and EOT was thus designed with a few modifications to Bitcoin. EOT uses the Bitcoin source code but with a few modifications.

Technical Detail of EOT:

Name: - EOT COIN, Symbol EOT

Coin type: - Proof of Work

Time between blocks: - 90 seconds

Block Size: - 1 MB

Block Reward: - 100 coins

Reward Halving: - every 500,000 blocks

Total Coins 200,000,000

A total of 100,000,000 coins - 50% of the total will be pre-mined and the balance will be mined.

The advantages of EOT:

Fast Payments:

New blocks are mined every 90 seconds thus ensuring that transaction are fast and efficient

Peer-to-Peer:

Now you are not dependent on banks anymore who have the power to block your account, devalue, or even confiscate your money. With EOT all your funds are controlled by YOU and all money transfers are controlled and verified by a distributed network. The decentralized network of users worldwide gets rid of the need for intermediaries and their fees.

Security:

EOT is protected using advanced cryptography. Transactions are processed not by a bank, but by the distributed power of thousands of independent computers all over the world.

Global Payments:

You can transfer money anywhere, to anyone who has a EOT wallet. These transfers can't be blocked by third parties and can be transferred cross-border almost instantaneously.

New Opportunities:

EOT embraces the new world and creates opportunity for new business to be developed with the currency and the "encryption of things" and has tremendous potential for growth.

EOT Tokens

As we have seen above 100,000,000 of EOT Coins will be issued as pre-mined. The process of getting these coins distributed into the market is handled via an offering on the waves platform [wavesplatform.com/downloads.html].

100,000,000 Million EOT tokens are offered for purchase on the wave platform and will be transferable to EOT coins 90 days after issue when mining will commence.

For more details on EOT tokens: - http://eottoken.com