Beyond the bitcoin - Smart decentralised financial contracts of the future

Ethan Choi

Abstract

The invention of bitcoin in 2008 brought to existence a novel new form of currency unlike any other in mainstream circulation. Often coined as the first “decentralised digital crypto-currency”, it has gained footing as a tradable alternative currency. With major technology and financial institutions investing millions into bitcoin technology, its development is a large industry in its own right, and the combined value of exchanged bitcoins is in the billions.

While there is hesitation for the currency itself to become accepted globally, one consequence is becoming clear; the protocol behind the bitcoin may be a much bigger innovation than the currency itself. The elegant solution to exchanging money on a platform where nobody can be trusted, has led to the peer-to-peer public ledger known as the blockchain - giving rise to a powerful new way of transacting transparently, securely, and almost instantaneously, without the need to trust anybody. This is in contrast to traditional centralised methods, where transactions are enabled by a trusted intermediary such as a bank or insurer.

Currency may be just the first application for the blockchain. This concept can also in theory be used for much more complex financial transactions, giving rise to the idea of “smart contracts” that can execute themselves transparently and irrefutably given certain conditions are met - all without the need of a trusted third party arbitrator. Examples can include: transactions written to the public ledger instructed to only execute when a death is registered thus acting like a notary or life insurance contract; or insurance claims transacting automatically only if no other claim is made to the public ledger on the same asset, eliminating multi-claim insurance fraud completely.

This paper explores the basic concepts of the technical components required, existing execution of applications, and insurance applications.

Introduction

In 2008, during the turmoil of the GFC, a novel new form of currency was anonymously released. Under the pseudonym Satoshi Nakamoto, a paper was published outlining what would eventually become bitcoin - an open source “decentralised digital crypto-currency"; a type of peer to peer currency where financial transactions could be made all without a trustworthy intermediary such as a bank acting as a facilitator or even a central server. Despite the bitcoin having no linked value nor the backing of a central bank or government, the elegant and novel technological currency, gained traction. It was not long before interest in bitcoins extended beyond cryptographic interest groups to gain a footing as a real tradable alternative currency. These days the market capitalisation of bitcoins exceed $10 billion (USD) at current, albeit volatile, exchange rates (October 2016).

To the layman user, bitcoin seems very much like a normal currency, and knowledge of how it works is not necessary to use it. It can be transacted with in a similar fashion to online banking, there are market based exchange rates to other currencies, and you can even use it to pay for your pizza (in participating pizzerias only), while at the same time being extremely secure, anonymous, and unable to be manipulated internally by governments. As a currency however there have been hesitations (such as the Chinese government banning banking institutions from engaging in the bitcoin industry in 2013), and in the foreseeable future it seems bitcoins may remain limited to the fringes.

Despite what may become of the currency, what has become evident is that the technology behind the bitcoin may have far greater implications. Developed on the basis of a "public ledger" known as the blockchain, the bitcoin protocol has attracted great interest and investment in solving problems that seem worlds apart from the initial idea of a cryptocurrency. The technology could potentially be used for much more complex financial transactions, giving rise to the idea of “smart contracts” that can execute themselves transparently and irrefutably given certain conditions are met - all without the need of a trusted third party arbitrator via a peer to peer network. Other applications include land registries without a centralised server, to immutable ledgers of assets such as cars or diamonds limiting fraud on such items, whether in trading or in insurance.

Interesting uses of blockchain technology beyond the bitcoin currency have let to millions invested in the "fintech" start-up sector with the expectation that the blockchain technology may have far more valuable implications than the bitcoin currency it started off as.

Before discussing the novel approaches to using the blockchain for non bitcoin purposes, a basic technical understanding of how the blockchain and bitcoin technology is designed is necessary.

Characteristics of bitcoin design

Peer-to-peer

Bitcoins can be digitally sent over the internet securely from one individual to another without the payment needing to go through a bank or clearing house. Therefore whether it is in day to day transactions, or overseas remittances, fees charged by financial institutions can potentially be bypassed. Also without a controlling intermediary, accounts cannot be frozen, and there are no arbitrary limits or bank pre-requisites. A transaction becomes similar to sending an email.

The public blockchain

A public ledger known as the blockchain records the bitcoin transactions, and replaces the need for a trusted central server. The blockchain is stored distributed over the network on the computers running bitcoin software with its own local copy of the blockchain, and constantly updated when a new transaction is made (approximately every 10 minutes). As the existence of bitcoins only resides on the blockchain itself, it is not possible to double spend it, or to falsely claim any bitcoins, as the owner of the bitcoin is specified publically.

Transparent and private

All transactions are recorded on the blockchain which is public, leading to a transparent ecosystem. While it is possible for anyone to see all transactions publically, funds are not tied up to real world entities such as personal information, and instead transactions are only linked to bitcoin "addresses". For improved privacy, transactions could be enacted over multiple new bitcoin addresses for transactions.

Ownership

Ownership of a bitcoin is required to be able spend a certain bitcoin on a specific address. Transactions (transfer of ownership) can only be enacted by digitally signing the transaction with a cryptographic "private key" of the owner which verifies against a "public key" on the blockchain. Due to the cryptographic nature of the signing process, private keys, and the design of the blockchain, hacking the blockchain and therefore stealing bitcoins is extremely difficult. It is however possible to hack computers storing the bitcoin wallets (private keys) itself or physically steal the hard drive in which the wallet is stored. If a bitcoin wallet is physically lost, then the bitcoins on the blockchain will remain forever unspendable as nobody will have the capability of digitally signing the transaction.

Bitcoin wallets / private keys

Unlike what the name implies, a bitcoin wallet does not "store" any bitcoins. Instead it holds the necessary digital keys to unlock the bitcoins currently embedded in the blockchain, and transact them. Therefore the digital wallets can be stored on a hard drive, externally on a USB drive or even printed on a piece of paper.

Miners

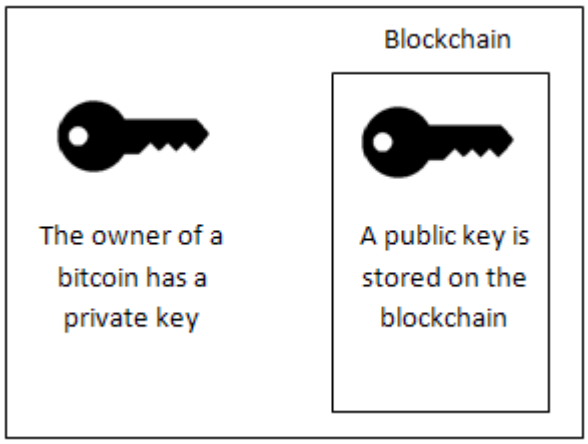
While an intermediary is not required to certify transactions, a "miner" is require as a record-keeping service to append transactions to the blockchain and also to "create" newly minted bitcoins.

Miners are simply computers which create new blocks of transactions to attach to the distributed ledger blockchain. In order for a block to be created and accepted by the rest of the network, proof of a specific problem must be provided, and this proof is computationally expensive. This must also be achieved before any other miner manages to create their own block first. To reward miners for their transactional services, new bitcoins are created and given to the miner when a new block is "mined".

Open source

As the original implementation was released in open source code, numerous developments have arisen from the original software, with a host of other crypto currencies separate to bitcoin now in existence. Of these, bitcoin has

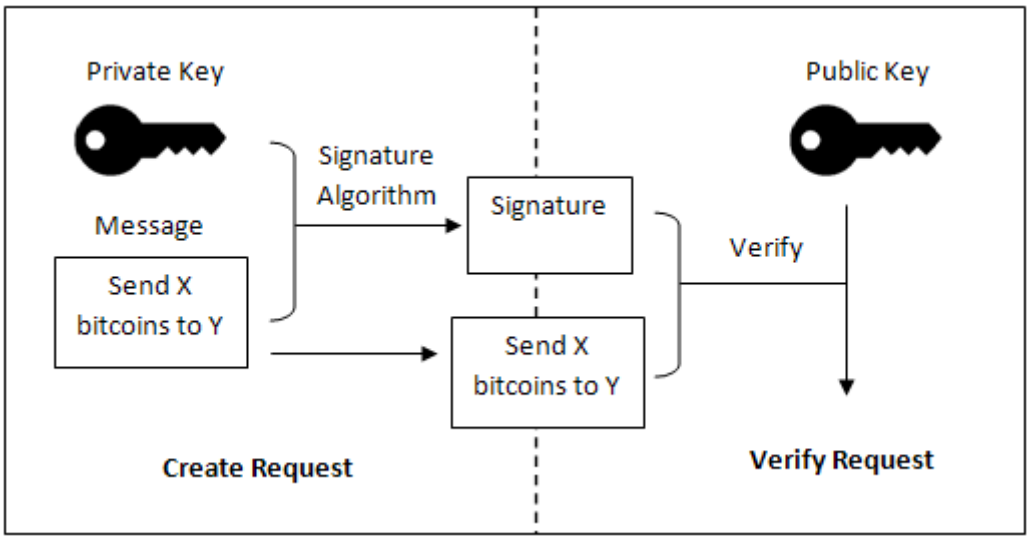
How does the blockchain work?



1. Cryptographic keys

Owning a bitcoin simply means that one has the "private key" of a bitcoin, a type of cryptographic password. Its corresponding "public key" is stored on the blockchain and only together the two keys can verify ownership.

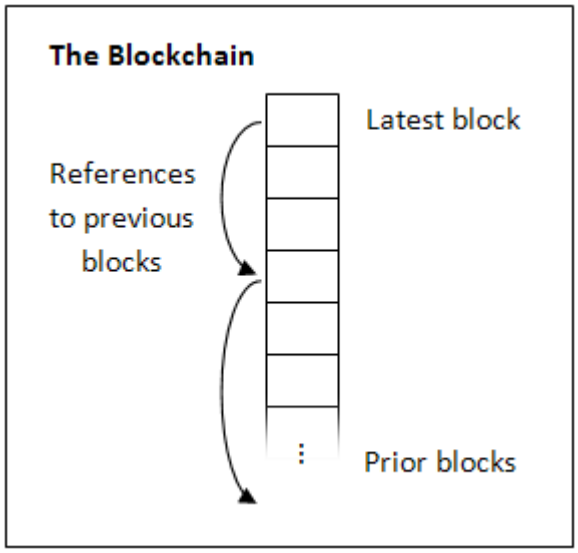
It is important to not give away the private key as this is equivalent to allowing anyone else to spend the money; however it is necessary to somehow show ownership of the private key to authorise a transaction. This is achieved with a special algorithm (Elliptic Curve Digital Signature Algorithm ECDSA for bitcoins) to create a "signature". It is not possible to derive the private key from the signature, but the public key can prove that a signature was created by the correct public key.



By pushing the private key plus a "message" through such an algorithm, a verifiable signature is created. Furthermore, due to the fact that the private key and the message were used as inputs to the signature creation, the message can no longer be changed, otherwise the signature will no longer be valid due to mismatching with the validation of the private key + message signature. Therefore all parties on the network can be satisfied that the bitcoin owner is verified, and the request message has not been tampered with, even though the request is clearly visible. A unique signature is required for every transaction.

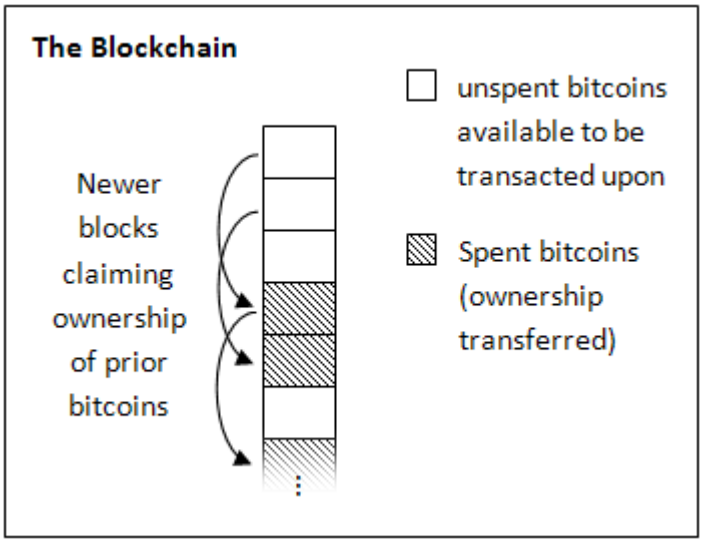
2. Blockchain

The blockchain is a public ledger, synchronised and stored by a vast number of computers (miners) over the bitcoin network. It consists of a series of "blocks" which are sequentially appended to the latest block on the chain. Each block contains the transactional information.



Individuals do not have a "balance of funds" in the traditional sense, instead each transaction refers to an earlier block in the blockchain where ownership was transferred. That block would then in turn refer to the previous block in which they were transferred and so on, until the very beginning of when the bitcoin was created.

This verifies that a bitcoin can only be spent once on a given transaction, since it is clearly visible publically if any new blocks have laid a valid claim to the block in question. An individual who attempts to use the same bitcoin to pay two parties simultaneously will be unable to create a valid block. If they were sent a request one after another, the second request would be invalid, and the recipient of the payment would be able to clearly see that the payment was invalid in the first place by having a look at the publically available blockchain and seeing that it had already been spent prior. An invalid block cannot be added to the blockchain in any case.



While checking every transaction to the beginning of blockchain inception seems time consuming, it can be made faster with an index of unspent transactions. The initial local copy of the block chain needs to be verified initially in a time consuming manner to prove that all blocks adhere to the referencing process, with no double spending but this can just be performed once initially. The bitcoin blockchain is currently approximately 90 GB (as at October 2016).

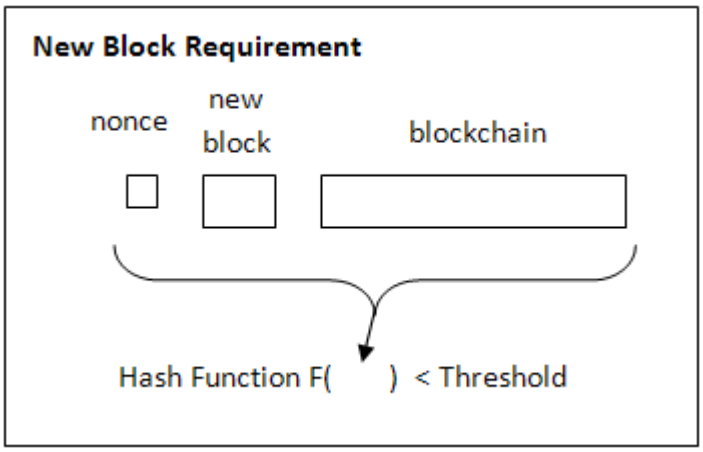
3. Sending a request

To spend a bitcoin, a request is sent on the bitcoin network with the correct signature and recipient address, which is then received by a vast network of computers, which are called "miners". Miners collect requests and create new blocks to be placed onto the blockchain.

4. Miners

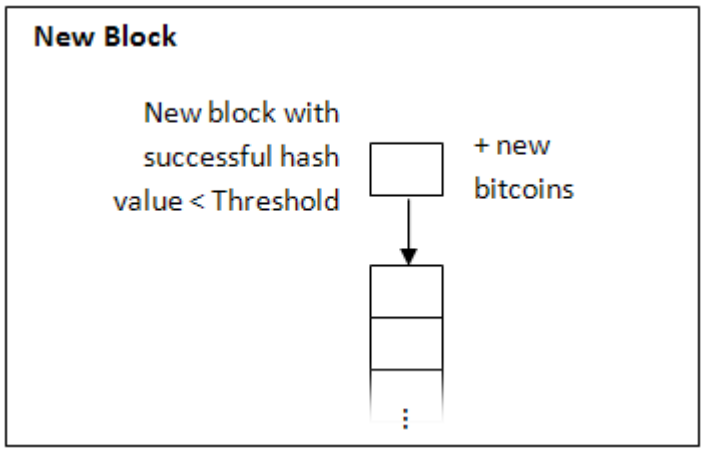
The miners collect request broadcasted from across the web and form new "blocks" to be appended to the blockchain. Miners do this because for every new block they append, brand new bitcoins are "mined" and come into existence and rewarded to the miner. All bitcoins in the blockchain will eventually link back to a bitcoin created in this form. Furthermore, requests may even come with self imposed transaction fee provisions, which miners may prioritise if they wish. For a block to be appended to the blockchain however requires solving an extremely difficult mathematical problem, one which no single computer or entity could calculate easily within a relatively short frame of time.

The calculation involves taking the requests to form a new block, along with previous blocks, and an arbitrary number (a 4 byte field called a nonce) and sending it through a "hash function" (SHA-256 in bitcoin) to obtain a hash value. The only way for a block to be accepted by the blockchain is if this hash value is below a threshold which is set to an adjusting difficulty level.



While calculating a hash value is relatively straight forward, calculating a hash value which is below a threshold is very difficult. It is virtually impossible to predict the output of a hash function such as SHA-256, therefore the only way to attempt to create a hash value below the threshold is to brute force attempt multiple combinations by iterating through the nonce until by chance the result is under the threshold. Possessing greater computing power therefore will increase success, at the cost of higher electricity costs.

Furthermore to ensure that the calculation will continue to be difficult into the future, the threshold dynamically changes over time based on a target of 1 new block every 10 minutes. The number of new bitcoins rewarded is also halved every 210,000 blocks produced. This means that there will only be a finite number of bitcoins in total circulation ever, at 21 million expected to be reached in 2140. After this point in time, miners will have to



rely on transaction fees set by the requestors. While paying a transaction fee is optional, miners may choose to prioritize requests with higher fees. Despite the eventual finite number of bitcoins, coins can be divided to fractions, with units such as 0.00000001 bitcoin colloquially referred to as 1 Satoshi.

5. Longest chain wins

Since creating a valid new block for the blockchain is extremely difficult, this turns adding a block to the blockchain into a competition with the vast number of bitcoin miners all independently attempting to create or "mine" new blocks to be added to the blockchain before someone else does.

Once a new block is formed, it is broadcast to other miners within the network. The other miners receiving the new blockchain will check the validity of the new block, then start using this new, longer blockchain and carry on from there. If there are multiple versions of the blockchain in circulation, only the longest chain will be trusted and propagated and added upon by the network.

This ensures that even with propagation delays, and potentially multiple different length blockchains, the longer chains are more likely to become longer leading to more confidence in blocks the longer it has been on the blockchain. There will be no incentive for miners to attempt to work on a shorter chain as this chain would not be considered by other miners, and therefore any newly created bitcoins would be worthless on the shorter blockchain.

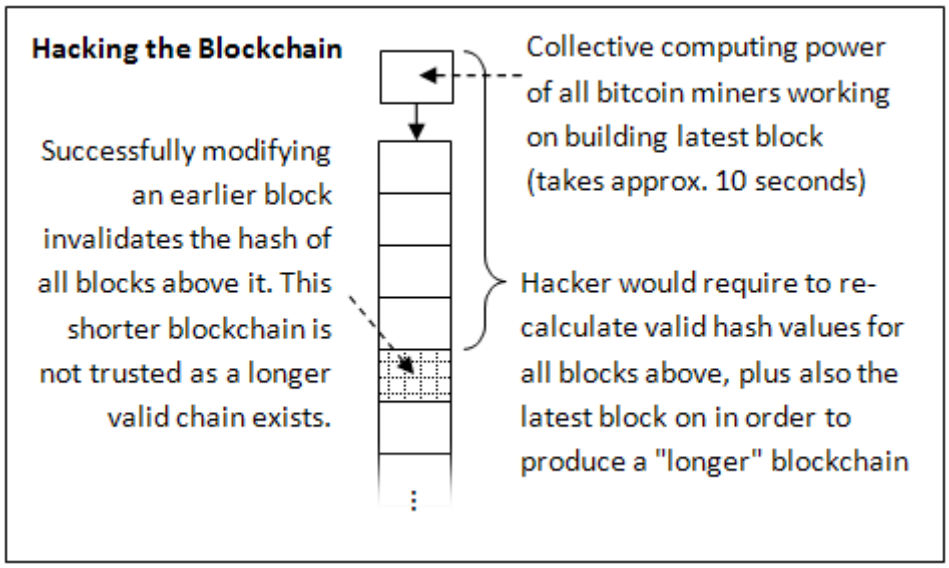
The reason for this design is the elegant solution to the problem of trusting the blockchain where everyone is anonymous and nobody can be trusted.

Difficulty in Hacking

With the whole system being a competition where miners collectively race to build the next block, hacking the blockchain would require an enormous amount of computing power, all to alter only one transaction. In order to alter information in the blockchain, the hacker would need to change the information in a prior block, solve the necessary cryptographic puzzle (hash function < threshold), and then solve the cryptographic puzzle for every single block attached after the hacked block, plus mine the latest block. This would also need to be done all before the blockchain is updated (every 10 seconds).

With the rest of the world mining away at the latest block, this would require the computational power of more than half the total of the world's bitcoin miners in order to successfully keep up with the latest block, let alone the historic blocks.

Changing an old block and pretending that the new blocks appended on afterwards are invalid would not work either, as all other miners would only trust the longest and therefore most secure blockchain, and ignore the shorter hacked blockchain.



Through mathematical confidence, the blockchain represents a completely publicly visible, secure and trust-less system where the whole system can be administered without a central authority, relying purely on the greed and self interest of complete strangers to secure it.

It is however possible for bitcoins to be stolen if say the hard drive containing the private keys to a bitcoin wallet were to be physically stolen, or a computer system where keys are stored is hacked to obtain the private keys. A number of high profile cases such as the Mt. Gox bitcoin exchange in Tokyo are such examples. These however are issues relating to keeping private keys secure, rather than directly impacting the blockchain.

Beyond the bitcoin: Smart contracts

While the blockchain was originally designed to store units of value (known as bitcoins), they can be adapted to store or represent other kinds of digital information. For the first time in March 2014 a new feature was added to the blockchain that allowed 40 bytes of metadata to attach to every transaction. This resulted in a host of non financial information to be creatively included into the blockchain from hello messages to excerpts from WikiLeaks, all permanently and publically imbedded into the immutable blockchain. In order to destroy these records, one would have to destroy all computers of the world on the blockchain network. Baring this, it would be almost impossible to change, censor, or to dispute the time of publication or author.

It was not long before people realised that this type of technology could be hugely beneficial in other applications, not only limited to currency. Simple applications may already be possible with the current blockchain architecture such as a basic secure storage systems or an anti censorship medium such as the example of embedding WikiLeaks whistle blowing documents. Other applications may require modifications to the blockchain by revising its open source code.

A possibility is to add other verifications at the block creation stage which the miner would be capable of validating. Currently only bitcoin ownership validation is checked for, however it would be relatively straight forward to also add other validation instructions such as “only transact if valid owner plus if the share price of XYZ drops below $10”. Other examples of conditions could be to transact when one's own name appears on an obituary, with all assets transacted to an heir. Numerous other potential proposals have also been envisioned.

These may all one day lead to the convention of self-executing, self-enforcing "smart contracts".

Share Trading

A company could buy a number of existing bitcoins and "colour" them with a label while specifying that these coloured bitcoins represent ordinary shares in the company. The company could then sell them and then from then on, share trading could ensue on the blockchain, without the need of an expensive share market listing on a separate exchange (such as the NZX), while still enjoying the liquidity and security of a highly efficient trading platform on the blockchain. Since only ownership of bitcoins are changed, reference to the "coloured" bitcoin and subsequent ownership would be publically visible. Here the underlying bitcoin may have its own currency value; however a “coloured” bitcoin would have the intrinsic premium value of owning the company which will be taken into account independently by anyone wishing to purchase them, and so the underlying bitcoin value will only be a nominal one used as a vehicle.

Dividends to shareholders could also be automatic, all without the need of a bank account, as payments can simply be directed to the blockchain addresses of those who currently hold coloured bitcoins.

Escrow service

Possible escrow services could exist by changing the validation requirement to require say 2 signatures instead of the 1 owner signature, or perhaps a majority such as 4 out of 7 specified signatures required before a transaction is approved and a new block is created to enact the

transaction. As soon as the necessary signatures were provided, the transaction would enact, appending to the blockchain and therefore would be binding and irreversible once transacted.

Asset Registries

Various assets are at risk of document tampering and fraud, especially in paper based, or even corrupt government based central repositories. By linking various assets either by serial numbers or other digital fingerprint to the blockchain, ownership can be represented by ownership of the specific blockchain address. In this way only one entity can lay claim to the asset, and once the asset is transferred, the ownership is transferred on the blockchain and cannot be tampered with. Such a registry function would have large benefits for insurance purposes also.

Blockchain based land registries are already being developed by a start-up Factom Inc. In other high risk items such as diamonds, a start-up Everledger is producing permanent blockchain legders for diamond certifications and related transactions histories. This would allow insurers, purchasers, and law enforcement to check transaction histories of stones, and to detect fraud.

Insurance Claims handling

Blockchain technology could allow customers and insurers to manage claims in a transparent manner. Often in a claims process, disputes can arise where claims are taken to disputes authorities, however on the blockchain, an unbiased network would validate claims, ensuring only valid claims are paid if certain conditions are met. The insurer would be unable to delay payments as well, as these smart contracts would enforce the payments instantly, triggered automatically when valid claims requirements are met. In simple cases, the entire policy itself could be a blockchain reference, with no paperwork or fine print required.

In this manner, claims could be paid before the customer has even called the insurance company without the need of sophisticated detection software from the insurance company. This may be more apparent in conjunction with the Internet of Things (IoT), where everyday objects become interconnected and capable of transmitting information. In this manner claims handling could become more efficient requiring less insurance processes if the digital policies themselves would execute automatically, and with improved customer experiences.

Insurance Fraud prevention

In the typical case of taking out multiple insurance policies on a single asset and claiming multiple policies, the blockchain could eliminate this type of fraud. While multiple policies held by different insurers may be difficult to share and detect currently, on the blockchain every asset is transparent and publically visible. Furthermore if the asset is registered to the blockchain, and subsequent insurance policies are also smart contracts linked to this asset address, a successful claim would automatically render any other policies invalid as they would no longer be able to claim the same bitcoin block transaction twice.

Another example may be in the case of valuable items such as diamonds in the previous example. If a listed asset such as a diamond were to be claimed fraudulently, after payment it would become impossible to officially transfer the registered asset (such as the allegedly stolen diamond) which is

already registered on the blockchain network. Any subsequent sale of the diamond would be easily detectable as the imprinted serial number would be identifiable on the a publically available ledger

Democratic voting

Blockchain could be the technology which enables the transparent and secure, yet anonymous voting to be performed entirely online. Due to the lack of a central server, it is not possible to tamper with the voting process underway on a blockchain in an undetectable way, and unlike in paper voting, votes cannot be misplaced or lost in the traditional sense.

By treating transactions as votes, a blockchain could keep track of all votes cast. The votes would be visible transparently and the final count would be indisputable as the votes would be publically visible and able to be counted by anyone, along with an audit trail ensuring that no votes were changed, removed, nor illegally added. While this information would be publically available, personal voting preferences would be secure as no personal information can be linked to a publically visible transaction address.

As long as the initial disbursement of voting bitcoins to individuals are ensured and valid, the process of voting itself could be secure and indisputable.

Real estate auction

An auction contract is publically visible on the blockchain outlining all conditions of the sale and the asset. The blockchain registry is advertised to potential bidders. With special conditions on the smart contract, individuals could bid on the contract, with the contract set to execute on the highest bidder after a certain specified time, along with other various conditions such as reserve. The smart contract will execute if the conditions are all met and validated, and will not execute at the given time if all conditions are not met. The execution of the contract would be linked to the asset title holding on the blockchain itself which would transfer to the new owner automatically, all without the need for any intermediary. The purchase money, in the form of bitcoins would also be authorised to change ownership in the same transaction all at once.

Existing Applications

With aspirations of realising the full potential of the blockchain technology, hundreds of new blockchain based crypto currencies have been and continue to be developed by constantly emerging new start-ups. The largest examples include: Ethereum (enable programmable smart contracts), Ripple (financial institution international payment focus), Litecoin (alternative to bitcoin), and Monero (bitcoin with protocol differences). Due to the emerging nature of the technology, many such projects are still constantly under development and work as proof of concepts.

Ethereum

Ethereum is one of the leading smart contract protocols with $1 billion (USD, October 2016) market capitalisation in Ethers (Ethereum equivalent of a bitcoin). The blockchain of Ethereum has the native ability to program in smart contracts for every transaction, while also being a crypto curency, allowing for complex transactions and contracts between untrusted parties.

Ethereum Smart Contract Auction Example

```
function bid() {
        if (now > auctionStart + biddingTime)
                Throw;
        if (msg.value <=highestBid)
                throw;
        if (highestBidder != 0)
                highestBidder.send(highestBid);
                highestBidder=msg.sender;
                highestBid = msg.value;
                HighestBidIncreased(msg.sender, msg.value);
}

//end the auction and send the highest bid to the beneficiary.

function auctionEnd() {
        if (now <= auctionStart + biddingTime)
                throw;  //auction did not yet end
        if (ended)
                throw; //this function has already been called
        AuctionEnded(highestBidder, highestBid);
        beneficiary.send(this.balance);
        ended=true;
}
```

Source: www.ethereum.nz, 3months.com

Everledger

A more clear-cut example of blockchain registry implementation, Everledger is a permanent ledger for diamond certifications and transaction histories. While it has started with diamonds, it could easily extend to any other luxury item which typically rely on paper certificates such as luxury watches.

Conclusion

When bitcoin was anonymously and mysteriously released publicly, great optimism arose over the potential for a revolution in the transaction of currencies. While it is not clear if the currency will become mainstream, this may in fact only be just the first application for the underlying technology - the blockchain. The concept can also be altered to be used for much more complex financial transactions, giving rise to the idea of "smart contracts" that can execute themselves irrefutably, immutably, and transparently - all automatically without the need of a trusted third party intermediary or arbitrator.

It is still very early days in the development of blockchain smart contract technology, however with such a large portion of the global economy based on the provision of intermediary services, a smart contract protocol has the potential to disrupt almost all of these industries. Traditional industries may not only be those disrupted. Services providers of the likes of Uber, airbnb, and kickstarter, which are regarded as major disruptors within the current technological generation, could also potentially be replaced by an intermediary-less medium which smart contract blockchains would enable. This has led many to look beyond the bitcoin and realise the true potential of the smart decentralised financial contracts of the future.

References

Bitcoin.org, from https://bitcoin.org/en/

Crypto-Currency Market Capitalizations, from https://coinmarketcap.com/

Deloitte 2016: *Blockchain applications in insurance*, from https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdfs

Ethereum.nz conference 2016, from http://www.ethereum.nz/

Ethereum.org, from https://www.ethereum.org/

Everledger, from http://www.everledger.io/

Peck, M. 2015a: IEEE Spectrum: *The Future of the Web Looks a lot like Bitcoin*, from http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin

Peck, M. 2015b: IEEE Spectrum: *The Bitcoin Blockchain Explained*, from http://spectrum.ieee.org/video/computing/networks/video-the-bitcoin-blockchain-explained

The Economist. 2015: *The great chain of being sure about things*, from http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable