Saurabh Kumar
MSc AIS(18441238)
Hong Kong Baptist University
18441238@life.hkbu.edu.hk

Blockchain*

History

The introduction of Bitcoin in 2009 by way of Satoshi Nakamoto may be considered as a Pioneer moment within the evolution of virtual forex. Although modern, as it turned into the primary decentralized cryptocurrency, Bitcoin's maximum considerable contribution to the sector is that it added to the mainstream standards like blockchain and smart contracts.
despite the fact that the primary work on a cryptographically secured chain of blocks started 1991 via pioneers of the enterprise, Stuart Haber and W. Scott Stornetta and continued at some stage in the mid-2000's. The first blockchain changed into conceptualized by using Satoshi Nakamoto in 2008, which later applied as a central factor of Bitcoin.

Introduction

The aim of this paper is brief exploration of blockchain, with the key inquiries to be answered:

- What is blockchain?
- How does it work?
- It's possibilities.
- Future improvements.
- Blockchain Applications

In order get answer all of those queries initially . This paper are going to be a survey of what people have already written on blockchain, analysis done on blockchain or perhaps achieved with blockchain. For the last question this paper can try and provide a epigrammatic summary of the various variables that each one have one thing to try with blockchain and the way they act with one another. And it'll offer some insights into however the creator of the blockchain will influence bound aspects of the blockchain.
There are speedy developments among blockchain and currently going on. There are many alternative varieties of blockchain that surfaced, every slightly completely different from each other in many alternative respects. For this reason this paper focusses on the primary blockchain, the Nakamoto blockchain that is that the most documented blockchain because of its association to Bitcoin.
Even with this restriction, there many new terms and ideas that area all tangled with one another.

Blockchain Architecture Considerations:

To better understand blockchain we first need to discuss the design aspects –

- Blockchain platform
- Nodes overall in blockchain & the its discovery process
- Transactions which makes blocks running in the Nodes
- Security that produces the Blocks
- Adding newer blocks to the Chain

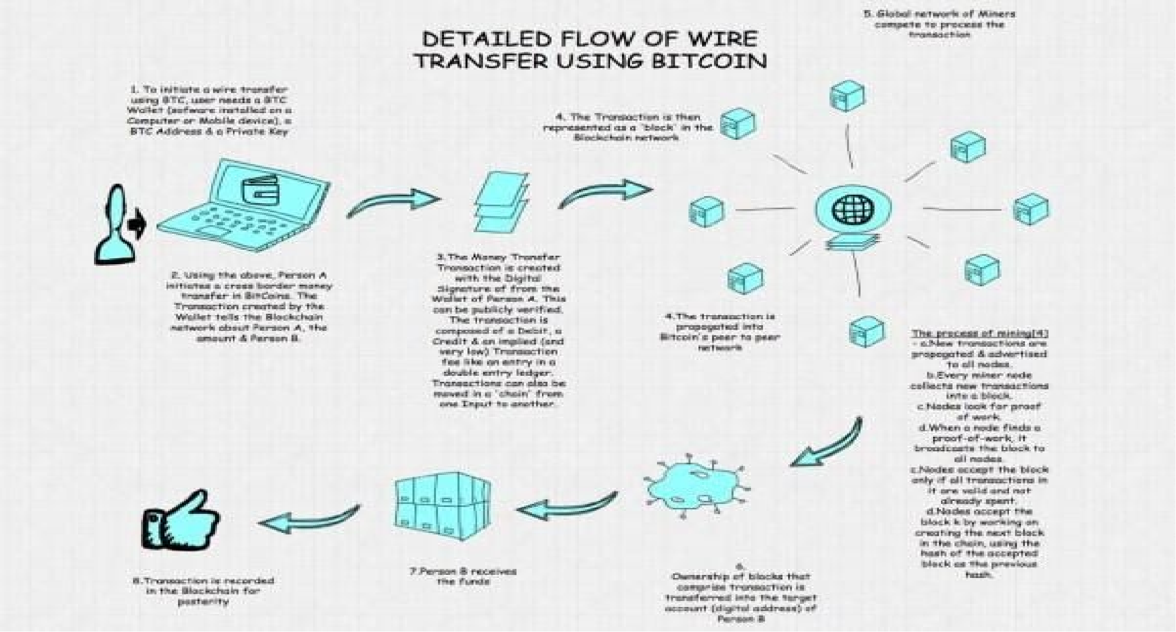

DETAILED FLOW OF WIRE TRANSFER USING BITCOIN
1. To initiate a wire transfer using BTC, user needs a BTC Wallet (software installed on a Computer or Mobile device), a BTC Address & a Private Key
2. Using the above, Person A initiates a cross border money transfer in BitCoins. The Transaction created by the Wallet tells the Blockchain network about Person A, the amount & Person B.
3.The Money Transfer Transaction is created with the Digital Signature of from the Wallet of Person A. This can be publicly verified. The transaction is composed of a Debit, a Credit & an implied (and very low) Transaction fee like an entry in a double entry ledger. Transactions can also be moved in a 'chain' from one Input to another.
4. The Transaction is then represented as a 'block' in the Blockchain network
4.The transaction is propogated into Bitcoin's peer to peer network
5. Global network of Miners compete to process the transaction
The process of mining[4] - a.New transactions are propogated & advertised to all nodes. b.Every miner node collects new transactions into a block. c.Nodes look for proof of work. d.When a node finds a proof-of-work, it broadcasts the block to all nodes. c.Nodes accept the block only if all transactions in it are valid and not already spent. d.Nodes accept the block k by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
6. Ownership of blocks that comprise transaction is transferred into the target account (digital address) of Person B
7.Person B receives the funds
8.Transaction is recorded in the Blockchain for posterity

Fig: 1 – Wire Transfer of Bitcoin using the Blockchain shared ledger

Blockchain Platform

Blockchain runs at the dispensed network of severs. Foremost utility is a transaction database modelled as isolated ledger, this is shared by means of all nodes (servers) that run the full stack install. It is consequently a one hundred % decentralized transaction flow that acts as a tremendously translucent ledger. Any node running the Blockchain software program can run the complete Blockchain regionally. At the same time as the Blockchain data can be stored in any relational it can also be stored in a flat document depending on user preferences.

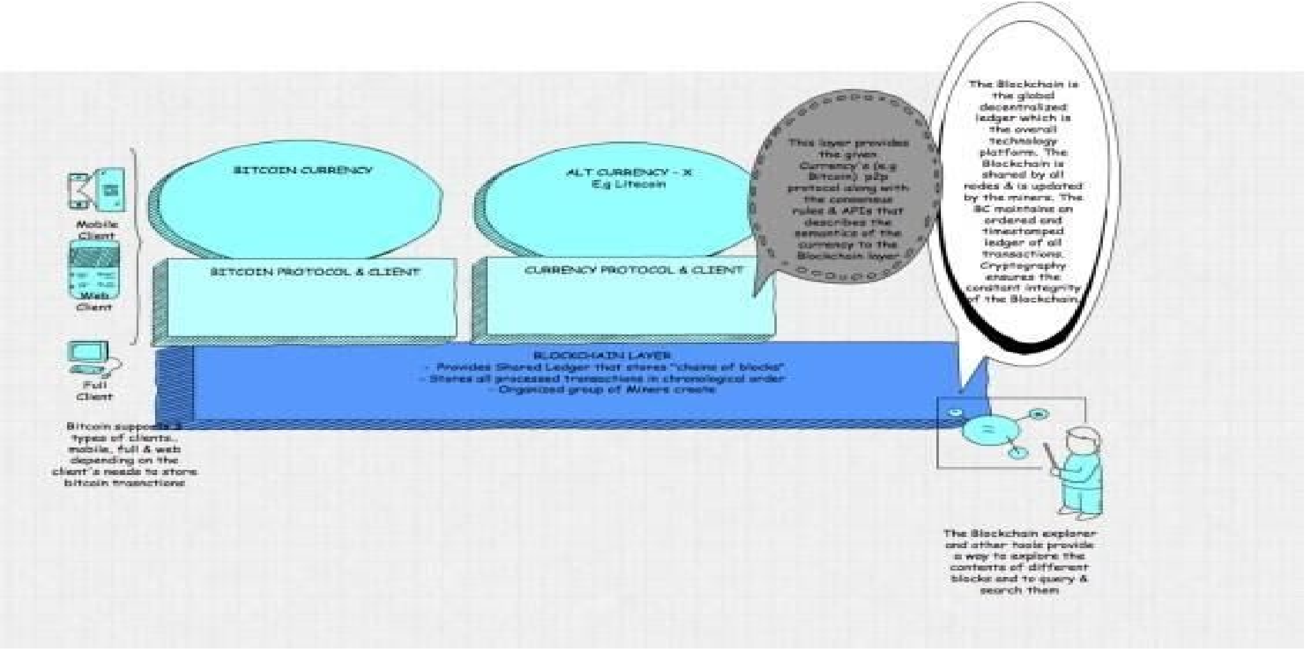
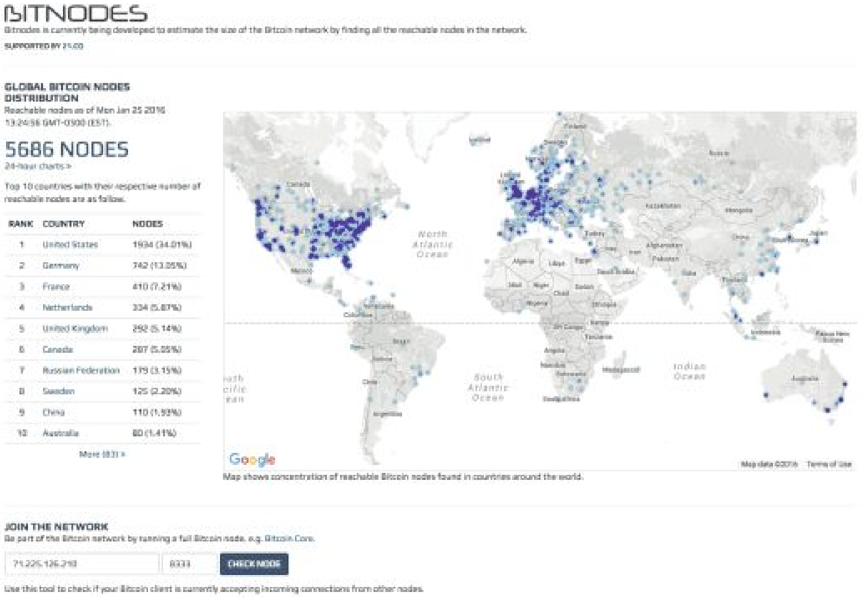

Mobile Client
Web Client
Full Client
Bitcoin supports 3 types of clients.. mobile, full & web depending on the client's needs to store bitcoin transactions
BITCOIN CURRENCY
ALT CURRENCY - X Eg Litecoin
BITCOIN PROTOCOL & CLIENT
CURRENCY PROTOCOL & CLIENT
This layer provides the given Currency's (e.g Bitcoin) p2p protocol along with the consensus rules & APIs that describes the semantics of the currency to the Blockchain layer
The Blockchain is the global decentralized ledger which is the overall technology platform. The Blockchain is shared by all nodes & is updated by the miners. The BC maintains an ordered and timestamped ledger of all transactions. Cryptography ensures the constant integrity of the Blockchain.
BLOCKCHAIN LAYER
- Provides Shared Ledger that stores "chains of blocks"
- Stores all processed transactions in chronological order
- Organized group of Miners create
The Blockchain explorer and other tools provide a way to explore the contents of different blocks and to query & search them

Fig 2 – Blockchain Architectural Layers

Nodes in the Blockchain:

Blockchain is a peer to see (P2P) network functioning at the IP protocol on the net. A Peer to peer community is essentially a flat topology with no centralized node, hierarchy, or unique server node. All nodes equally provide & can take services while collaborating thru a consensus service. The nodes inside the blockchain play the role of a primary bank or a depended on third party. Every node have the copy of a the blocks database that consist of the price entary of every bitcoin ever created and the owner information.
The graphic below shows the current number of nodes active in the bitcoin network and their locations on the globe.



BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

SUPPORTED BY 21.CO

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon Jan 25 2016 13:24:56 GMT-0500 (EST).

5686 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1934 (34.01%)
2	Germany	742 (13.05%)
3	France	410 (7.21%)
4	Netherlands	334 (5.87%)
5	United Kingdom	292 (5.14%)
6	Canada	287 (5.05%)
7	Russian Federation	179 (3.15%)
8	Sweden	125 (2.20%)
9	China	110 (1.93%)
10	Australia	80 (1.41%)

More (83) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

JOIN THE NETWORK

Be part of the Bitcoin network by running a full Bitcoin node, e.g. Bitcoin Core.

71.225.126.210 | 8333 | CHECK NODE

Use this tool to check if your Bitcoin client is currently accepting incoming connections from other nodes.

Fig 3 – Blockchain Nodes – Jan 25,2016

There are 4 basic node types. All of the node types explores and maintain connectivity with peers & validate blocks.
Full nodes keeps the complete copy of the blockchain database and can check any operation without the need for an external check-up. On the other side, nodes that only store a subset of the blockchain database verify transactions using a method called Simplified Payment Verification (SPV).

Miners perform the core method by that transactions get confirmed & processed and eventually enclosed within the blockchain. To be confirmed as valid, transactions 1st packed in an exceedingly organization & format referred to as a Block that should satisfy crypto rules that get verified by the blockchain network. Cryptography additionally prevents already added blocks from being additional changed as doing thus would invalidate all following blocks – that secures system integrity.
The manual labourer node thought is exclusive to blockchain because it confers it a high level of security as a result of half the manual labourer nodes dearly termed the "51% attack " (which may be a computationally not possible deed to perform at scale), the network can not be compromised or seized.

Network Protocol Stack: Once nodes get started, they perform a peer discovery to contact the other valid node employing a given port over TCP protocol. The Blockchain stack is represented below and is superimposed on the OSI stack. The Blockchain Message Exchange specifies the acknowledgment logic between nodes yet because the serialisation format for messages changed over the wire.

The Blockchain Intersection Network provides higher level linguistics that permit multiple varieties of blockchains (public, vertical specific blockchains) to co-exist yet as provides management abstraction for an equivalent. Developers can basically use this layer to increase bland blockchain to support other forms of applications which might leverage the present blockchain to validate their transactions. E.g. other forms of virtual currency, sidechains etc.

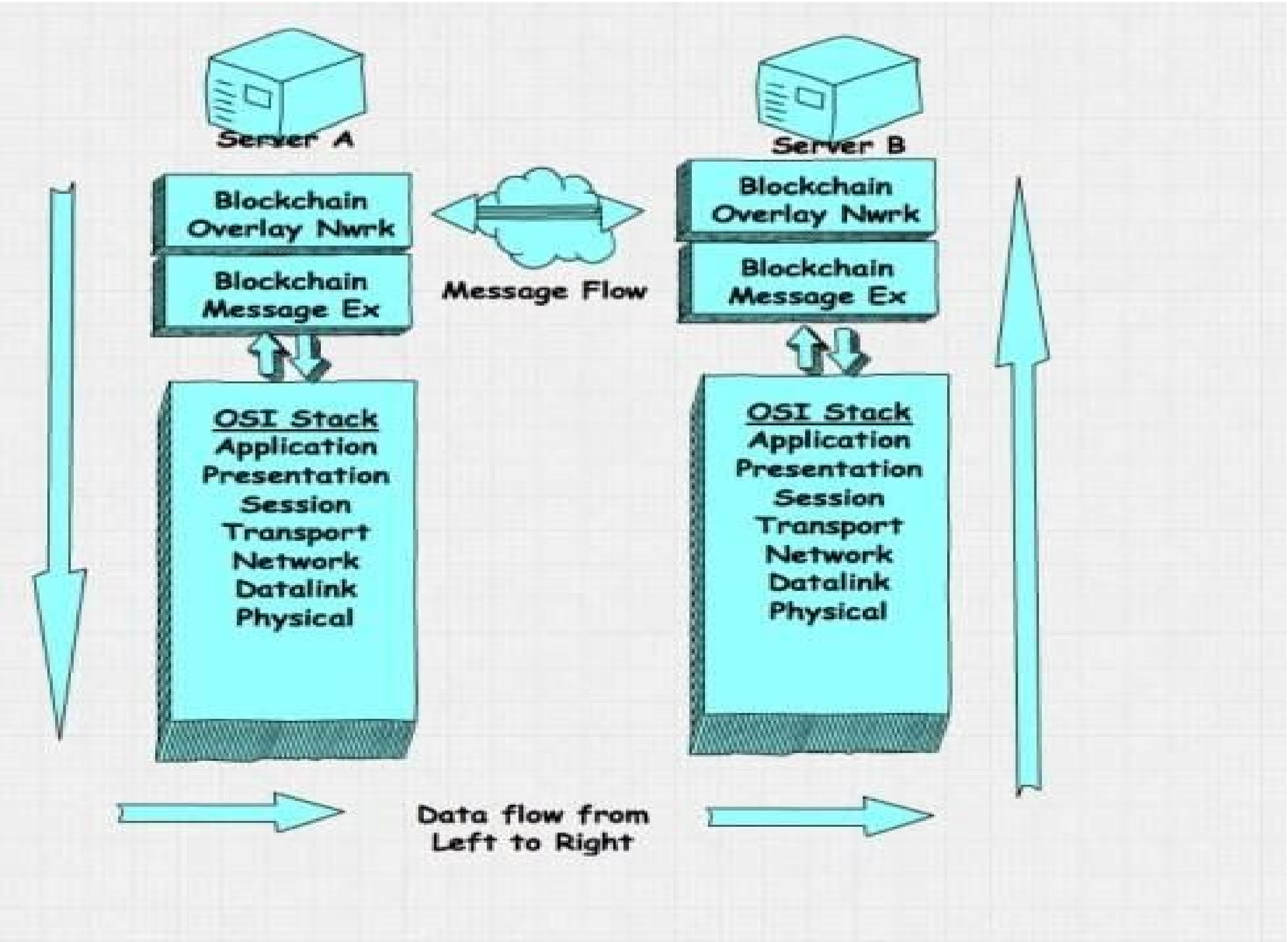


Fig :4- Blockchain Network Architecture

Transactions and Blocks:

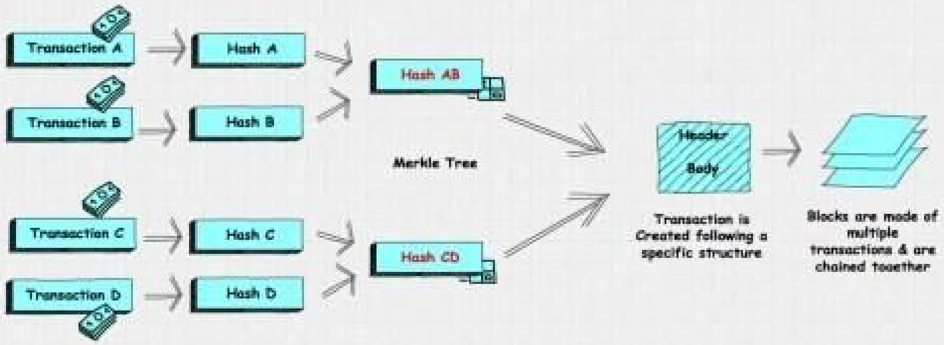
The blockchain execution consists of two kinds of records: transactions and blocks.

Salient features of transactions –

Transactions can be created by any client using a Mobile Wallet or any other client app.

Transactions consist of the real business data to be stored in the blockchain

Blocks keeps the sequence of transactions in the blockchain. Transactions are entered into the blockchain based on certain sequences


Transaction A
Hash A
Transaction B
Hash B
Hash AB
Merkle Tree
Transaction C
Hash C
Transaction D
Hash D
Hash CD
Header
Body
Transaction is Created following a specific structure
Blocks are made of multiple transactions & are chained together

The illustration above shows a simplified version of how individual transactions are combined to create blocks that are eventually chained together. A block of one or more new transactions is collected into the transaction data part of a block. A data structure called the merkle root is stored in the block header. This ensures an already recorded transaction cannot be modified or otherwise changed without modifying the block that records it and all following blocks. Each block of transactions also stores the hash of the previous block's header thus chaining the blocks together.

Fig:5- Transactions are converted into Blocks

The illustration shows however forex transactions into blocks. As may be seen, once a dealings (typically a booth purchase or wire transfer or Mastercard payment etc) is acquiesced into the system, a dealings (say dealings A) is generated that's pushed into the blockchain node network. A mineworker node(s) intercepts this to try some health checking, once done and it's determined that this is often a legit dealings, it's fed into a cryptographical hash operate as pictured to come up with a novel string of digits. it's then even be combined with alternative transactions as shown. The created hash is then hold on with alternative information into the header of a knowledge structure known as a block. The header is vital because it becomes the premise for running the hash operate once more to form a baby block.

The hash operation is employed because the scientific discipline puzzle that the miners race to resolve by wanting over just about trillions of potentialities. The mineworker that solves it 1st submits it for a check by alternative nodes and once found, the block is hold on into the blockchain for posterity. The mineworker node is then attributable a really tiny proportion of the dealings as fees.

Blockchain: Future Improvements.

Blockchain was firstly created only for decentralising ledger for Bitcoin. Now, Blockchain technology seems to influence vast number of industries within the very couple of years.

Some of the most exciting future blockchain improvements.

Improved automation

We've seen the start that what can be accomplished with smart contracts, however there's plenty to come.

We are motivated to believe it won't be long till all insurance claims are settled mechanically due to algorithms keep among sensible contracts. All the knowledge required to method a claim (from multiple sources) and judge the proper outcome can mechanically be keep among the blockchain. Ultimately, the method of subsidence the claim will begin while not somebody's lifting a finger.

This will serve to enhance the accuracy of claims, whereas cutting the price for insurance firms, permitting them to lower premiums (if they need to try to so).
The improvement of smart contracts and thus the automation of blockchain can play an enormous role in its mass adoption across many totally different industries. Many start-ups performing on introducing a blockchain-based answer to political ballot. In The insurance sector the automation of blockchain will improve the accuracy of claims, while reducing the cost for insurance company, so that they can lower premium costs.

Improved speed

Improving the speed of Blockchain processing is very much needed, because this is something which pushes it back. To process a single block the current processing time is 6Second per block. There have been a recent development which is done by one company named DasCoin who claims to decrease the processing time from 6 second to 3 seconds, which is tremendous development. But in comparison the Visa merchant does 5000 transactions per second huge difference. Though the Visa is not based on blockchain principle. There is much work needed in improving the transaction speed (and maybe better security too).

Improved (DAO) decentralized autonomous organizations

The concept of decentralized autonomous organizations (DAOs) was one of the most talked uses of the blockchain. $150+ million worth of capital funding was raised in to launch the first DAO (called'The DAO) in 2016, but this was right way hacked and the project was eventually sacked. DAOs has shut down, but there is still many work going on to improve the capacity of blockchain technology. We can't predict what the future has to offer, but one thing is for sure — blockchain technology had only touched the surface of what we'll see happen in the coming years.

Blockchain Applications

Blockchain Applications That Are Shaping Your Future.Blockchain information storage can become a huge disruptor shortly. (3-5 years).Current cloud storage services many centralized — The users should place trust in an exceedingly single storage supplier. "They" management all of your on-line assets.

On the opposite hand with the Blockchain, this will become suburbanised it is also in beta-testing cloud storage employing a Blockchain-powered network to enhance security and reduce dependency. To boot, users (you) will loan their excess storage capability, Airbnb-style, making new marketplaces.

Anyone on the net will store your information at a pre-agreed value. Hashing and having the info in multiple locations square measure the keys to securing it.

Digital Identity

Blockchain technology answer to several digital identity problems, wherever identity is unambiguously attested in an incontrovertible, immutable, and secure manner. Current ways use problematic password-based systems of shared secrets changed and hold on insecure systems. Blockchain-based authentication systems area
unit supported incontrovertible identification victimization digital signatures supported public key cryptography. In blockchain identity authentication, the sole check performed is whether or not or not the dealings was signed by the right personal key. it's inferred that whoever has access to the personal secret's the owner and therefore the precise identity of the owner is deemed irrelevant .

Smart Contracts

Smart contracts solve the matter of go-between trust between parties to an agreement, whether or not that's between individuals transferring assets like gold, or execution choices between two parties in an exceedingly contract.

Conclusion

As mentioned higher than, most of those applications square measure still underdeveloped the long run potential of the blockchain applications remains un raveling. consecutive couples of years are going to be all regarding experimenting and applying to all or any aspects of society. despite that application comes 1st on a worldwide scale. all-time low line is, Blockchain is here to remain and is re modelling however our society functions.

References

https://blockchain.info/api
https://bitcoin.org/en/developer-reference
”Mastering Bitcoin” – Andreas Antonopoulus – O’Reilly Press
https://bitnodes.21.co
https://en.wikipedia.org/wiki/Bitcoin_network
https://en.wikipedia.org/wiki/Block_chain_(database)
https://en.wikipedia.org/wiki/Blockchain
https://www.packtpub.com/mapt/book/big_data_and_business_intelligence/9781787125445/1/ch01lvl1sec8/the-history-of-blockchain
https://blog.modex.tech/a-brief-history-of-blockchain-smart-contracts-and-their-implementation-c3ac6f00f014
https://finance.yahoo.com/news/brief-history-blockchain-120057718.html
https://www.huffingtonpost.com/ameer-rosic-/5-blockchain-applications_b_13279010.html