HARRY BLAZER's NOTES FOR SPECIAL SOLARI REPORT BITCOIN: THE OP

I have quoted liberally from the following sources:

http://www.bitcoingroup.com.au

https://www.blockchainglobal.com

Wikipedia

Colin Cantrell's talk at Nexus Conference: https://www.youtube.com/watch?v=4HLzgDxcFH0&t=1137s

What is a Bitcoin: - It is the most popular crypto-currency and the first commercial implementation of a crypto-currency.

What is a Crypto-currency or Crypto-coin: A form of digital currency (virtual) that is produced by solving mathematical problems based on cryptography. It is in essence a chain of digital signatures.

What is Cryptography: **Cryptography** or **cryptology** (from Greek κρυπτός *kryptós*, "hidden, secret"; and γράφειν *graphein*, "writing", or -λογία *-logia*, "study", respectively[1]) is the practice and study of techniques for secure communication in the presence of third parties called adversaries.[2] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages;[3] various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation[4] are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, and communication science. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons from doing the same. The cryptography literature often uses the name Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.[5] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms. (wiki - https://en.wikipedia.org/wiki/Cryptography)

What is a Blockchain: A network of distributed databases used to maintain an immutable public ledger of transactions. It represents a record of all validated transactions grouped into blocks, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a "chain of blocks". Bitcoin represents the first commercial use of the blockchain.

A blockchain[1][2][3] – originally block chain[4][5] – is a continuously growing list of records, called blocks, which are linked and secured using cryptography.[1][6] Each block typically contains a hash pointer as a link to a previous block,
[6] a timestampand transaction data.[7] By design, blockchains are inherently resistant to modification of the data. A blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."[8][not in citation given (See discussion.)] For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which needs a collusion of the network majority.

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.[9] This makes blockchains potentially suitable for the recording of events, medical records,[10][11] and other records management activities, such as identity management,[12][13][14] transaction processing, documenting provenance, or food traceability.[15]

The first distributed blockchain was conceptualised by an anonymous person or group known as Satoshi Nakamoto, in 2008 and implemented the following year as a core component of his digital currency – Bitcoin – where it serves as the public ledger for all transactions.[1][not in citation given (See discussion.)] 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]

(wiki -https://en.wikipedia.org/wiki/Blockchain)

What are the origins of the Blockchain-based Bitcoin: Bitcoin is the first implementation of a concept called crytocurrency which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published by Satoshi Nakamoto and used the Blockchain.

Who is Satoshi Nakamoto? We don't know. But we know that the name is a pseudonym for the inventor of the Bitcoin protocol (in a Paper called: *Bitcoin: A Peer-to-Peer electronic Cash System),* which was made public via the Cryptography Mailing List in November 2008. This person or entity or group of persons then released the first version of the Bitcoin software client in 2009, and participated with others on the project via mailing lists until he, she, they, it faded away in the end of 2010. This entity was a member of the team that created the "open-sourced code" that runs the Bitcoin network but never revealed anything personal. The last anyone heard from Satoshi was in 2011, when this entity said "he had moved on to other things". Some estimate that he might have mined what are now billions worth of Bitcoins before "departing".

According to the Bitcoingroup.com.au:

Satoshi means "clear thinking, quick-witted, wise. Naka can mean "medium, inside or relationship" Moto can mean "origin" or "foundation". Those things would all apply to the person who founded a movement by designing a clever algorithm – which he did.

But someone we met at the Nexus conference, who was of Japanese decent and fluent in Japanese also interpreted the name this way:

Regarding the direct translation of Satoshi Nakamoto, the Japanese language is full of homophones, so Satoshi Nakamoto can be written in several different ways. However the most common way would be like this: 中本聡

In Japanese, the surname is written and spoken before the first name, so breaking it down:

Nakamoto: 中本

中 = *Center, central*

本 = *Origin, root, basis*

Satoshi: 聡 = *knowledgeable, intelligent, intelligence*

*So putting them all together, Satoshi Nakamoto or in effect Nakamoto Satoshi (*中本

聡*) translates to "the origins or roots are center intelligent" or can be understood as "originated inside central intelligence". I hope this all makes sense. If you believe that the powers that be like to hide their actions and intentions in plain site, then this name certainly is quite interesting.*

Let's look at this 8-page paper written by Satoshi that everyone quotes as the foundational document for Bitcoin to see what it says:

First we need to define a few terms:

Hash:

An algorithm (math function) which turns random sized data into a string of numbers of a fixed size (a signature), designed to be irreversible (infeasible to revert). According to Wikipedia the ideal cryptographic hash function has five main properties:

- *it is deterministic so the same message always results in the same hash*
- *it is quick to compute the hash value for any given message*
- *it is infeasible to generate a message from its hash value except by trying all possible messages*
- *a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value*
- *it is infeasible to find two different messages with the same hash value*

Hash Rate:

The number of calculations that your hardware can perform every second. Hash rates are measured in megahashes (MH/sec,), gigahashes (GH/sec,), and terahashes (TH/sec). The higher your hash rate compared to the current average hash rate, the more likely you are to solve a transaction block.

There are three main hardware categories for Bitcoin miners: CPU/GPU (graphic cards used in gaming); FPGA (Field programmable gate array -an integrated circuit designed to be configured after being built so they are customizable for Bitcoin mining; ASIC – an Application Specific Integrated Circuit – a silicon chip specifically designed to do a specific task which in this case is to process SHA-256 hashing problems for Bitcoin mining.

Node:

A computer or series of computers connected to the Bitcoin network that relays transactions to others.

Nonce:

An arbitrary number used only once in a cryptographic communication. Many nonces also include a timestamp.

Nonces are used in proof-of-work systems to vary the input to a cryptographic hash function so as to obtain a hash for a certain input that fulfills certain arbitrary conditions. In doing so, it becomes far more difficult to create a “desirable” hash than to verity it, shifting the burden of work onto one side of a transaction or system.

The Bitcoin Blockchain hashing algorithm can be tuned to an arbitrary difficulty by changing the required minimum/maximum value of the hash so that the number of Bitcoins awarded for new blocks does not increase linearly with increased network computation power as new users join. This is likewise achieved by forcing Bitcoin miners to add nonce values to the value being hashed to change the hash algorithm output. Because cryptographic hash algorithms cannot easily be predicted based on their inputs, this makes the act of blockchain hashing and the possibility of being awarded Bitcoins something of a lottery, where the first "miner" to find a nonce that delivers a desirable hash is awarded valuable Bitcoins.

(wiki https://en.wikipedia.org/wiki/Cryptographic_nonce)

Mining:

The act of generating new Bitcoins by solving complex cryptographic puzzles using computing hardware. A key: those cryptographic problems are in essence verifying/confirming transactions in the Bitcoin network, which is the equivalent of finding valid blocks and securing the global record of all transactions (the blockchain). Miners get rewarded in two ways for making the network work: through Bitcoins and through fees for validating transactions and maintaining the blockchain, thus making transactions possible . Note: the current difficulty level is so high that it is practically impossible for soloists or beginners to make a profit mining.

Proof of work:

A hashed block that is confirmed by the network as valid.

51% attack:

A condition in which more than half the computing power on a cryptocurrency network is controlled by a single miner or group of miners. That amount of power theoretically makes them the authority on the network. This means that every client on the network believes the attacker’s hashed transaction block. This gives them control over the network, including the power to:

- Issue a transaction that conflicts with someone else’s.
- Stop someone else’s transaction from being confirmed.

- Spend the same coins multiple times.
- Prevent other miners from mining valid blocks.

Turing Completeness:

In colloquial usage any real-world general-purpose computer or computer language is considered Turing Complete if it can approximately simulate the computational aspects of any other real-world general-purpose computer or computer language. In contrast, a universal computer is defined as a device with a Turing complete instruction set, infinite memory and infinite available time. Turing completeness is the ability for a system of instructions to simulate a Turing machine. A programming language that is Turing complete is theoretically capable of expressing all tasks accomplishable by computers. Nearly all programming languages are Turing complete if the limitations of finite memory are ignored.

Satoshi's Essay:

This essay is mostly in English with a little math at the end. But it is otherwise quite readable by ordinary folks. And also quite informative.

The vision: Non-intermediated peer to peer transactions of any size, done electronically over the net so transactions can occur anywhere, anytime, that are more efficient and cost effective than bank mediated transactions, using purely digital currency for payments that are non-reversible and structured so trust is superfluous.

Satoshi tried to solve for two primary problems that have in the past required the mediation of a trusted third party – double spend where the same piece of currency (Bitcoin) is used twice to make purchases; and reversibility of a transaction by a customer (figuring out ways to not pay for something that has been acquired).

Rather than go into detail about how he solved for these problems, let's summarize features of Bitcoin as it has evolved to the present:

1. Contains a public record of all transactions through the blockchain, which theoretically cannot be tied to an individual, that are confirmed as valid through consensus by a majority of nodes but which in turn increases overhead and transaction time as the Bitcoin network grows. This has been compared to a glass safety deposit box where everyone can see that there is something in the box but a specific user is the only one with the key to get in.
2. Time stamps for all transactions, which opens up the possibility for other uses of blockchain technology.
3. The need for wallets, exchanges, payment sectors – basically a whole superstructure of third party financial service providers (something Bitcoin

was supposed to make superfluous) where anonymity can no longer exist while opening up many more opportunities for hacking and fraud.

4. A Bitcoin wallet consists of two 'keys'. The public key, which is your wallet address and is how other people send Bitcoins to you; and the private key, which enables you to send Bitcoins to other people. The combination of the recipient's public key and your private key is what makes a crypto-currency transaction possible. If anyone else acquires the private key of your wallet, they can withdraw your funds. So if you keep your coins in either an online wallet or a hard-drive-based software wallet, you are vulnerable to attacks by hackers or malware that can log your keystrokes.

5. To send Bitcoins, you need two things: a Bitcoin address and a private key. A Bitcoin address is generated randomly, and is simply a sequence of letters and numbers. The private key is another sequence of letters and numbers, but unlike your Bitcoin address, this is kept secret. Think of your Bitcoin address as a safe deposit box with a glass front. Everyone knows what is in it, but only the private key can unlock it to take things out or put things in. When Alice wants to send Bitcoins to Bob, she uses her private key to sign a message with the input (the source transaction(s) of the coins), amount, and output (Bob's address). She then sends them from her Bitcoin wallet out to the wider Bitcoin network. From there, Bitcoin miners verify the transaction, putting it into a transaction block and eventually solving it.
6. Because Bitcoins exist only as records of transactions, you can end up with many different transactions tied to a particular Bitcoin address. Perhaps Jane sent Alice two Bitcoins, Philip sent her three Bitcoins and Eve sent her a single Bitcoin, all as separate transactions at separate times. These are not automatically combined in Alice's wallet to make one file containing six Bitcoins. They simply sit there as different transaction records. When Alice wants to send Bitcoins to Bob, her wallet will try to use transaction records with different amounts that add up to the number of Bitcoins that she wants to send Bob. The chances are that when Alice wants to send Bitcoins to Bob, she won't have exactly the right number of Bitcoins from other transactions. Perhaps she only wants to send 1.5 BTC to Bob. None of the transactions that she has in her Bitcoin address are for that amount, and none of them add up to that amount when combined. Alice can't just split a transaction into smaller amounts. You can only spend the whole output of a transaction, rather than breaking it up into smaller amounts. Instead, she will have to send one of the incoming transactions, and then the rest of the Bitcoins will be returned to her as change. Alice sends the two Bitcoins that she got from Jane to Bob. Jane is the input, and Bob is the output. But the amount is only 1.5 BTC, because that is all she wants to send. So, her wallet automatically creates two outputs for her transaction: 1.5 BTC to Bob, and 0.5 BTC to a new address, which it created for Alice to hold her change from Bob.
7. Proof of work represented by the longest chain (containing the most computational work or hashing), which is designed to increase in difficulty

with time and in turn increases overhead and the need for more and more sophisticated and expensive mining resources over time.

8. Limits on how fast blocks can be generated, to control the generation rate of Bitcoins

9. Limits and minimums on size of blocks

10. Limits on number of Bitcoins that can be produced in total and in turn creating a situation where Bitcoin will be commoditized – i.e. become a speculative investment in and of itself (and thus undermine its function as a universal currency)

11. A mechanism for subdividing Bitcoins to increase liquidity once total limit is reached (a satoshi, named in honor of satoshi, is 100 millionth of a single Bitcoin). I believe the smallest transaction you can send is 5430 satoshies.

12. Irreversibility of a transaction, which also means no ability to recover a Bitcoin once its gone – i.e. spent or stolen.

13. Bitcoin core runs on generic databases that require a fair amount of processing that is not relevant for crypto-currencies. Two major ones are Level DB for indexing (a creation of Google) and Berkeley DB (4.8) to manage wallet.dat and keys (from Oracle).

14. As part of the blockchain, data is processed by every node. As the number of Bitcoins increase and the number of transactions on the network increase, difficulty for mining is designed to increase as well and theoretically the network becomes more secure because of the cost involved with attacking it (in computational resources and electricity).

15. But the bigger it gets, the slower it gets.

    a. Data processed by every node creates a chain reaction of decreased propagation time as the slowest node creates the bottleneck (only as good as the weakest link).

    b. Messages in Bitcoin Core are processed in a queue. This means that slower messages from a node or denial of service attacks on the protocol can cause block propagation delays. A blockchain is one-dimensional and obeys the queue so if it reaches capacity it has only one way to go – backwards – creating transaction backlogs.

    c. Orphan rate increases for many reasons also bogging the system down (Detached or orphan blocks are blocks that appear valid but which are not part of the main chain. They can occur naturally when two miners produce blocks at similar times and the system has to choose one over the other thus orphaning one, or they can be caused

by an attacker with superior hashing power attempting to reverse transactions.

d. There are extreme memory requirements given how Blockchain is indexed and how copies of block headers are stored – so heavy overhead

16. Blockchains are not quantum computer resistant and thus can theoretically be hacked. (There should be full blown quantum computers in 5 years) The ultimate goal of cryptology: you want the ability for an entity to crack a code to take more time (processing time) than the years in the universe. Bitcoin uses an encryption key called SHA256 . For a classical computer, this would require 2 to the 256 power computations to crack the code (2 times itself 256 times)! But for a quantum computer, it would only require 256 to the three power iterations – or 256 times itself 3 times. A much, much, much smaller number.

17. Bitcoin has scaled faster than Moore's law (price halves every 18 months while processing power doubles in that same time span) – so traditional efficiencies in technology cannot help maintain the Bitcoin system's efficiency

18. Bitcoins don't exist anywhere. There is talk about someone having Bitcoins, but when you look at a particular Bitcoin address, there are no digital Bitcoins held in it, in the same way that you might hold dollars in a bank account. You cannot point to a physical object or even a digital file and say "this is a Bitcoin". Instead, there are only records of transactions between different addresses, with balances that increase and decrease (thus the need for the blockchain). Every transaction that ever took place is stored in a vast public ledger (the blockchain). If you want to work out the balance of any Bitcoin address, the information isn't held at that address; you must reconstruct it by looking at the blockchain.

19. It is unclear to me how Bitcoin is able to maintain sufficient liquidity to fuel a growing economy i.e. how mining for blocks that produces new Bitcoins (increases money supply) correlates in time with actual economic requirement for liquidity. Also, difficulty in mining increases as more users and transactions join the network – so kind of the opposite of easing credit to increase money supply in the current system.

Key caveat: in his paper, Satoshi on a number of occasions and in various ways confirms that the system only works as long as honest nodes (miners) control more CPU power than any cooperating group of attacker nodes. But the ultimate irony is that by having to build in increasing complexity into the mining function (and remember mining is primarily about keeping the network vital through hashing – through intense computation), an arms race was created where increasing

processing capability would be required to stay in the game, thus allowing those with the greatest financial resources who could afford the most of the latest-greatest in processing power and the associated electric bill, to centralize control.

He ends a section on "Incentive" with the following paragraph:

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Perhaps Satoshi was unaware of an autonomous Deep State with hidden and virtually unlimited funding and computing power, whose main objective is control. If you have the control, the money will come. Centralized control leads to centralized control of wealth as well. Isn't it ironic that one of the primary goals of Bitcoin – the creation of a universal digital currency – is also a primary goal of the globalists, the New World Order with its aspirations for replacing national sovereignty with a one-world government - and arguably the Deep State.

Now let's listen to Colin Cantrell, the founder of the Nexus convention and Nexus earth, as he talks about fundamental constraints with Bitcoin and the Bitcoin network. His company is dedicated to coming up with solutions that solve for these problems and make it possible to use crypto-currencies as an actual currency. (18:57)

https://www.youtube.com/watch?v=4HLzgDxcFH0&t=1137s

Conclusion: So it seems that Bitcoin has failed to deliver on all of its promises:

Decentralization, Democratization, Incorruptibility, Disintermediation, Efficiency (fast transactions), Reliability, Cheap Transaction Costs, Confidentiality

And in turn it has failed as a scalable currency and is basically a highly speculative, volatile, financial play, which if enough people buy in the value will go up and in turn will be making relatively few people very rich. At current price of $4300 and an initial price of a few cents, this turns out to be roughly 400,000x rate of return for a few early players in a few years – unprecedented but also unimaginable in the history of finance.

Additional Notes:

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.

5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Four major players in the Bitcoin business:

Exchanges –used to buy, sell and trade crypto-currencies for other crypto-currencies and/or national currencies, thereby offering liquidity and setting a reference price.

Wallet providers: a way of securely storing crypto-currencies and managing keys required to do transactions

Payments sectors that provide a wide range of services to facilitate payments using cryptocurrencies.

Miners: responsible for confirming transactions and securing the global record of all transactions (the blockchain). What they are really mining for are blocks to be hashed and confirmed as valid by them for use by the network for Bitcoins and fees.