BITCOIN AND BEYOND: SOCIO-ECONOMIC FORCES, ADOPTION OPPORTUNITIES AND RISKS

DR JOSEPH IKHALIA

DR JOSEPH IKHALIA

- Blockchain Researcher Since 2014
- Former IT Security Manager of the First Fully Licensed Blockchain Lottery in the World.
- Bitcoin Miner Since 2018
- Founder of the Real Cyber Nation Community and Dr Ikhalia Cyber Bootcamp
- Group Information Security Governance Manager – Utmost Group

WHY BITCOIN?

2008 FINANCIAL CRISIS

Cryptography Mailing List

Bitcoin P2P e-cash paper

2008-10-31 18:10:00 UTC - Original Email - View in Thread

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

SATOSHI'S FIRST EMAIL

Bitcoin: A Peer-to-Peer Electronic Cash System

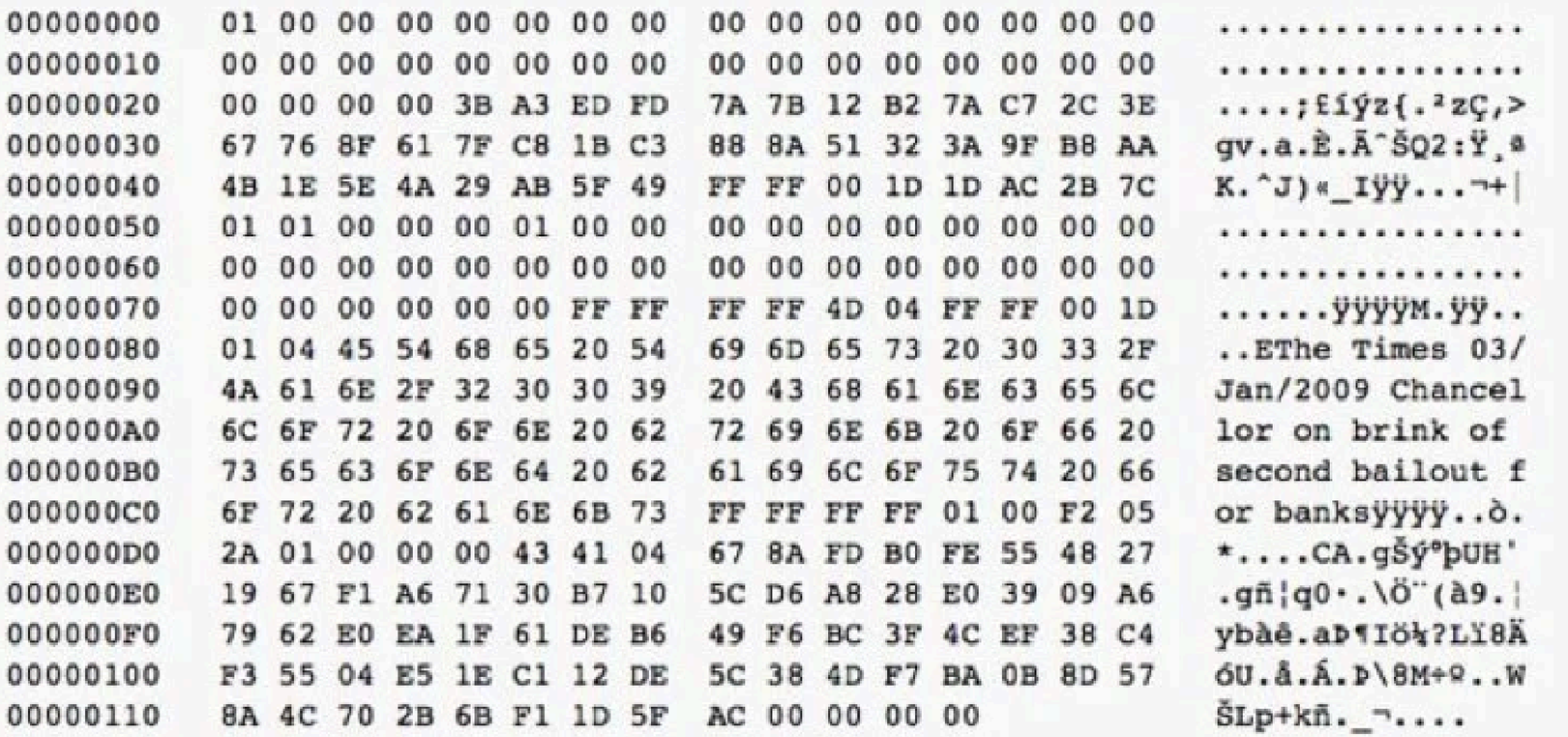
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

BITCOIN WHITE PAPER

RAW HEX VERSION

BITCOIN GENESIS BLOCK



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

THE FIRST BLOCK IN THE BITCOIN BLOCKCHAIN

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offiering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

HAL FINNEY

halfin

@halfin

Running bitcoin

7:33 PM - 10 Jan 2009

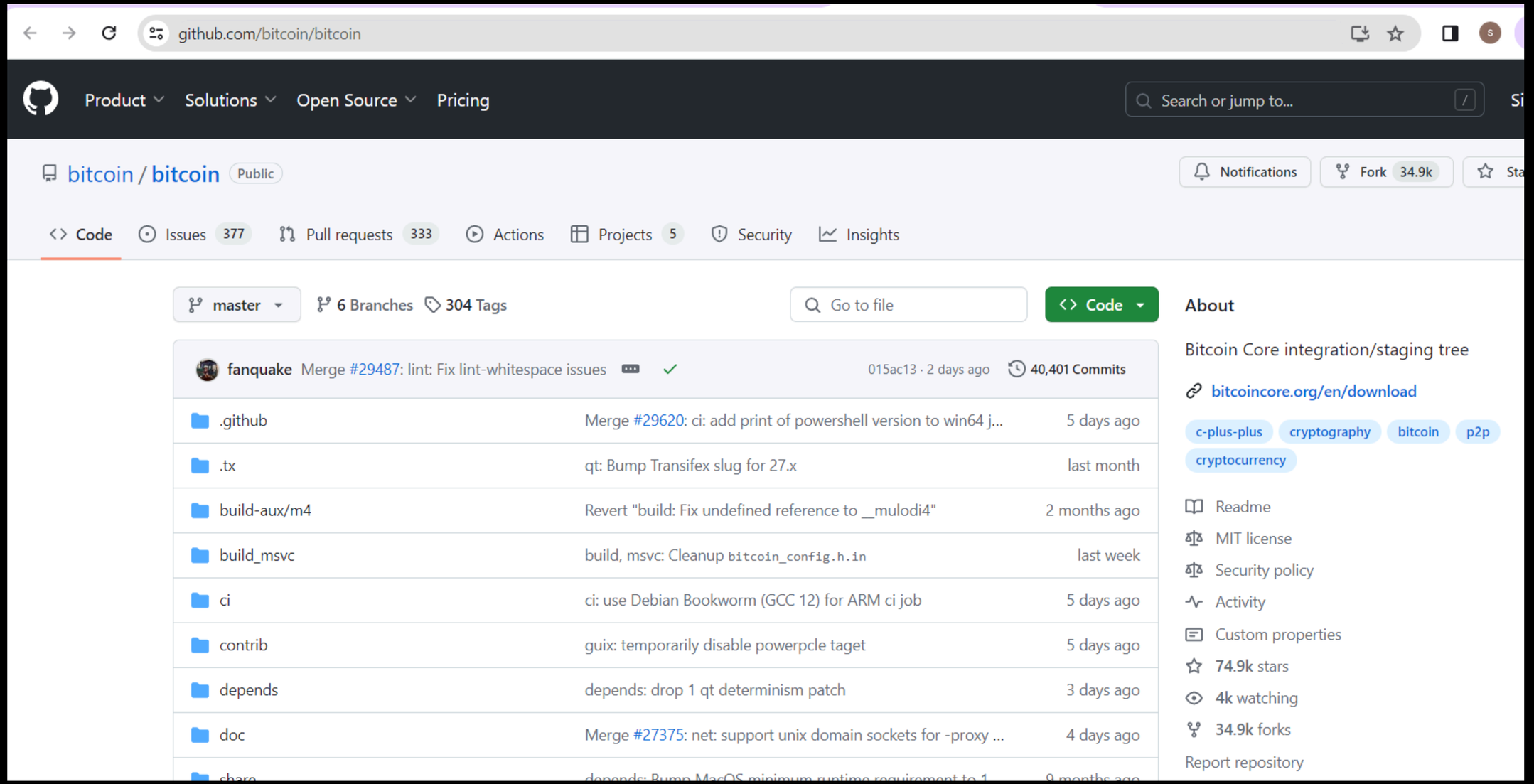
316 3.3K 8.1K

ONLY 21 MILLION BITCOIN WILL EVER EXIST

My choice for the number of coins and distribution schedule was an educated guess. It was a difficult choice, because once the network is going it's locked in and we're stuck with it. I wanted to pick something that would make prices similar to existing currencies, but without knowing the future, that's very hard. I ended up picking something in the middle. If Bitcoin remains a small niche, it'll be worth less per unit than existing currencies. If you imagine it being used for some fraction of world commerce, then there's only going to be 21 million coins for the whole world, so it would be worth much more per unit. Values are 64-bit integers with 8 decimal places, so 1 coin is represented internally as 100000000. There's plenty of granularity if typical prices become small. For example, if 0.001 is worth 1 Euro, then it might be easier to change where the decimal point is displayed, so if you had 1 Bitcoin it's now displayed as 1000, and 0.001 is displayed as 1.

WHY THE 21 MILLION CAP?

BITCOIN SOURCE CODE



https://github.com/bitcoin/bitcoin

BITCOIN NODES GLOBAL DISTRIBUTION

REACHABLE BITCOIN NODES

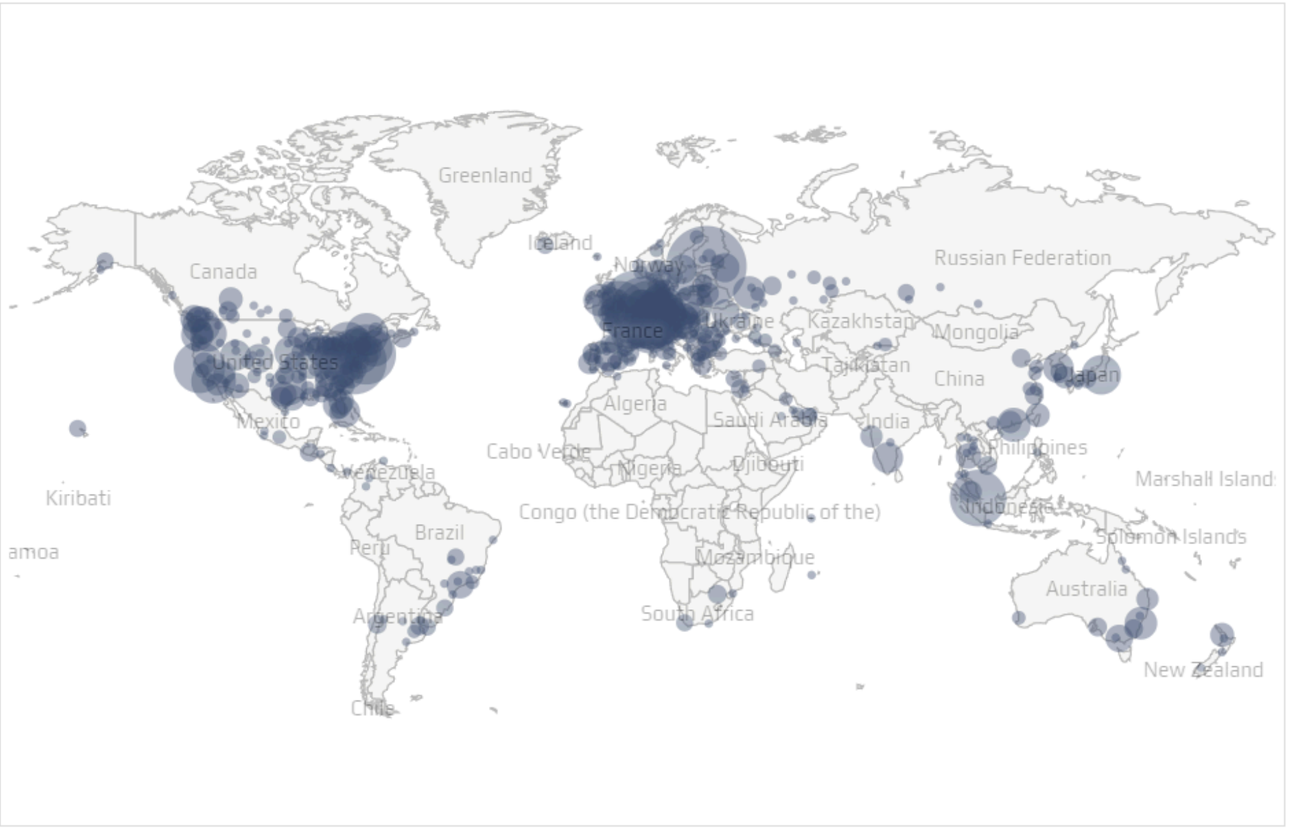
Updated: Sun Mar 17 19:44:45 2024 GMT

18794 NODES CHARTS

IPv4: +2.1% / IPv6: +8.5% / .onion: +11.5%

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

RANK	COUNTRY	NODES
1	n/a	12157 (64.69%)
2	United States	1598 (8.50%)
3	Germany	1595 (8.49%)
4	France	401 (2.13%)
5	Netherlands	340 (1.81%)
6	Finland	270 (1.44%)
7	Canada	270 (1.44%)
8	United Kingdom	199 (1.06%)
9	Russian Federation	169 (0.90%)
10	Singapore	150 (0.80%)



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

Activate Wind

https://bitnodes.io/

Bitcoin handles about 7 transactions per second (TPS), which is low compared to centralised systems like VISA, which can handle thousands of TPS.

Other “Blockchains”	Reason for Existence (Sarcastic)
Ethereum	To ensure that every decentralised app crashes your wallet with astronomical gas fees before it even becomes useful.
Cardano	To show the world that slow and steady wins the race—eventually. If it ever gets around to starting the race.
XRP	So banks can finally embrace decentralisation, but only if it's super centralized and controlled by one company.
Binance	A playground where crypto traders can enjoy the thrill of sketchy tokens
Solana	To give you lightning-fast transactions, as long as the network isn't taking one of its frequent “naps.”

BITCOIN ADOPTION

BITCOIN BULL AND BEAR MARKETS (2012 - 2024)

Phi-Deltalytics published on TradingView.com, September 14, 2019 19:17:19 EST

BITFINEX:BTCUSD, 1D 10399.0 ▲ +19.0 (+0.18%) O:10381.0 H:10400.0 L:10379.0 C:10399.0

PROPERTIES OF THE BITCOIN BLOCKCHAIN

DECENTRALISATION

There's no single authority controlling the Bitcoin Blockchain. Instead, a distributed network of computers around the world maintains a shared ledger of transactions. This eliminates the need for a trusted third party, like a bank, to verify transactions.

IMMUTABILITY

Once a transaction is recorded on the Bitcoin blockchain, it cannot be altered or deleted. This is because each block in a blockchain contains a cryptographic hash of the previous block, creating a tamper-proof chain of records.

TRANSPARENCY

All transactions on the Bitcoin Blockchain are publicly viewable. This transparency fosters trust and accountability within the network.

SECURITY

- Blockchain networks are highly secure thanks to cryptography and distributed ledger technology.
- Cryptography ensures that only authorised parties can access and modify data on the blockchain.
- Distributed ledger technology makes it nearly impossible to tamper with data on the blockchain, as any attempt to modify a record would have to be reflected in all copies of the ledger across the network.

IRREVERSIBILITY

Transactions on the Bitcoin Blockchain are irreversible. This means that once a transaction is confirmed, it cannot be reversed.

AUDITABILITY

Because all transactions on the Bitcoin Blockchain are recorded and publicly viewable, they are easily auditable.

https://www.blockchain.com/explorer/

SOCIO-ECONOMIC AND GEOPOLITICAL RISKS

SOCIO-ECONOMIC AND GEOPOLITICAL RISKS

- Financial System Disruption
- Wealth Inequality and Social Tensions
- Geopolitical Tensions and Sanctions
- Cybersecurity and Terrorism Financing
- Environmental Concerns

TECHNOLOGY RISKS

Dr. Joseph Ikhalia

Is Bitcoin's Security at Risk? Unveiling Three Crucial Issues

Joseph E. Ikhalia, Ph.D.

Jul 4, 2023 16

TECHNOLOGY RISKS

- Reduced Mining Incentives
- Hashrate Decline and Security Vulnerabilities
- Economic Factors Affecting Miners
- Long-Term Implications of Halving Events

BITCOIN OPPORTUNITIES

Dr. Joseph Ikhalia

Bitcoin’s Security: Riding the Wave of Global Liquidity

In a recent publication, I voiced my concerns regarding the security of the Bitcoin network, particularly as we...

May 6 11

BITCOIN OPPORTUNITIES

- Incentives for Renewable Energy
- Utilisation of Wasted Energy
- Liquidity Influx
- Global Trade Facilitation
- Nation-State Adoption

FOOD FOR THOUGHT

How might the increasing adoption of Bitcoin as legal tender in countries with cheap energy impact global economic dynamics and traditional financial systems?

THANK YOU!

QUESTIONS?

DrJosephIkhalia@gmail.com

WHAT'S NEXT?

- Subscribe to "The Real Cyber Doctor" on YouTube
- Register for My Monthly Cyber Bootcamp josephikhalia.com/cyberbootcamp