The Myths of Blockchain

History, technological realities & economic applications

Gunther Sonnenfeld ..: Co-Founder, Novena ..: January, 2021
More than anything else, the ‘blockchain’ is a mindset. It is not a single thing, a single approach nor a single solution. It can be used for good or ill purposes. What matters is the social, economic and environmental contexts in which it is applied, and the ways it can scale responsibly.
BACKGROUND

- world’s first Bitcoin POS system
- 14 international markets
- sold to private enterprise co.

- full energy ecosystem design
- integrated tech components
- corporate venture incubator

- IOT mobility scenarios
- market testing strategies
- civic utility explorations
BACKGROUND

Smart Ecologies

ecosystem development

Holonomials

algorithmic development

Non-Flationary Value

currency & asset development
CURRENT PROJECTS

- asset stabilization
- good carbon marketplace
- alternative healthcare
- content monetization

WE ARE AN AWARD-WINNING INNOVATION GROUP THAT TRANSFORMS FINANCIAL + ENVIRONMENTAL ASSETS WITH BLOCKCHAIN & DISTRIBUTED LEDGER TECHNOLOGIES.

https://www.novena.tech/
THE ARCHETYPE BLOCKCHAIN

caretaker verification  bundled treatment  data participation  advanced research
mobile apps  drug provenance  real-time monitoring  private profiling  elastic cloud

THE ARCHETYPE BLOCKCHAIN
We enable scarcity.

How?

By controlling access to digital goods through our decentralized gateway.

Just one of many underserved markets: academia.edu has 70 million users worldwide, sharing 150 million papers every year without any payment mechanism, nor means for authors to protect their material.

digitized academic paper

RAIR decrypt node provides a provably unique copy that the author can control, share and monetize in perpetuity.
Resale Economics

$8 secondary purchase
$4.80 to affiliate/reseller
$2.40 royalty to creator

$0.80 converted to RAIR tokens

.08 RAIR node
.72 RAIR monetization

DIGITAL OWNERSHIP ENCRYPTION
HISTORY
BLOCKCHAIN HISTORY

1940  • The Enigma Machine and the Purple Code were decoded.
1970  • An algorithm which split the encrypted keys into private and public was invented.
1992  • Merkle Tree
2004  • Reusable Proof Of Work system was introduced.
2009  • A Peer to Peer Electronic Cash System and blockchain introduction.
2005  • Ethereum Blockchain was invented.
The idea takes its roots from coding and deciphering. Early in the 1940s, a British mathematician Alan Turing, who was the first known cryptographer, deciphered the Enigma Machine. At the same time, the Americans decoded the Purple Code, a Japanese ciphering machine.
In the 1970s, Martin Hellman and Whitfield Diffie invented a special algorithm which split the encrypted keys into a pair — a private and a public key.
Developed in 1977 to encrypt & decrypt messages.
Then, in 1992, W. Scott Stornetta, Stuart Haber added Merkle Tree to the cryptography concept, boosting security, performance, and efficiency.
HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH

Laurie Law, Susan Sabett, Jerry Solinas
National Security Agency Office of Information Security Research and Technology
Cryptology Division
18 June 1996

Written 12 years before the infamous ‘Satoshi’ paper...
In 2004, a scientist and cryptographer Hal Finney introduced a system called RPoW, which was Reusable Proof Of Work. The system operated by getting a non-exchangeable Hashcash based PoW token and in return created an RSA-signed token that could then be transacted from person to person.

RPoW solved the double-spending problem by keeping the ownership of tokens registered on a trusted server. It also allowed users worldwide to verify its correctness and integrity in real-time.
BLOCKCHAIN HISTORY

Zug, Switzerland

+ home of interagency cryptography pre-WWII
+ international tax haven & intel hub
+ centralized repository for global ID profiling
Dorian Satoshi Nakamoto says he couldn’t have invented bitcoin—he’s too broke for internet access
THE MANY ‘SATOSHIS’

Laurie Law
Susan Sabett
Stefan Brands
David Chaum
Jerry Solinas
Amos Fiat
Tatsuaki Okamoto
Tony Eng
Torben Pederson
Moni Naor
Kazuo Ohta
Alfred Menezes
Neils Ferguson
Martin Hellman
Hal Finney
Jan Camenisch
Jean-Marc Piveteau
Markus Stadler
Craig Wright
Stuart Haber
Sebastian von Solms
Whitfield Diffie
Jan Camenisch
W. Scott Stornetta
David Naccache
John McAfee
I could be the inventor of Bitcoin.
Or the blockchain.
Which means I invented binary code, hashing algorithms and elliptical curves.
Yet, I bleed and my eyesight is degrading.
I could be Satoshi.
I could be your father from another mother.
I can be anything you want me to be.
But first, I need your private keys...
REALITIES
BLOCKS & CHAINS

BLOCK

a container of data

CHAIN

connects containers of data

BLOCKCHAINS: “Recordbooks of transactions”
LEDGERS: “Many recordbooks of transactions”
**FACT:** The more nodes you have in a crypto network, the weaker the network becomes. Why? Because with more nodes, you get further and further away from provable collisions. Collisioning is used to substantiate and support the majority of network transactions.
THE ‘SHAs’

+ SHA-1 limited attribution & collisioning
+ SHA-2 improved staking & consensus
+ SHA-3 (keccak) multiple attribution, no need for mining

SH1 vs SHA 256
Ethereum’s version “Ethash” uses various seed sizes to generate a 1GB block through padding, absorbing & then squeezing hash combinations. It produces large hashes through key stretching which makes the network slow.

Larger bit configurations can produce more optimal hash versioning, but they still make the network slow.
CRYPTO NETWORKS

trust(less) issues

throttled transaction speeds

poor node configuration
Hacking is not only about stealing or breaching, but patterning and simulating.

**CRYPTOHACKING**

- Bitcoin compromises
- Blockchain compromises
- Network compromises

- Routing theft of wallets
- Canvassing of networks
- Node infiltration
SECURITY & SCALE

Y axis = Security (theoretical)
X axis = Scalability
MATH MATTERS

- advanced hashing
- elliptical curve inversion
- super prime factoring

For every positive natural number, \( f \) is defined as the string:
\[
\langle \langle f \rangle \rangle = \text{Hash}\left( f \text{'}s text \right)
\]
where \( f \) is the \( f \text{'s text} \). Note that being able to test if two nodes within this representation are connected involves use of the sub-tree isomorphism problem, a problem whose complexity is known to be polynomial.

In the example above the two core trees, with their extra markers, are represented using parenthesis as shown below. The tree tags used in this example are also shown below.

In the example above the two core trees, with their extra "childless-child" markers, are represented using the parenthesis shown below. The tree tags used in this example are also individually shown below.

\[\text{(t)} = \text{hash}\]

<table>
<thead>
<tr>
<th>Tree 1</th>
<th>Tree 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash 1</td>
<td>((( )) )</td>
</tr>
<tr>
<td>Hash 2</td>
<td>((( )) )</td>
</tr>
<tr>
<td>Hash 3</td>
<td>((( )) )</td>
</tr>
<tr>
<td>Hash 4</td>
<td>((( X ) ) )</td>
</tr>
<tr>
<td>Hash 5</td>
<td>((( )) )</td>
</tr>
</tbody>
</table>

Converting these expressions into a total number of bits:

<table>
<thead>
<tr>
<th>Tree 1 with no tags</th>
<th>Tree 2 with no tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 nodes (2x) with extra markers (2x)</td>
<td>9 nodes (2x) with extra markers (2x)</td>
</tr>
</tbody>
</table>

36 bits

32 bits

Each tag is counted twice to represent both sides of the tagged occurrences:

<table>
<thead>
<tr>
<th>Hash 1</th>
<th>Hash 2</th>
<th>Hash 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 nodes (2x), two occurrences (2x)</td>
<td>4 nodes (2x), two occurrences (2x)</td>
<td>5 nodes (2x), two occurrences (2x)</td>
</tr>
<tr>
<td>3²2²</td>
<td>4²2²</td>
<td>5²2²</td>
</tr>
</tbody>
</table>

12 bits

16 bits

20 bits
QUANTUM RESISTANCE

BITS

0

1

QBIT

‘0’

‘1’

RESISTANT

‘0’ + ‘1’

(superpositional)

(interpositional)
SUPER PRIME FACTORING

(starting point to get to root prime values or “super primes”)

\[ 2^{511.5} \]

511 is a **deficient number** - a natural number that is strictly larger than the sum of its proper divisors.

\[ 7 \times 73 \]

1, 7, 73, 511

\[ 1 + 7 + 73 = 81 \]

\[ 2^{555} = 511 \times 5 \]

(number of linear operations required in a preimage or “meet in the middle” attack on SHA-256)

\[ 7 \times 73 \]

1, 7, 73, 511

\[ 261 \]

121

\[ 2^{555} = 511 \times 5 \]

(non-linear prime factors as pairs)

*511 is a multiple of itself, therefore it is relatively easy to get to zero*
HOLONOMIAL HASHING

**Smart Strings** are a 1 bit succinct binary representation of both natural numbers and natural numbers and natural labeled trees.

- parallel computability
- exponential scalability
- adaptive storage capacity
THE IDENTITY CHALLENGE

- SSI issues (zero knowledge proofing)
  solution: node authentication
- Biometric issues (Pii data)
  solution: authentication libraries
- Storage issues (replicant databases)
  solution: autonomous decrypt nodes
ALTERNATIVE APPROACHES

- agent-centric models
- distributed mesh networks
- focused development hubs

Figure. User 1 validates transactions between Users 2 and 3 WITHOUT knowing any decrypted information about the details of the transaction.
Right now, in most western economies, we are experiencing hyperinflationary conditions. This means the prices of goods and services can rise more than 50% a month. It also means that the purchasing power of money typically lessens as prices fluctuate. In other words, cash is available through quantitative easing to invest in things, and spend on things, yet there are less assets, or alternatives, to choose from.
Detach the word ‘security’ or ‘token’ or ‘commodity’ or ‘digital asset’ from a cryptocurrency for a moment and we can consider an evolutionary concept:

non-flationary value

**Inflation**
occurs when the price of products and/or services spike, while the purchasing power of money decreases.

**Deflation**
occurs when there is a general reduction of prices in the economy.
Non-flation can occur when supply and demand dynamics are combined with managed purchasing power such that price fluctuations are balanced out by assets (resources) people can use and recreate on their own.
MIXED MONETARY LOGIC

**fiat**
- monocultural
- single unit of account
- inflationary

**crypto**
- monocultural
- singular value
- disinflationary

**assets**
- polycultural
- value variant
- multiflationary
ASSET STABILIZATION

Real, physical assets (like natural resources) are the greatest hedge against inflationary risk.

full ecosystem representation

full data representation
ALTERNATIVE ASSET DEMAND YIELD

- **leveling demand**
- **value stabilization**
- **value regeneration**
- **ASSET FULCRUM** (origination)
- **(volatility)**
- **(reinvestment)**
- **(tax revenue)**
- **labor force stabilization**
- **labor force initiation**
- **ASSET THRESHOLD**
- **D** (increasing demand)
- **D2**
- **Q***
- **Q**
- **P***
- **P**

**Price** vs **Quantity**
DIGITIZING STABLE ASSET VALUE

real assets, real utility

real estate + land development

collateralized debt
mini-perms
equity prefs
clawbacks

regenerative asset creation + I.P.
convertibles
equity prefs
clawbacks
buyouts
bond vehicles

TIER 1

managed growth
horizontal scale

TIER 2

real-time risk amortization

TIER 3

licensing & shared asset pools
cryptoequities
cryptocurrencies
crypto securities
elastic bonds
co-licensing
fairshare notes
asset transfers

ASSET THRESHOLDS

(caps-outs)

horizontal scale

managed growth

real-time risk amortization

real assets, real utility

TIER 2

regenerative asset creation + I.P.
convertibles
equity prefs
clawbacks
buyouts
bond vehicles

TIER 1

real estate + land development

collateralized debt
mini-perms
equity prefs
clawbacks

TIER 3

licensing & shared asset pools
cryptoequities
cryptocurrencies
crypto securities
elastic bonds
co-licensing
fairshare notes
asset transfers

ASSET THRESHOLDS

(caps-outs)

horizontal scale

managed growth

real-time risk amortization

real assets, real utility
REAL BLOCKCHAIN ECOSYSTEMS

SMART ECOLOGIES + MAGIC CITY
a regenerative economic platform (co-design & advisory)

A blockchain-based trust and reputation system will be designed to manage, share and build incentives to reward all participants.

The Magic City project is a 17.7 acre, $1.5B true mixed use, low to zero footprint and regenerative real estate development that will play host to a health and wellness center, an event center, pop-up shops, and interactive parks. With the Smart Ecologies approach, we will include a science wing, a technology wing, as well as vertical farming and renewable technology components that are all on-site. The project is being developed within one of Dade County’s most promising neighborhoods, with the intention of greatly improving employment rates while maintaining affordability.

More comprehensive planning will enlist the local community through unique on-boarding processes via holistic experience design, co-develop applied agricultural + emerging technology skills, co-design open curricula, and create new jobs. Partnerships with the likes of Holo, Schneider, Siemens and Google will catalyze tenancy and as integrated partners they can build their own presence to test products actively with local segments and cross-country cohorts.
ADAPTIVE GOVERNANCE
REGENERATING INVESTMENT
GLOBAL CURRENCY STACK

- **digital sovereigns** (treasury-backed)
- **complementary digital (crypto)currencies** (asset-backed)
- **collateralized digital stores of value** (network-backed)
TAKEAWAYS

Blockchains & distributed ledgers are only as good as their real world uses. Anything built on the current Internet infrastructure is hackable. A better economic system requires different logic.
Thank you.

https://www.novena.tech/