



Blockchain, Cryptocurrency and the Achilles Heel in Software Developments

Justin Y. Shi | shi@temple.edu

January 2022



Outline

- Money and Cryptocurrencies
- Web 3.0 and the Achilles Heel in computational software infrastructures
- The blockchain protocol
- Public and private (permission-based) chains
- The blockchain blues: scalability war - POW vs. POS
- Vulnerability in crypto-exchanges
- The need for crypto-infrastructure 2.0
- Summary

Money and Cryptocurrencies

Money



Money is any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts, such as taxes, in a particular country or socio-economic context. The main functions of money are distinguished as: a medium of exchange, a unit of account, a store of value and sometimes, a standard of deferred payment. Any item or verifiable record that fulfils these functions can be considered as money.

[money | Definition, Economics, History, Types, & Facts | Britannica](#)

Fraud, Inflation and Economic Freedom

- More money supplies give higher inflation pressure
- Financial crisis breeds growing distrust of central banks: 2008 sub-prime mortgage crisis gave birth of the political [Tea Party](#) and the blockchain protocol by [Satoshi Nakamoto](#).

US National Debt Clock

- [U.S. National Debt Clock : Real Time \(usdebtclock.org\)](https://usdebtclock.org)
- Every child born in US already owes over **\$61,000** portion of the national debt.

Outline

- Money and Cryptocurrencies
- **Web 3.0 and the Achilles Heel in legacy software infrastructures**
- The blockchain protocol
- Public and private (permission-based) chains
- The blockchain blues: scalability war - POW vs. POS
- Vulnerability in crypto-exchanges
- The need for crypto-infrastructure 2.0
- Summary

Cryptocurrencies, NFT and Web3.0

- The blockchain protocol delivered traditional database could not: a) Fault tolerant zero downtime, zero loss, b) Decentralized, c) Ledger immutability.
- Anyone can start a cryptocurrency to store values if there are enough people who believe in the value.
- NFT(Non-fungible Token) is a generalization of crypto-value store idea for unique valuable objects in the world. It attracted many applications and gamer [protests](#) as well.
- Decentralized computing is sometimes called [Web 3.0](#)

The Achilles Heel in Legacy Software Infrastructures

- Centralized authority (server).
- Scaling dilemma: expanding infrastructure must choose either performance or reliability.
- Single-point failure cannot be eliminated.
- Planned and unplanned downtimes are not preventable.
- Arbitrary data losses cannot be eliminated.
- The **Achilles Heel**: APIs assuming unrealistic network and processor reliabilities: **MPI, RPC, RMI, ...**

What is Wrong with Legacy APIs?

- **RPC**: Remote procedure call-> depends on a procedure running on a remote computer that may not be there in time.
- **MPI**: Send or Recv -> depends on a remote partner to receive or send messages.
- ...
- The client has no retransmission discipline. Everything is one-shot deal.

Outline

- Money and Cryptocurrencies
- Web 3.0 and the Achilles Heel in legacy software infrastructures
- **The blockchain protocol**
- Public and private (permission-based) chains
- The blockchain blues: scalability war - POW vs. POS
- Vulnerability in crypto-exchanges
- The need for crypto-infrastructure 2.0
- Summary

Digital Currency and Anti-Spam Research

Challenge:

How can an email server avoid forwarding spam messages?

Solution:

1. Make the requester to solve a hard puzzle for messages to be forwarded.
2. If the puzzle is too hard and the messages are few, the residual value can be saved for future use (digital currency original form).

How to Avoid Double Spending?

Solution:

1. A sequential chain of transactions that each must be validated by the majority of the validators.
2. The validation process must be slow enough (~ 10 min) making double spending of the same balance practically impossible even if **the network partitions**. The validation difficulty will increase if the validators work too fast.
3. For transactions of \$1M or more USD, current industry standard requires 6 confirmations before committing the transaction to the chain (for a total about 60 min).

How to Avoid Centralized Authority?

- Any computer can become a validator by joining the network of transaction chains.
- Each validator will hold the entire ledger of all transactions from the genesis day.
- Winning validator: the first one to complete the validation process will be compensated. The very first block compensation is 50 BTC. This number halves approximately every four years (210,000 transactions). Since May 2020, 6.25 Bitcoins per block mined. It will hit zero in 2140.

Immutability

- For security, once the transaction is committed to the chain, it should not be possible to alter it.
- Every node holds the entire ledger of all transactions since the genesis day. Thus, data in bigger networks are safer.
- The Bitcoin network, or any other cryptocurrency network, should operate 24/7 regardless network and computer crashes.

Q: What if solar winds shutdown half world's computers at the same time?

A: Your ledger will still be fine.

HOW DOES BLOCKCHAIN WORK?



1



Request

A transaction is requested.

2



The transaction is then shared with other people in the network.

3



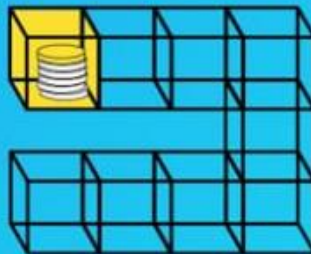
Those in the network must verify the transaction.

4



Once the transaction is verified, it's added to a block with other transactions.

5



That block is added to a chain of previously verified blocks.

6



Then it is broadcast to all nodes to do the same

Why is Blockchain so Special?

Everything: Immutability, data resilience, decentralized processing without central server, zero single-point failure, zero downtime, zero data loss.

Checkpoint: No database today could promise transaction immutability and permanency regardless network and computer crashes.

Why Fault Tolerant Computing Hard?

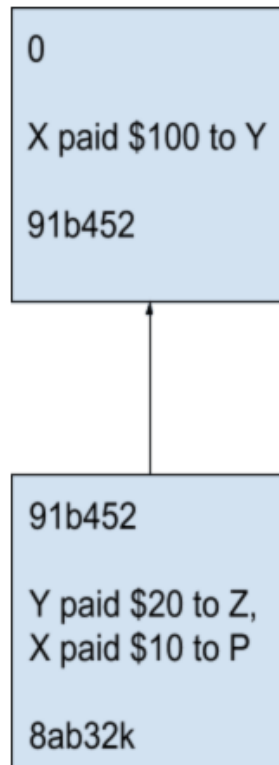
Because all legacy programming paradigms assume reliable computers and networks: Message Passing Interface (MPI), Remote Procedural Call (RPC), Remote Method Invocation (RMI), shared memory (OpenMP), Memory-Mapped files, named pipe, semaphore, signal, Actor, Scala, Concurrent ML, AppleScript, event loop, Erlang, Go, Objective-C, Rust, Smalltalk, HyperCard/LiveCode, Rust, ...

How to Program Blockchain?

- Y paid \$20 to Z
- X paid \$10 to P

Finally, we have the `hash_itself` value which is basically `Hash("Y paid $20 to Z, X paid $10 to P", 91b452)`. This turns out to be `8ab32k`.

Representing pictographically, our Blockchain looks like the following:



What's so special about this "data structure"?

Did You See IP Addresses?

- .No.

- .There is no assumption on the computer or network reliabilities.

- .The protocol is strong enough to recover from the extreme failure cases.

Outline

- Money and Cryptocurrencies
- Web 3.0 and the Achilles Heel in legacy software infrastructures
- The blockchain protocol
- **Public and private (permission-based) chains**
- The blockchain blues: scalability war - POW vs. POS
- Vulnerability in crypto-exchanges
- The need for crypto-infrastructure 2.0
- Summary

Public Chains

- There are more than a thousand cryptocurrencies:
<https://www.coinbase.com/browse>
- Not all are public chains.
- Public chains: Bitcoin, Ethereum, ...
- Any computer with a network connection can become a full node.
- POW (proof of work) is required to validate transactions and receiving rewards [10 min/block:
 $50 \text{ BTC} \times 6 \times 24 \times 365 \times 4 (1 + 1/2 + (1/2)^2 + (1/2)^3 + \dots) \sim 21,000,000 \text{ BTC}$.
- Once BTC supplies are exhausted, users must pay transaction fees to the miners.

Private Chains

- Private chains are permission-based. They only accept authorized nodes (centrally controlled).
- Dedicated servers. Transaction processing speed is faster than public chain.
- At least 7 nodes are required to offset Byzantine attacks.
- Data will only be lost if all nodes crash at the same time.
- Banks prefer private chains.

Outline

- Money and Cryptocurrencies
- Web 3.0 and the Achilles Heel in legacy software infrastructures
- The blockchain protocol
- Public and private (permission-based) chains
- **The blockchain blues: scalability war - POW vs. POS**
- Vulnerability in crypto-exchanges
- The need for crypto-infrastructure 2.0
- Summary

Regulatory Challenges

- Governments are generally hostile to cryptocurrencies, except for small countries that local currencies are crashed: El Salvador.
- My prediction: Cryptocurrencies will persist regardless governments' efforts to shut them down.

Blockchain Scaling Challenges

- Public Chain:

- Growing energy waste. Only a small number of miners are required for transaction security. Most miners are working blindly.

- Growing ledger will eventually shutdown the entire chain since every node must hold the entire ledger.

Private Chain Scalability Challenges

- Each node must hold entire ledger.
- Adding nodes will slow down transaction processing speed.

Outline

- Money and Cryptocurrencies
- Web 3.0 and the Achilles Heel in legacy software infrastructures
- The blockchain protocol
- Public and private (permission-based) chains
- **The blockchain blues: scalability war - POW vs. POS**
- **Vulnerability in crypto-exchanges**
- The need for crypto-infrastructure 2.0
- Summary

The Scalability War

- POW (Proof of Work) by solving a difficult hash rate problem.
- POS (Proof of State) by each miner posting an “stake” balance before validating transactions. Random selection of approving committee. Resolve the committee after each block. Faster than POW.
- Penalty for off-line and for mining a bad block.
- Still experimental. Only Cardano offers POS in production.

Ledger Partition

- The current Bitcoin ledger size is about 350GB from the genesis day.
- It grows about 10GB per month.
- The ledger will eventually crash all if ledger is not partitioned.
- Ethereum 2.0 has ledger sharding planned (expected 2023).

Crypto-Exchange Vulnerabilities

- Crypto exchanges are typically powered by legacy database servers.
- Their vulnerabilities are well known. (FBI's intercept of Colonial Pipeline's Ransome ware payments)
- Legacy software scalability challenges are embarrassing.

Outline

- Money and Cryptocurrencies
- Web 3.0 and the Achilles Heel in legacy software infrastructures
- The blockchain protocol
- Public and private (permission-based) chains
- The blockchain blues: scalability war - POW vs. POS
- Vulnerability in crypto-exchanges
- **The need for crypto-infrastructure 2.0**
- Summary

Understand Scalability

- Scalability seems to have many definitions in different communities: performance, resilience, infrastructure size, capital spending, ...
- This one makes the most sense:

A **scalable service** = expanding its processing infrastructure will enhance the service performance, reliability and security at the **same time**.

Is Scalable Service Possible?

- Scientifically, YES.
- The Internet is a living example.
- All man-made structures will fail if over-sized.
The internet does not have problem. Why?

Current Fin Tech Affaires

Confidence in **fiat money** is **dwindling**.

Interests in digital cryptocurrencies are **sweeping** the world.

Retail banks still employ **transaction auditors**.

Planned and unplanned service **downtimes** are growing as infrastructure expands.

Sarbanes-Oxley's Act (SOX, 2002) triggered **asynchronously replicated DR** sites.

Transaction losses are covered by legal clauses as “cost of doing business”.

Almost every major bank has a research project on **crypto currency** or decided to build internal chains and accept cryptocurrencies.

Cryptocurrency “gate keepers” (**exchanges**) still suffer service downtimes and service losses (Coinbase, Binance, etc.)

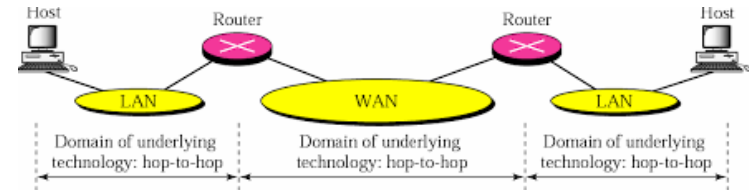
Common Technology Difficulties

How to eliminate data losses?

How to add strong encryption/decryption without performance penalty?

How to scale infrastructure for better performance without reliability degradation?

Lessons from the Past



1983: MIT failed experiment -> End-to-End Arguments in System Designs: <https://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf>

1993: The Impossibility of Implementing Reliable Communication in the Face of Crashes: <https://groups.csail.mit.edu/tds/papers/Lynch/jacm93.pdf>

2013: OSI: The Internet that wasn't: <https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt>

Subtitle: How TCP/IP eclipsed OSI to become the global protocol for computer networking

2000: Brewer's CAP (Consistency, Availability, network Partition tolerance) conjecture): <https://dl.acm.org/doi/10.1145/564585.564601>

2002: CAP Theorem (ACM Digital Library: <https://dl.acm.org/doi/10.1145/564585.564601> , Seth Gilbert and Nancy Lynch)

What Has Blockchain Done?

Proved massive **synchronous transaction replication** (general ledger) is practically feasible. (2021: **68.42m** blockchain wallet users, each wallet is replicated 14,000+ times)

Proved **zero transaction loss** is practically feasible. Even though no statistician would agree that 100% reliable ledger is possible.

Lessons Learned

Blockchain is an end-to-end protocol implemented using TCP/IP.

Hop-to-hop protocols (TCP/IP) is only good enough for streaming services (Netflix, Youtube, web searches), but **NOT good enough** for transactional and mission critical services.

Arbitrarily reliable systems are practically feasible.

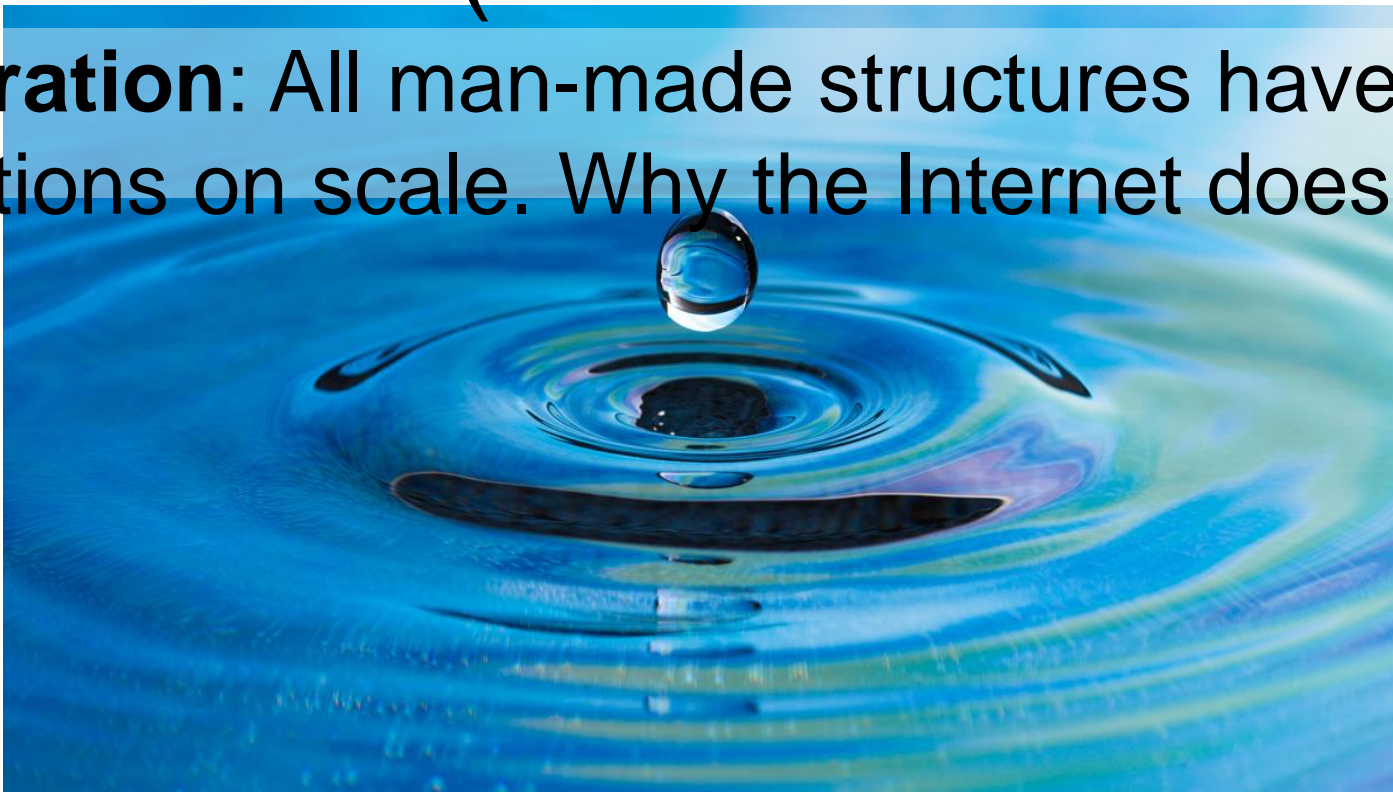
Even with the blockchain protocol, scalable performance is still **elusive**.

Well-Known Impossibilities

- .The Impossibility of Implementing Reliable Communication in the Face of Crashes (Alan Fekete, Nancy Lynch, Yishay Mansour, and John Spenelli, 1993, JACM)
- .Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services, (Seth Gilbert, Nancy Lynch, 2002, ACM SIGACT News (CAP Theorem))

The Internet's Fons Juventae(Fountain of Youth)

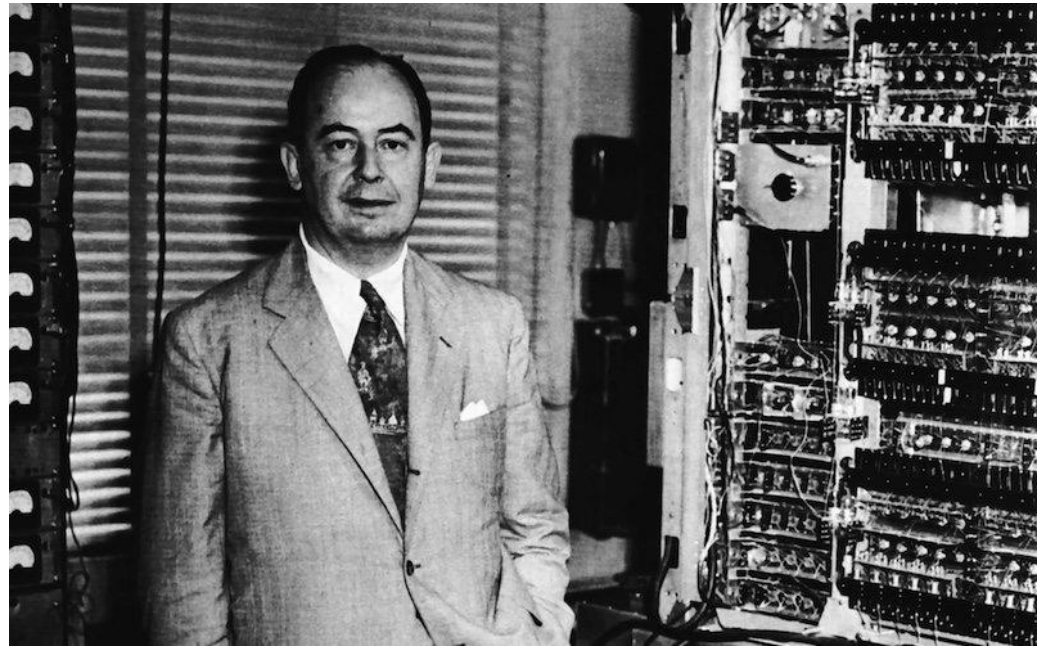
Inspiration: All man-made structures have limitations on scale. Why the Internet doesn't?



It was Written in 1952

The Internet “DNA”
code was written by
von Neumann in
1952:

[https://www.peliti.org/
Notes/vonNeumannN
ew.pdf](https://www.peliti.org/Notes/vonNeumannNew.pdf)



Statistic Multiplexing

All Rights Reserved (c)2021-2022, Justin Y. Shi

Revelations

The standard **hop-to-hop APIs are fundamentally flawed** for scaling.

Service performance and reliability actually rely on the **same technology** challenge: How to enable all resources (processing, storage, network) be always exploited?

Technically Speaking

All services are delivered via APIs (application programming interfaces). What API (and **runtime**) would enable full resource statistic multiplexing automatically?

Three Challenges:

- How to program without assuming device reliability? (blockchain, bittorrent)
- How to enable all resources be exploited automatically? (?)
- How to convert legacy systems for the business communities? (?)

Top Programming Fallacy

Network is Reliable

Research Updates

Service performance and reliability are the **same function** when performance = 0 is the failure.

To avoid the scaling traps using the hop-to-hop APIs, **Active Content Addressable Networking** was introduced (patent pending).

Statistic Multiplexed Computing (SMC) was introduced to enable performance harvesting in arbitrary scales (patent pending).

Performance is unconstrained if the problem size is open: **Amdahl's Law**.

For fixed size services, the economic law of “diminishing return” must be followed.

Reliability can be arbitrarily high (practically zero-loss).

Security can **be arbitrarily strong** without performance drawbacks.

A Peek into the Future

- Active Content Addressable Networking to enable IP-address-less communication.
- ACAN runtime kernel for statistic multiplexing resources.
- Elimination of programming fallacy by including the timeout/retransmission protocol in all client programs.
- Infinitely scalable (adding a processor, a network connection can enhance the application's performance and reliability at the same time)

Q: What about the law of “diminishing return”?

The Quantum Computer Connection



IBM's 51 qbit Quantum Computer

vs.



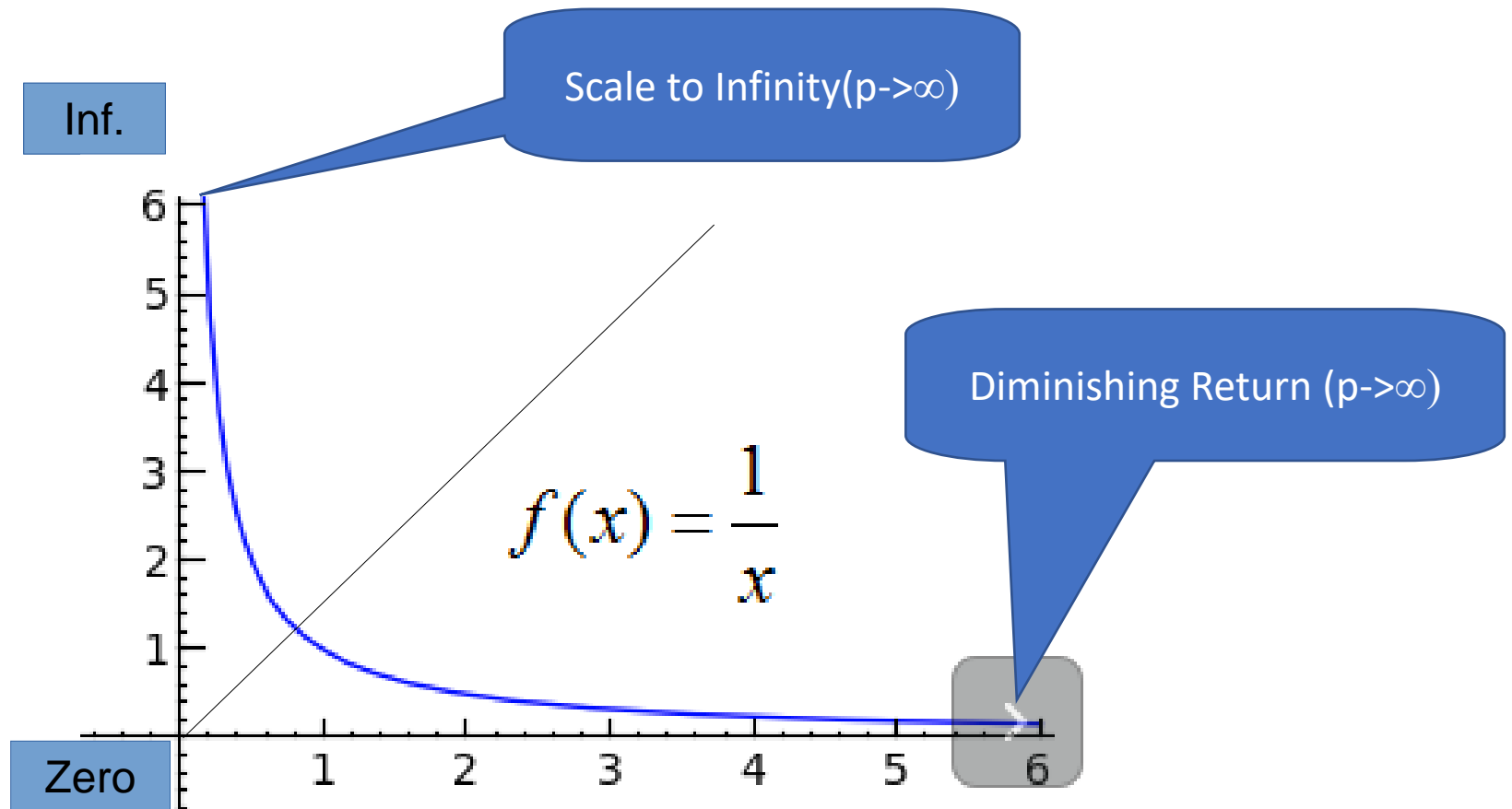
$$\text{Speedup}(p \uparrow) = \frac{1}{s \downarrow}$$

Amdahl's Law: Percentage of serial work

Amdahl's Law

- Let x = percentage of serial codes, the speedup of any parallel application is above bounded to $S_p\{p \rightarrow \infty\} = 1/x$, where p = number of parallel processors.
- If the application problem size is fixed, then the law of “diminishing return” applies.
- If the application problem size is open, then infinite scaling is possible.

What is in the 1/x Curve?



Fin Tech and Cyberinfrastructure

Inter-dependent

Mission critical







Zero-loss feasible

Unlimited performance feasible

Unlimited security feasible



Web 3.0 Ready

| WEB 2.0 | | WEB 3.0 |
|---|---|---|
| Criteria | Web 2.0 | Web 3.0 |
|  Definition | The second generation of internet services focused on interaction. | The third generation of the internet focused on decentralization and semantic learning. |
|  Focus | The focus is primarily on community development. | The focus is on empowering individual users. |
|  Technologies | <ul style="list-style-type: none">• AJAX• JavaScript• HTML5• CSS3 | <ul style="list-style-type: none">• Artificial intelligence• Machine learning• Decentralized protocols |
|  Types of Applications | Web applications | Smart applications based on AI and ML |
|  State of Data | The network owns the data | Entities have ownership over the data and its sharing and use |
|  Features | <ul style="list-style-type: none">• Improved interaction• Introduction of web applications | <ul style="list-style-type: none">• Smart, web-based applications and functionalities• The better blend of web technology and knowledge representation |

CREATED BY 101BLOCKCHAINS.COM

About the Speaker

Justin Y. Shi earned his MS and PhD from University of Pennsylvania. He joined the CIS Department of Temple University in 1985. He was the elected and appointed Chairman of the CIS Department from 2007-2009, Associate Chairman 2010-2015. His research focused on mission critical computing infrastructures for high performance data intensive applications. He was awarded multiple patents on stateless computing architecture and lossless transaction processing technology. His new inventions include mission critical active content addressable network and statistic multiplexed computing technology applied to data intensive systems include blockchains, databases, file systems and object stores for financial transaction processing and controllers in deep space probes, unmanned vehicles, nuclear power plants, software defined networks, and smart grids.

