

Blockchain - Present Status and (Possible) Future

Bebo White



SLAC National Accelerator Laboratory/
Stanford University



bebo@slac.stanford.edu



This work is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States
See <http://creativecommons.org/licenses/by-nc-sa/3.0/us/> for details

Perhaps the lasting disruptive
legacy of the cybercurrency
discussion is blockchain



Caveats

- I am fascinated by the mathematics and technology behind the blockchain so may be willing to overlook some of its issues
- I find the state of blockchain technology as exciting as the early days of WWW
- my experience with the blockchain lies primarily in cryptocurrencies
- SLAC has no official projects based on blockchain technology, but *I am trying...*

What is the Blockchain?

(1/3)

- a distributed database/ledger that provides an unalterable, (semi-) public record of digital transactions;
- each block aggregates a timestamped batch of transactions to be included in the ledger (blockchain);
- each block is identified by a cryptographic signature;

What is the Blockchain?

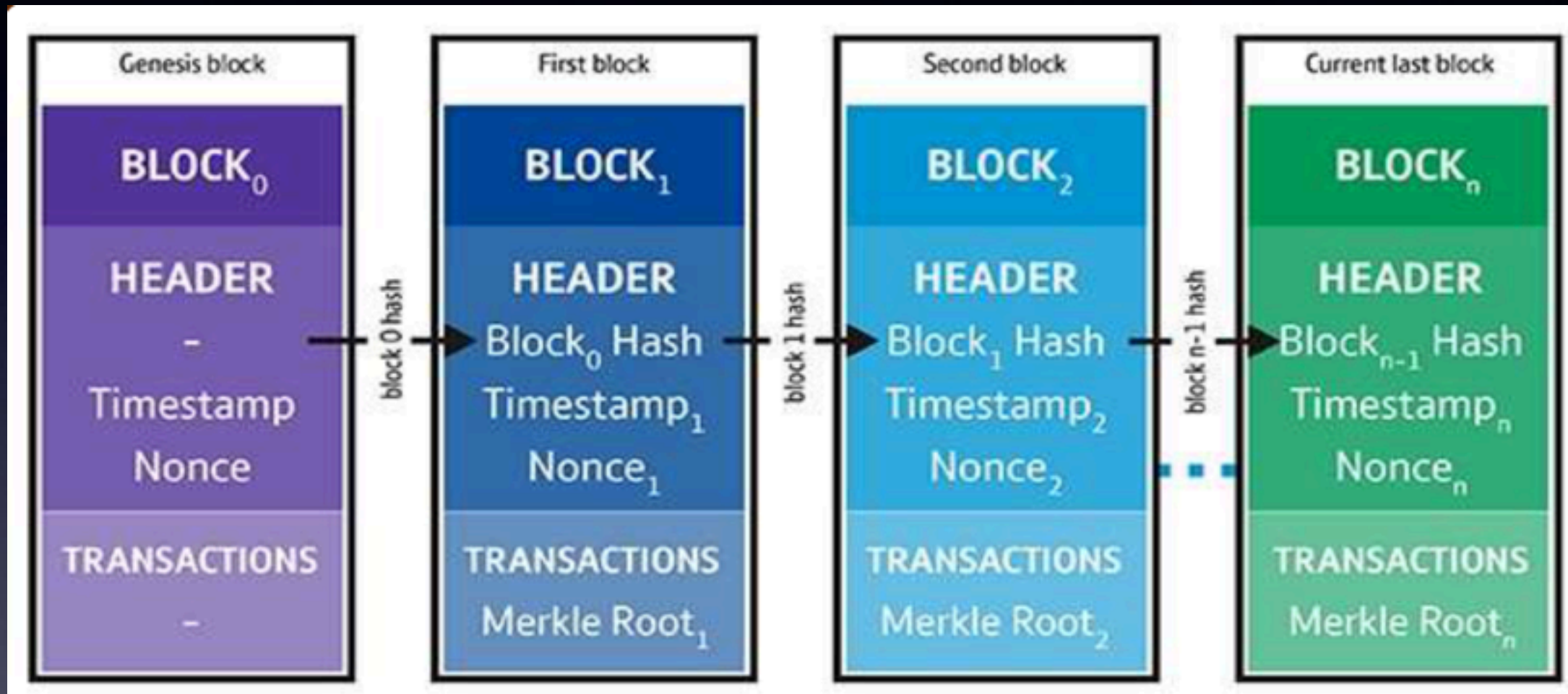
(2/3)

- blocks are all back-linked, i.e., they reference the signature of the previous block in the chain (kind of like a linked list);
- that chain can be traced all the way back to the very first block created;
- this provides an un-editable (compromised) record of all transactions made;
- the chain can be controlled by any single entity;
- the chain has no single point of failure.

What is the Blockchain?

(3/3)

- most importantly (perhaps) - it is very hard to add blocks to the blockchain e.g., bitcoin mining
- its strengths are in
 - distribution
 - technical robustness
 - lifespan
 - non-modifiability
 - unquestionable provenance



Why Blockchain?

- just because we can, should we?
- “The idea that everyone (and their descendants) has to have a copy of THE ledger of all transactions in the universe (now and future) has always smelled fishy to me”
- the idea that people could have computers in their homes...
- the idea that people have all the world's knowledge at their fingertips...

“Blockchain? - the equivalent of being
the first to figure out that peanut
butter and chocolate go well together”
-Jeff Flowers

A blockchain is “a technology that allows people who don’t know each other to trust a shared record of events”
- Bank of England

BLOCKCHAIN

WALLET

DATA

API

ABOUT

Q

BLOCK, HASH, TRANSACTION, ETC...

GET A FREE WALLET

LATEST BLOCKS

SEE MORE →

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (KWU)
491063	7 minutes	1749	8,079.26 BTC	ArtPool	1052.11	
491065	10 minutes	2051	11,074.44 BTC	ViaBTC	1,100.04	3,992.05
491064	35 minutes	251	5,795.55 BTC	ArtPool	1,007.32	3,996.74
491063	36 minutes	371	887.48 BTC	BTC.com	1,014.21	3,992.93

NEW TO DIGITAL CURRENCIES?

Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.

[BUY BITCOIN →](#)
[LEARN MORE →](#)
[GET A FREE WALLET →](#)

SEARCH

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Q

13FdATdYGGnWWPwt7URgi24LbFGWMT9JvM

Search

https://blockchain.info

Does this mean that I have only done one bitcoin transaction ever?

BLOCKCHAIN

WALLET

DATA

API

ABOUT

Q

BLOCK, HASH, TRANSACTION, ETC...

GET A FREE WALLET

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary

Address

13FdATdYGGnWWPwt7URgi24LbFGWMT9JvM

Hash 160

18b443307eb1eac9d2289462a3c6f80b4fd66e47

Tools

Related Tags - Unspent Outputs

Transactions

No. Transactions

1

Total Received

0.002861 BTC

Final Balance

0.002861 BTC

Request Payment


Donation Button

Transactions (Oldest First)

Filter ▾

2c6526e0609f16da5fd99e52ca7b6de80b6812b0a5d9c67468bd8967672		2017-01-03 09:52:51
1HDAQczS8z2FY999KjaunyBFXhPXuHPQ5f	→	<div>1NkAApcnzMzrEqZD2UTK4o3SdM5PrGYt1H</div> <div>13FdATdYGGnWWPwt7URgi24LbFGWMT9JvM</div> <div>0.098039 BTC</div> <div>0.002861 BTC</div> <div>0.002861 BTC</div>

STU, April 2018



Director's Fellow
MIT Media Lab

MIT Has Started Issuing Diplomas Using Blockchain Technology

Blockchain technology is proving to offer major advantages beyond its well-known applications in the sphere of cryptocurrency. A new app allows MIT graduates to prove ownership of their degree using the digital ledger.

DIGITAL DIPLOMA WITH BLOCKCHAIN

Since the school's inception, the Massachusetts Institute of Technology has issued paper diplomas to over 200,000 students. This summer, a pilot program saw 111

SHARE

WRITTEN BY
Brad Jones

Revised: 10/20/17

#Blockchain #Diploma #LearningMachine #MIT

Blockcerts Wallet
By Learning Machine
Open iTunes to buy and download apps.

Description
Blockcerts is a mobile app for people to easily create and share official records signed and independently verified using the blockchain.

Blockcerts Wallet Support

What's New in Version 2.0.3
* Fixed a bug where v2 Blockcerts might not verify correctly
* Added additional domains for external links to open in-app

iPhone Screenshots

Own your official records with a secure passphrase

Receive records multiple issuing organizations

Verify

Suppose your family history, personal preferences, etc. was on a blockchain?

- you would control
 - content
 - credibility
 - visibility
- would identity theft be a problem or would this be a true online identity?
- could I use my personal information bits like coins/tokens of value?
- to the first order this appears to be a compelling concept

A Critical Look at Decentralized Personal Data Architectures

Arvind Narayanan
nar@cs.stanford.edu

Solon Barocas
solon@nyu.edu

Vincent Toubiana
vincent.toubiana@icrystal-incident.com

Helen Nissenbaum
helen@nyu.edu

Dan Boneh
dabo@cs.stanford.edu

February 20, 2012

ABSTRACT

While the Internet was conceived as a decentralized network, the most widely used web applications today tend toward centralization. Control increasingly rests with centralized service providers who, as a consequence, have also amassed unprecedented amounts of data about the behaviors and personalities of individuals.

Developers, regulators, and consumer advocates have looked to alternative decentralized architectures as the natural response to threats posed by these centralized services. The result has been a great variety of solutions that include personal data stores (PDS), infomediaries, Vendor Relationship Management (VRM) systems, and federated and distributed social networks. And yet, for all these efforts, decentralized personal data architectures have seen little adoption.

This position paper attempts to account for these failures, challenging the accepted wisdom in the web community on the feasibility and desirability of these approaches. We start with a historical discussion of the development of various categories of decentralized personal data architectures. Then we survey the main ideas to illustrate the common themes among these efforts. We tease apart the design characteristics of these systems from the social values that they (are intended to) promote. We use this understanding to point out numerous drawbacks of the decentralization paradigm, some inherent and others incidental. We end with recommendations for designers of these systems for working towards goals that are achievable, but perhaps more limited in scope and ambition.

1. BRIEF HISTORICAL OVERVIEW

The search for alternatives to centralized aggregation of personal data began in the late 1990s which saw a wave of so-called ‘negotiated privacy techniques’ including commercial ‘infomediaries’ [24, 16]. These entities would store consumers’ data and help facilitate the drafting of contracts that set the terms of the exchange and use of data. The 1999 book *Net Worth* [23] galvanized both industry and privacy advocates, generating hopes for a future in which privacy problems could be solved through a mix of decentralized storage and private contracts, potentially obviating the need for privacy law or even the adoption of fair information practices [10, 30].

Within five years, nearly all of this excitement had faded and all commercial (Persona, Privada, Lumeria, etc.) and community (P3P) initiatives had floundered [1] — some in truly spectacular fashion, such as AllAdvantage. And yet, by the end of the decade, many new initiatives and projects that shared almost identical goals emerged. Vendor Relationship Management (VRM) [35] has gained steady momentum as a general set of principles that aim simultaneously to improve user privacy, enhance customer autonomy, and increase market efficiency through a combination of mechanisms that aggregate data in a single (per-user) repository under users’ control and tools to negotiate agreements that would grant outside organizations access to and use of that data.

Parallel efforts to develop so-called personal data stores (PDS), personal data servers, personal data lockers/vaults, and personal clouds [18] have focused more narrowly on the platforms and protocols to support unified repositories of user data that could be managed locally by the user or outsourced to a trusted third party. The impetus for these projects are varied, ranging from user interest in aggregating one’s own data in a single location to better derive benefits from their mixing and matching to more explicit interests in privacy (user control) and commerce (a market place for sharing, including possibilities for cash payments in exchange for data) [13].

The similarities between these and earlier efforts can be quite stark: Mydex’s recent white paper, “The Case for Personal Information Empowerment” [28], recapitulates much that was described in a white paper released a full decade earlier by Lumeria, a failed infomediary [30]. To describe this as a simple case of “an idea whose time has come” would be to miss the important lessons that these earlier and recurring failures should offer those who wish to pursue decentralized personal data architectures.

Decentralized social networking has been a largely parallel, sometimes overlapping line of development with similar motivations. We subdivide such social networks into federated (ecosystem of interoperable implementations in the client-server model) and distributed (peer-to-peer). The term distributed social networking is frequently but incorrectly used to describe all decentralized social networks.

- technical disadvantages inherent to any decentralized system
 - computational limitations
 - susceptibility to network unreliability
 - slow network speed
 - redundant data that may or may not be synchronized
- lack of economies of scale to defray the costs of decentralized systems
- cognitive burden of people managing their own data and how likely it is for this to work reliably for long periods of time at scale
- the tendency of even decentralized systems to assume characteristics of centralized systems because people start using the same pathways

- what about as the EU rolls out the General Data Protection Regulation (GDPR)?
- regulators must take blockchain both seriously and literally as a technology
- “blockchains, as currently designed, are incompatible with the GDPR” (Michele Finck, Oxford)
- what is “personal information” - a person’s public blockchain address?
- in general, encrypted data is viewed as personal data, making much of the blockchain susceptible to GDPR regulation

- this may lead to redundant systems e.g., companies building traditional database systems to manage any personally identifiable information off a blockchain - does this defeat the blockchain benefit?
- blockchain address pseudonyms are only as secure as any system resolving them to real identities, which Web trackers, cookies, beacons, etc. can unmask rather simply
- this is a rich research area IMHO

by Giulio Prisco, Apr 05, 2018

Wireless Carriers Developing Blockchain-Based Identity Management Systems

f Facebook

🐦 Twitter

in LinkedIn

✉ Email



**A Case Study for Blockchain in Healthcare:
“MedRec” prototype for electronic health records and medical research data**

White Paper

Ariel Ekblaw*, Asaph Azaria*, John D. Halamka, MD†, Andrew Lippman*

*MIT Media Lab, †Beth Israel Deaconess Medical Center

August 2016

Note: The abstract and first three sections of this white paper are drawn from a peer-reviewed, formally accepted paper, presently being prepared for publication with IEEE through their Open & Big Data Conference, August 22-24, 2016.

MedRec: Using Blockchain for Medical Data Access and Permission Management

IEEE Original Authors: Asaph Azaria, Ariel Ekblaw, Thiago Vieira, Andrew Lippman

This material is adapted and included here with permission of the IEEE, including permission for publication by the ONC Blockchain Challenge if selected.

Could the Blockchain help to
address “fake news?”

What’s a viable model?

CADZ METZ BUSINESS 03.22.17 09:15 AM

FORGET BITCOIN. THE BLOCKCHAIN COULD REVEAL WHAT’S TRUE TODAY AND TOMORROW

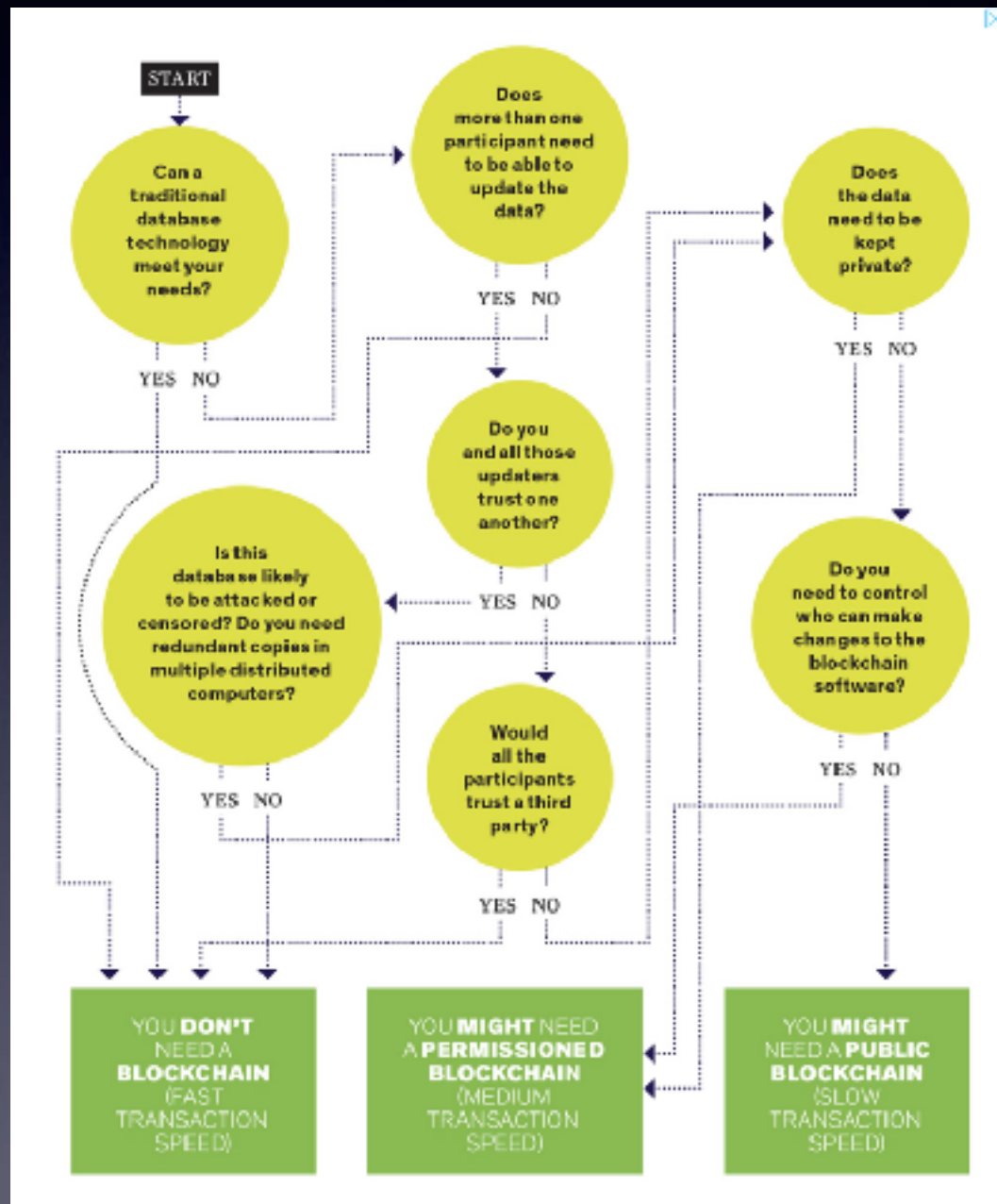


GETTY IMAGES

Back to empowerment and transparency

- “Diamond Blockchain”
- Slave labor goods
- Hernando DeSoto’s work on land titles

Is a Blockchain for you? - public or private?



Blockchain as a platform

- another geeky paper

- “Let’s make the blockchain programmable” - “a world computer”
- Ethereum specifications
- “a child of Bitcoin and BitTorrent”
- Ether is not just another coin
- Redefines mining/POW
- Quantifies “smart contracts”
- enables “cryptoeconomics”

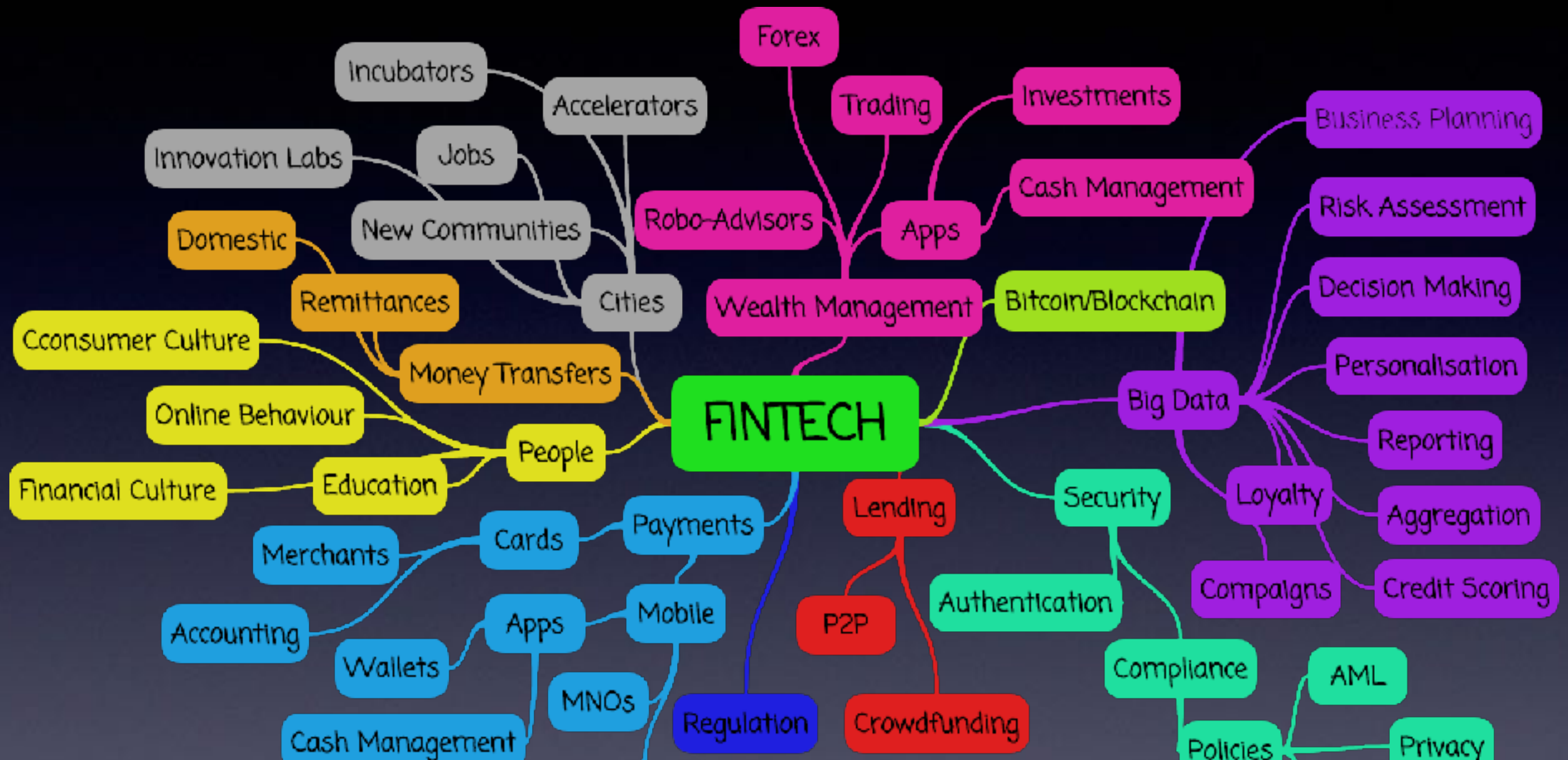


Ethereum White Paper
A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM
By Vitalik Buterin

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the “bitcoin”, a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the “bitcoin” as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi’s grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized digital currency. Satoshi’s blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin’s technology, and how the blockchain concept can be used for more than just money.

Commonly cited applications include using on-blockchain digital assets to represent custom currencies and financial instruments (“colored coins”), the ownership of an underlying physical device (“smart property”), non-fungible assets such as domain names (“Namecoin”) as well as more advanced applications such as decentralized exchange, financial derivatives, peer-to-peer gambling and on-blockchain identity and reputation systems. Another important area of inquiry is “smart contracts” - systems which automatically move digital assets according to arbitrary pre-specified rules. For example, one might have a treasury contract of the form “A can withdraw up to X currency units per day, B can withdraw up to Y per day, A and B together





“A compelling FinTech example is the potential for Blockchain technology to replace legacy post-trade processes that currently require trusted third parties such as clearinghouses and depositories to manage and administer the clearing, settlement, and custody associated with trades and payments”
—*Dhar & Stein, CACM, 10/2017*

Media > News

Blockchain Will Become ‘Beating Heart’ of the Global Financial System

Published

Friday 12 August 2016

Share



Peter Vanham, US Media Lead, Public Engagement, Tel.: +1 646 592 5907, E-mail: pvan@weforum.org

- Blockchain, the technology behind bitcoin could profoundly alter the way banks do business worldwide, lowering their operating costs and making financial services securer and more accessible, a World Economic Forum report finds

“Blockchain is the new quantum physics:
A really, really hard science that no one
understands, ambushed by clowns like
Deepak Chopra looking to make a quick
buck on solutionist nonsense”
——Chris DeRose (TED talk)

“Blockchain does nothing
but circumvent the rules
we have imposed on
banks to keep them honest”
——Izabella Kaminska (FT
Alphaville)

Cryptoeconomics

- The 3rd part of Satoshi's vision
- “past is provable, future is predictable”
- Uses cryptography to prove actions occurring in the past
- Predicts that economics can ensure that actions occur in the future

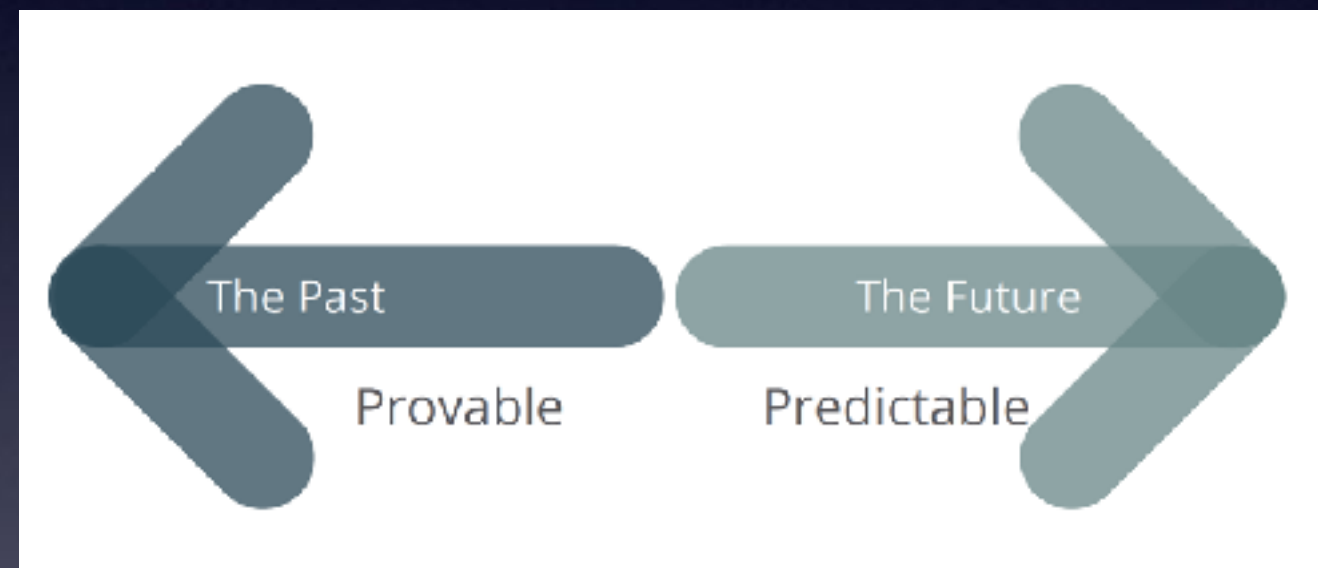


(Ref: Justin Poirier)



Cryptoeconomics - why does it work?

- Works because people trust math and people like money
- Establishes trust, even between pseudonymous parties
- Makes trust in a person or third party optional
- Reduces the cost of an intermediary to only the actual transaction cost (remember the UN example?)



(Ref: Justin Poirier)

Disintermediation

- Third parties are no longer needed to
 - establish identity or prove creditworthiness
 - distribute media
 - mediate communication between parties
 - mediate transfers of value

SingularityHub

Singularity University SingularityU Global

TOPICS IN FOCUS EXPERTS EVENTS VIDEOS

Experts

Blockchain Will Be the Foundation of Trust in the Metaverse

By Aaron Frank · Oct 17, 2017 · 4562

▼

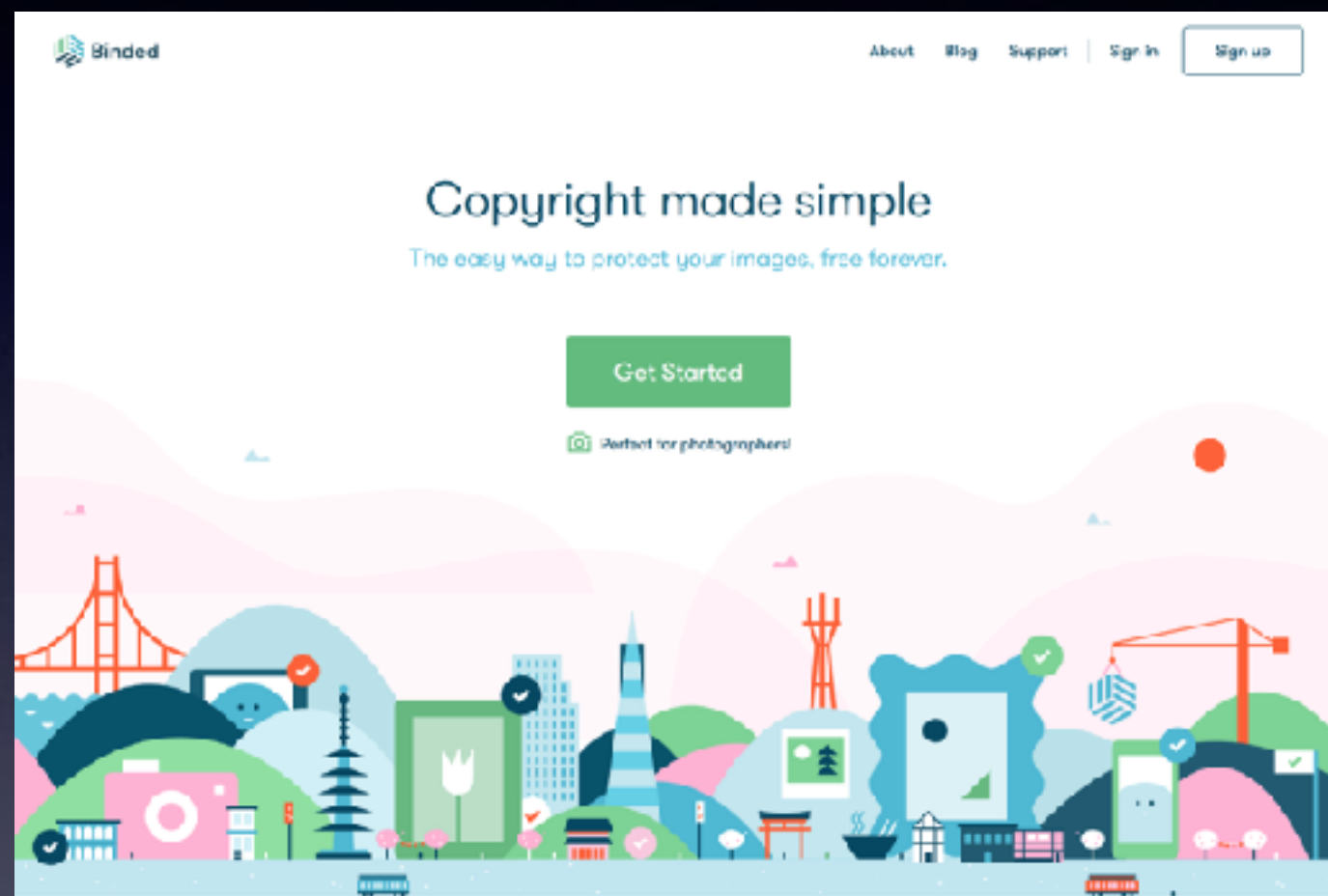
f t r + SK

"Virtual worlds are going to be one of the first killer apps for blockchains and perhaps the deepest users of them" – Fred Ehrsam, Co-Founder, Coinbase

Don't miss a trend.
Get Hub delivered to your inbox



Price: US\$100,000



7 Mar

Digital Science and Katalysis Lead Initiative to Explore Blockchain Technologies for Peer Review

TAGS: [#blockchainforresearch](#) , [Blockchain](#)

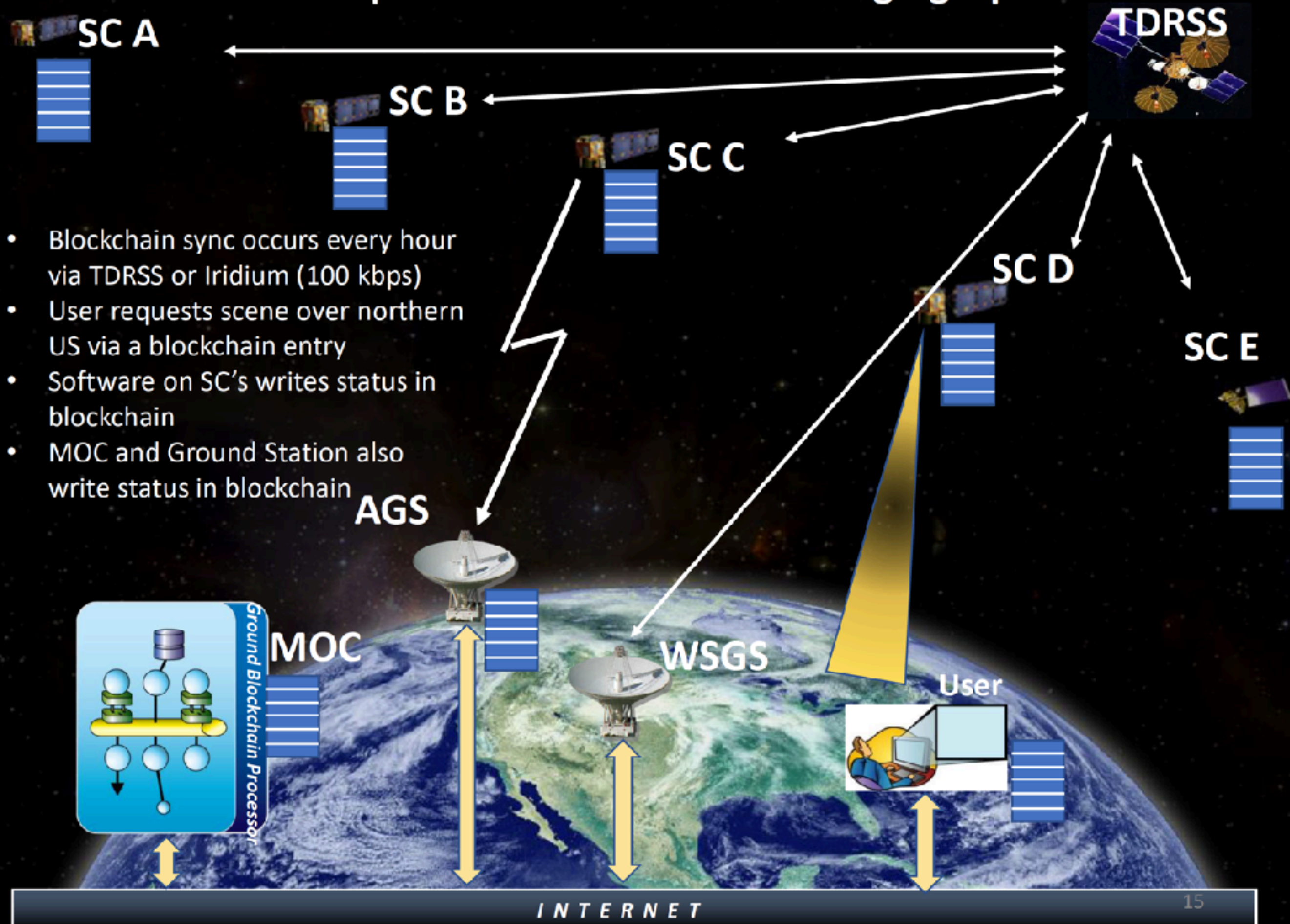
The initiative is an important step towards a fairer and more transparent ecosystem for peer review and explores the utility of decentralized data stores in supporting trusted assertions that connect researchers to their activities.

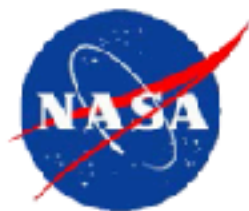
Boston, MA, USA and London, UK 7th March 2018: Digital Science and Katalysis are pleased to announce the launch of a pilot project to test blockchain technologies to support the peer review process. They are joined in this pilot project by founding partner Springer Nature.

The problems of research reproducibility, recognition of reviewers and the rising burden of the review process, as research volumes increase each year, have led to a challenging landscape for scholarly communications.

In its initial phase, this initiative aims to look at practical solutions that leverage the distributed registry and smart contract elements of blockchain technologies. Later phases aim to establish a consortium of organisations committed to working together to solve scholarly communications challenges that centre around peer review.

Blockchain in Space Scenario 1 – Basic Imaging Operations





Basic Imaging Operations

- User enters image request, location and timeframe via blockchain entry
- Assets provide availability which includes overflight times, inview times for ground stations and prescheduled conflicts
- First available asset schedules image time and downlink time as needed
- Operation errors, outages etc. are recorded on blockchain
- Completion time, downlink time to ground station and successful publishing of data to user specified location are documented in blockchain.

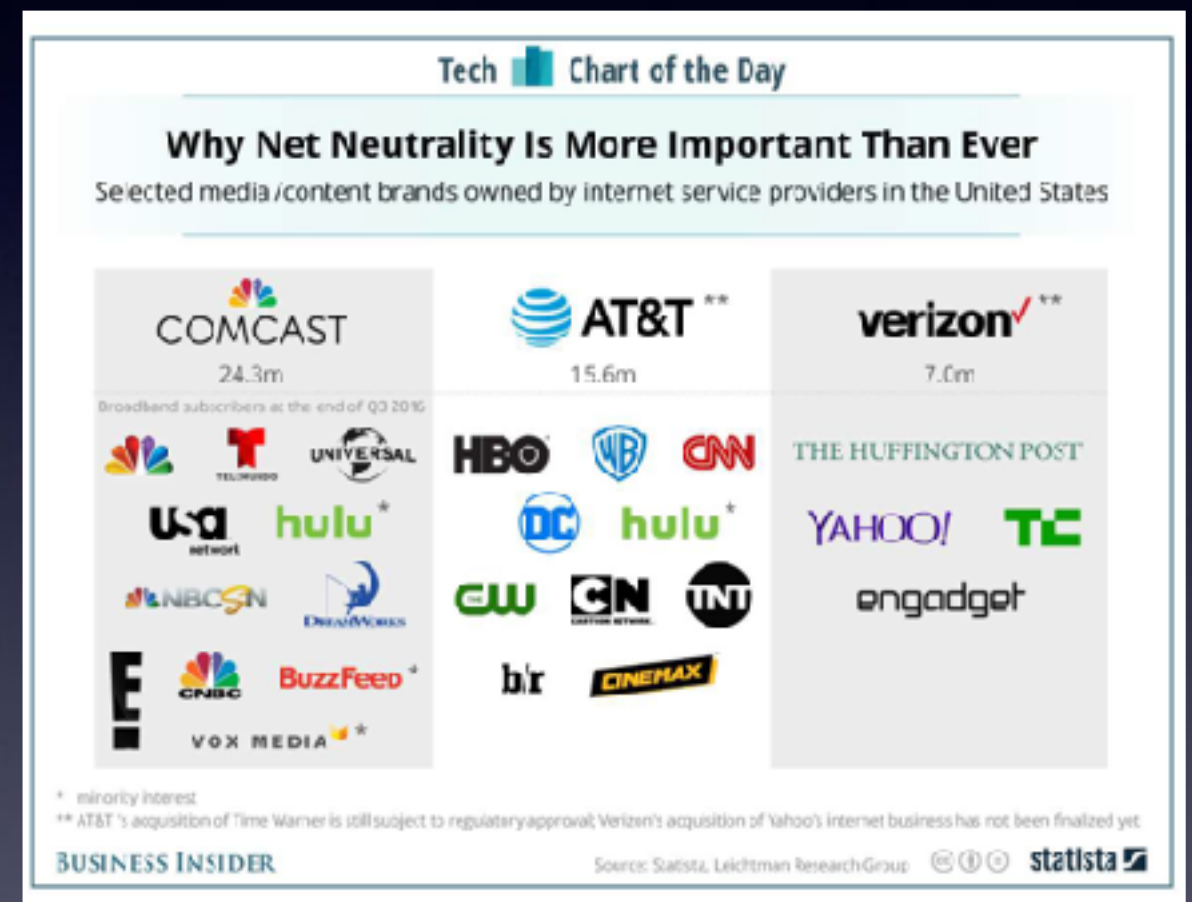
What's wrong with the Internet?

- Centralized (?) - DNS?, CAs?
- Vulnerable to censorship
- Client/server architecture/model is vulnerable to attack
- Suspicious incentives (?)
- Content and infrastructure often controlled by the same players
- Lack of permanence(?)
- Users have lost control of their data



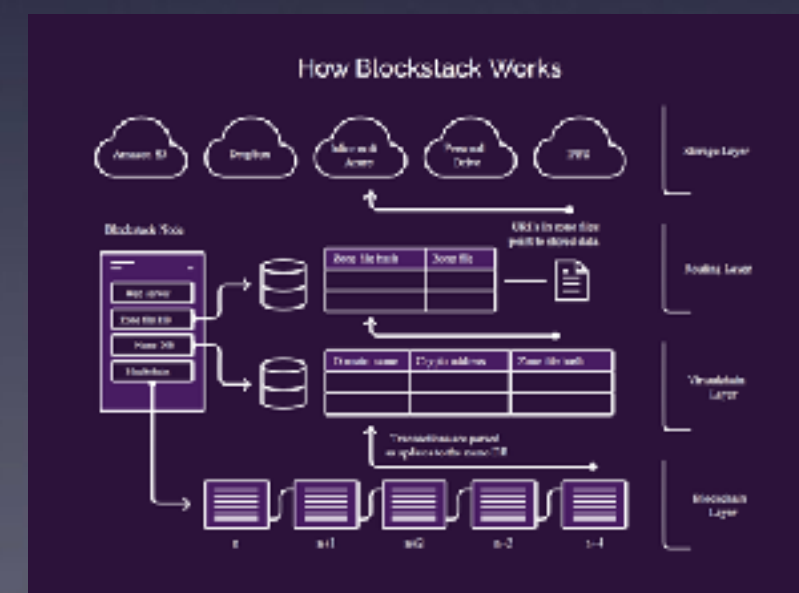
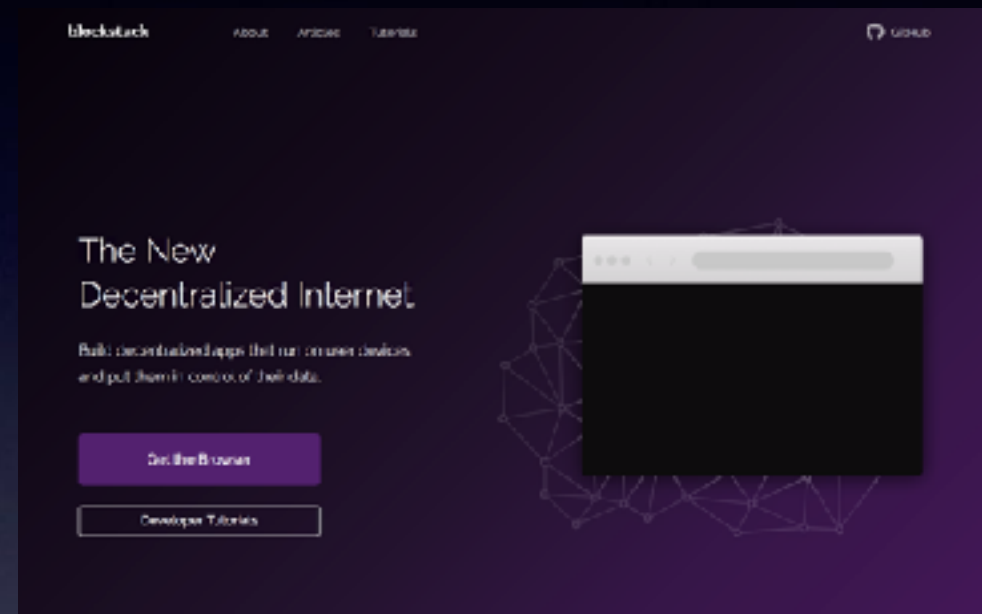
Example - Net Neutrality

- Media consolidation
- Media owned by the same parties that control infrastructure
- User data is controlled by those who control media and infrastructure
- Net neutrality is vulnerable to political tampering
- Rules can be changed arbitrarily by private parties



Is the Blockchain a foundation for a new Internet? (please don't call it 3.0!)

- Decentralized
- P2P architecture
- Neutral
- Censor-proof
- Geographically diverse
- Encrypted natively
- Incentivized protocols
- Native payments
- Transferable value
- User owned
- What would a decentralized Web look like?



Can Blockchain really help drive the next important tech eras?

- Does it really represent one of the next important tech era after mainframe, PC, Internet/Web, cloud, mobile?
- Internet: transfer of information; Blockchain: Internet++
- De-centralized systems vs. centralized systems
- Public, private, parallel/forking, and intersecting blockchains - a network of Blockchains?
- What could its role be in
 - Commerce/business/shared economies
 - Security/Privacy
 - Internet of Things
 - etc,etc,etc.

Summary and conclusions

- Blockchain is not the solution to everything, the *hype* (positive and negative) surrounding Blockchain must be taken seriously
- Blockchain (with or without cryptocurrency)
 - is a part of **grand experiments** in technology, sociology, economics, business, environmental issues, etc. that should not be ignored
 - can lead (or has led) to significant **disruptive technologies** based upon established principles (hype?)
 - has begun to evolve and spawn/fork exciting new variations
 - provides a potentially powerful development platform comparable to that of the Internet (hype?)
 - will continue to raise non-trivial issues surrounding adoption and regulation
 - defines a rich area for innovative research
 - requires a new wave of SMEs and developers

A Blockchain-based Decentralized Data Storage and Access Framework for PingER

Saqib Ali[†] and Guojun Wang[‡]
School of Computer Science and
Educational Software, Guangzhou University,
Guangzhou, P. R. China, 510006
Emails: {saqibali, csgjwang}@gzhu.edu.cn

Bebo White
Stanford Linear Accelerator Center
P.O. Box 4349,
Palo Alto, California 94309-4349
Email: bebo@slac.stanford.edu

Roger Leslie Cottrell
Stanford Linear Accelerator Center
P.O. Box 4349,
Palo Alto, California 94309-4349
Email: cottrell@slac.stanford.edu

Abstract—The blockchain is an innovative technology which opened doors to new applications for solving numerous problems in distributed environments. In this work, we design a blockchain-based data storage and access framework for PingER (world-wide end-to-end Internet performance measurement project) to remove its total dependence on a centralized repository. We use the permissioned blockchain and Distributed Hash Tables (DHT) for this purpose. In the proposed framework, metadata of the files is stored on the blockchain whereas the actual files are stored off-chain through DHT at multiple locations using a peer-to-peer network of PingER Monitoring Agents. This will provide decentralized storage, distributed processing, and efficient backup capabilities to the PingER framework.

Index Terms—Permissioned blockchain, Distributed ledger technology, PigER, Decentralized system

1. INTRODUCTION

The blockchain is a peer-to-peer distributed ledger in which records called blocks are linked and secured using cryptographic hashes [1]. By design, blockchains are decentralized, secure, immutable and extremely fault tolerance making it suitable for record management activities i.e., financial transactions, identity management and authentication [2]. Blockchain can be deployed as permissionless (Bitcoin or Ethereum blockchain) or permissioned i.e., Hyperledger¹. In permissionless or public blockchain the actors in the system are not known. Anyone joins or leave the network at any time which may raise security risks in the network. In permissioned or private blockchain only known and identifiable set of participants are explicitly admitted to the blockchain network [3]. This reduces the presence of malicious actors within the network. As result only authenticated and authorized actors can participate in the network which increases the security of the system as required by the enterprise applications [4].

The concept of permissioned blockchain is gaining a lot of interest especially for non-financial use cases (other than the cryptocurrencies) in which the users are authenticated and authorized to participate in the network [5]. The interesting non-financial areas that leverage the opportunities of permissioned blockchains include health, government services, supply chain

management, Internet of Things, peer-to-peer cloud storage and many more [6], [7]. The P2P cloud storage (i.e., STORJ², Sia³, Filecoin⁴) is an interesting application of blockchain as it provides a decentralized data storage facility without the need of a trusted third party or a client-server architecture. The decentralized data storage will help to eliminate the most traditional data failures and outages by increasing the security, privacy, and control of the data [8], [9].

Pinger (Ping End-to-end Reporting)⁵ which is a worldwide end-to-end Internet performance measurement framework developed and managed by the SLAC National Accelerator Laboratory USA [10]. The client-server architecture of Pinger consists of 50 active Monitoring Agents (MAs) in 20 countries of the world. These MAs probe 700 remote sites located in 170 countries of the world [11]. The ping statistics for each MA-remote site pair are stored on a local MA. The data archived by each MA is fetched daily by the SLAC to a centralized repository of text archives as shown in Figure 1.

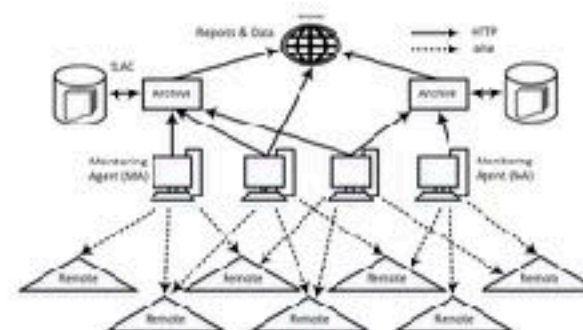


Fig. 1. PingER data storage and access architecture

The current architecture of the Finger is highly dependent on the SLAC computing resources, e.g., archival space, processing and uptime. Therefore, there is a need to ensure the future of the Finger data if/when SLAC support goes away. Further, different Finger nodes have different tasks.

[†]Department of Computer Science, University of Agriculture, Faisalabad, Pakistan, 38000. Email: saqib@uaf.edu.pk

*Correspondence to: csjwang@gzhu.edu.cn

¹<https://www.hyperledger.org/>

²<https://doi.org/10.1016/j.jm.2019.05.001>

⁵<https://sia.tech/>

^a<https://filecoin.io/>

⁵www.icpmc.hac.stanford.edu/inter/

The Distinguished Speakers Program is made possible by



**Association for
Computing Machinery**

Advancing Computing as a Science & Profession

For additional information, please visit <http://dsp.acm.org/>

About ACM



ACM, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence.

ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

With over 100,000 members from over 100 countries, ACM works to advance computing as a science and a profession. www.acm.org

Thank You!
Questions? Comments?

bebo@slac.stanford.edu

I encourage you to get onboard
- your ideas are needed!

