# From Trough to Plateau: How Blockchain will Disappoint Before it Massively Disrupts HR

**Rick Barfoot, HRNX Integrations**

**Mahesh Kharade, Harbinger Group**

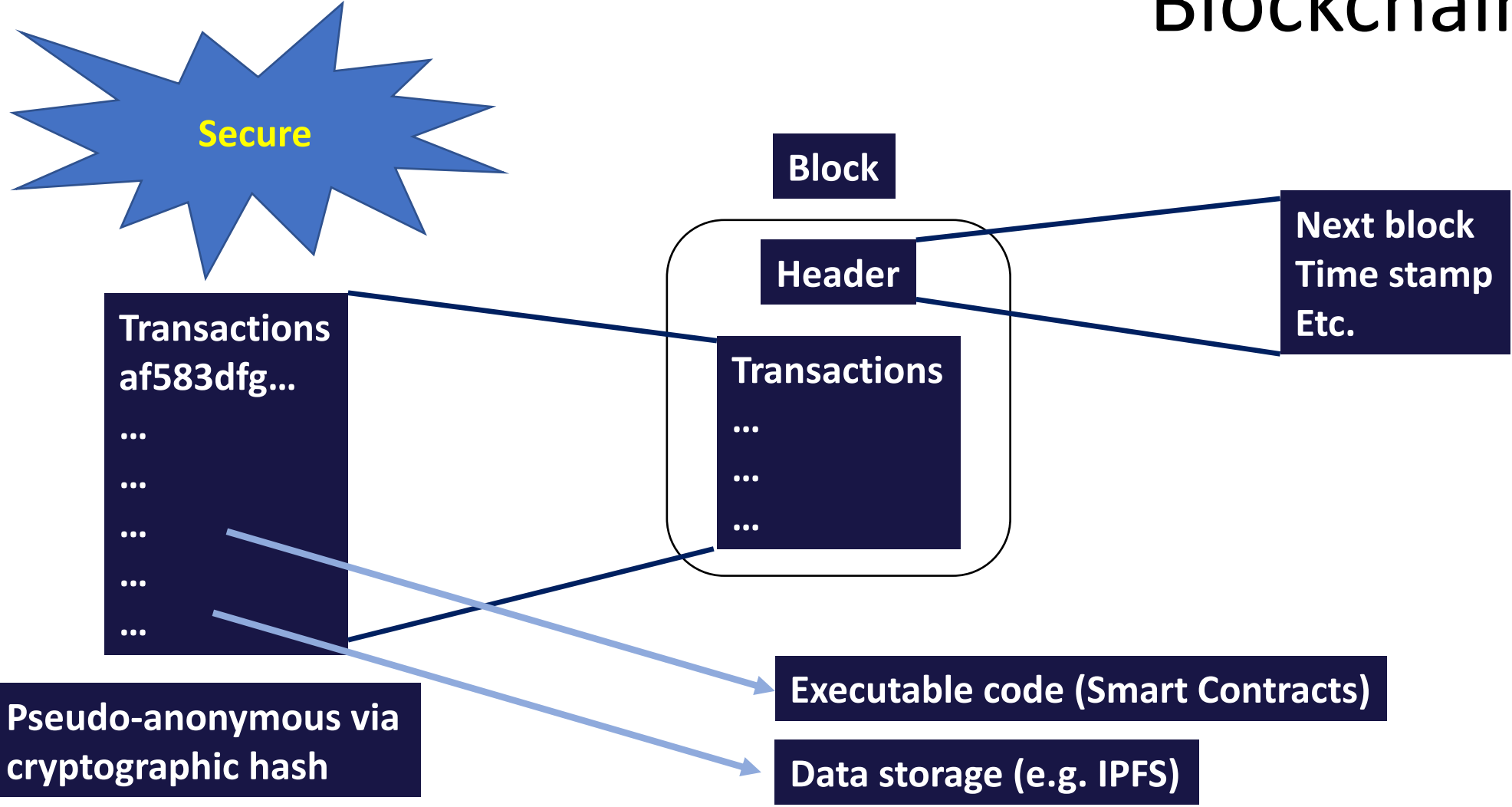# Bitcoin: A Peer-to-Peer Electronic Cash System

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.
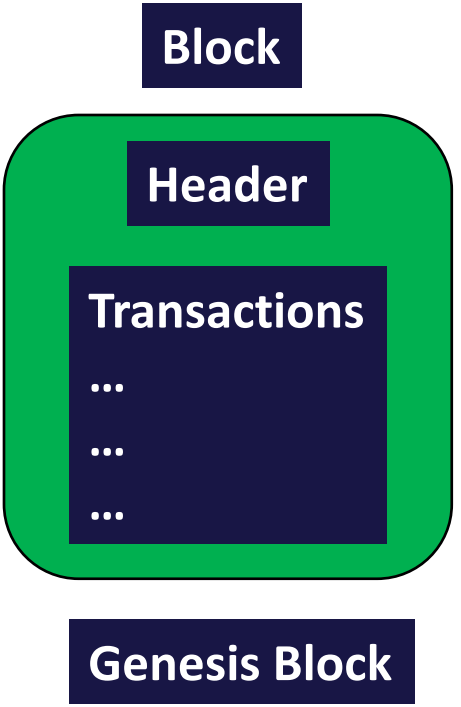
## 1.    Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must
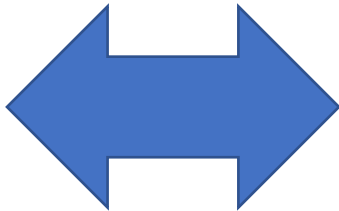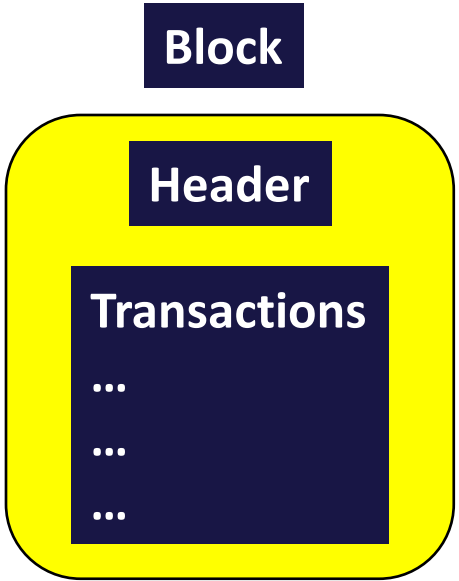
# Blockchain 101

**Secure**

**Block**

**Header**

**Next block**
**Time stamp**
**Etc.**

**Transactions**
**af583dfg...**
...
...
...
...
...

**Transactions**
...
...
...

**Pseudo-anonymous via cryptographic hash**

**Executable code (Smart Contracts)**

**Data storage (e.g. IPFS)**

# Blockchain 101

**Block**

**Header**

**Transactions**
...
...
...

**Genesis Block**

# Blockchain 101

**Block**

**Header**

**Transactions**
...
...
...

**Genesis Block**

**Block**

**Header**

**Transactions**
...
...
...

Validate or "mine" the next block

Consensus mechanisms:
- **Proof of work**
- **Proof of stake**

- **Token economy**

**Decentralized**
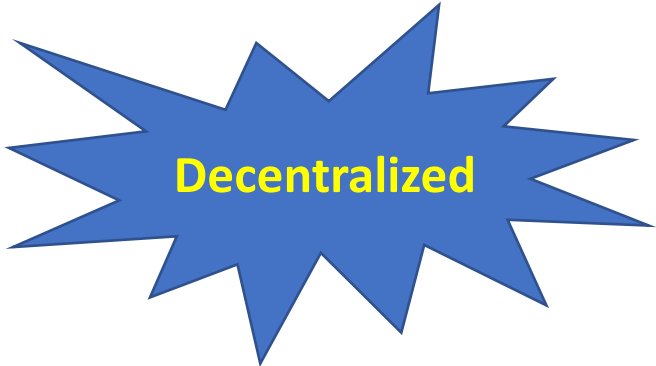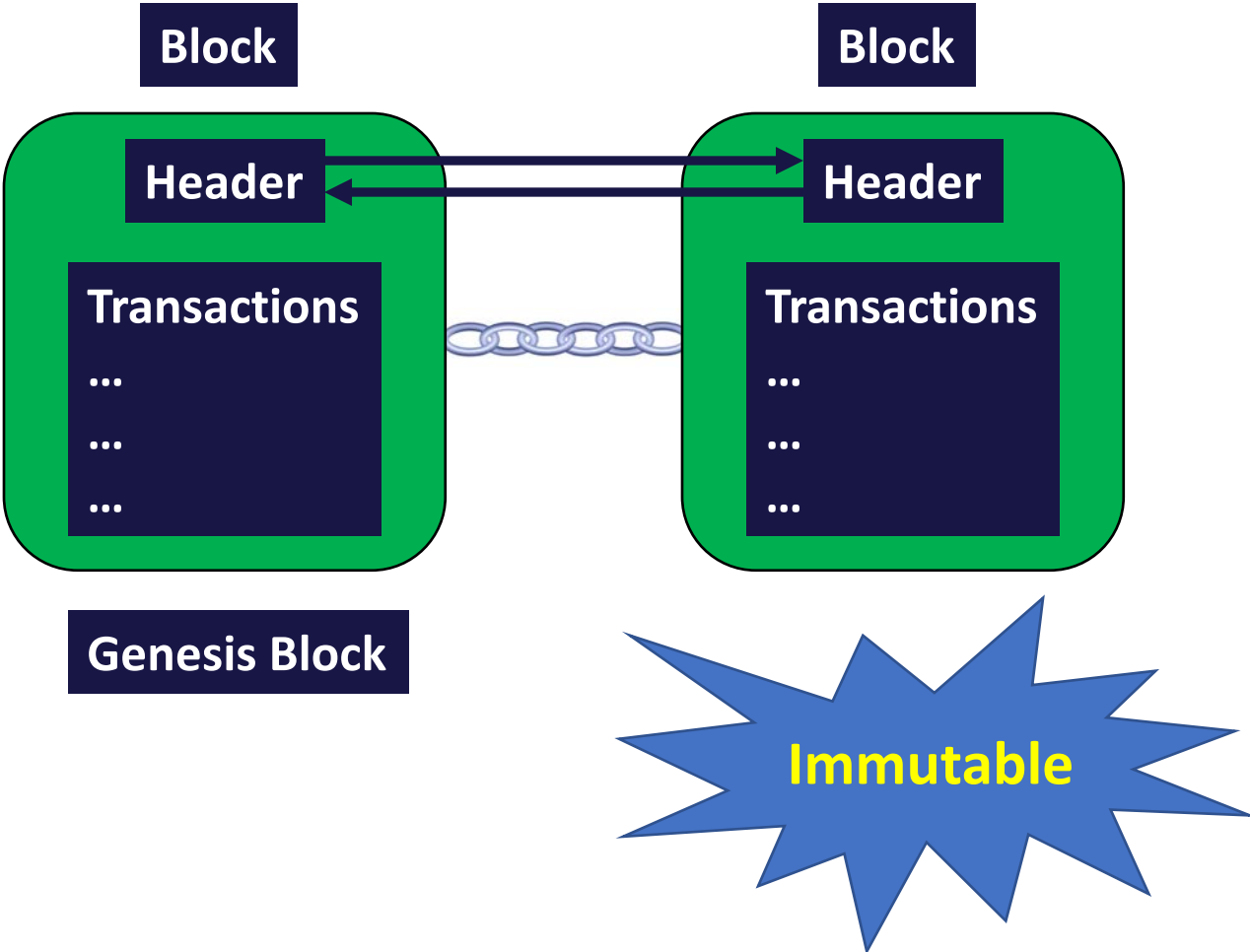
# Blockchain 101
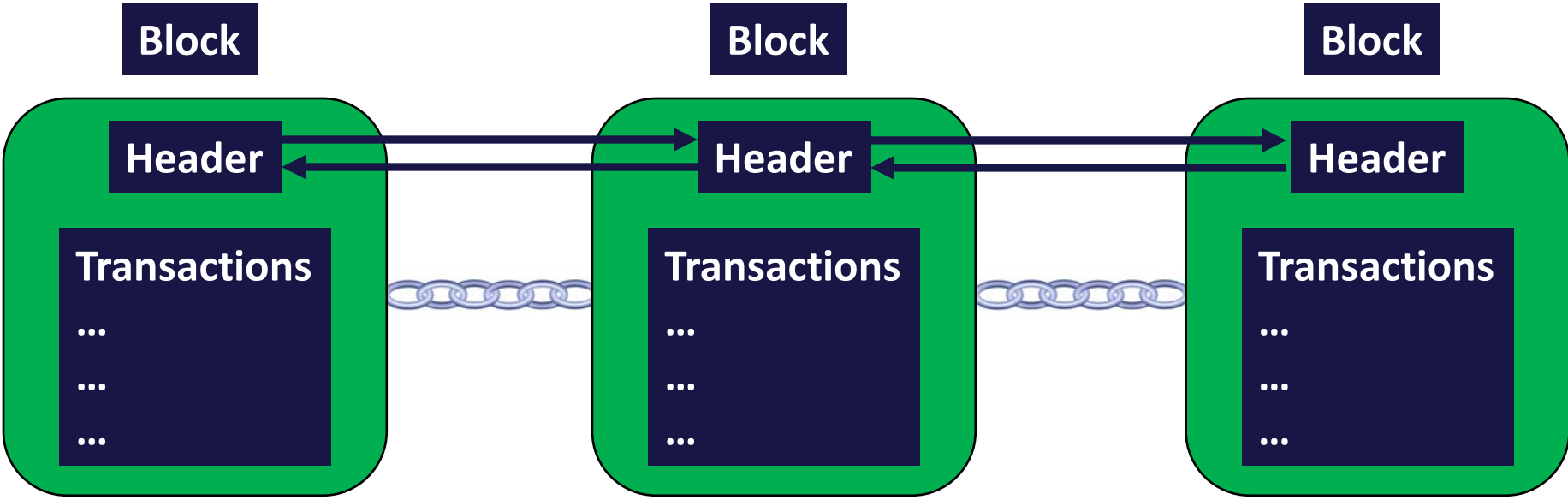
# Blockchain is an innovation, not an invention...

## References

[1]   W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2]   H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3]   S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4]   D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5]   S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6]   A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7]   R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8]   W. Feller, "An introduction to probability theory and its applications," 1957.

- Distributed, decentralized, peer-to-peer network
- Immutability
- Cryptographic hash
- Consensus mechanism

**A Globally Shared State & Trust Layer for the Internet**

"Not since the Web itself has a technology promised broader and more fundamental revolution than blockchain technology."

- Hyperledger project

"*Blockchain promises to* **reshape industries** *by enabling trust, providing transparency and* <mark>reducing friction across business ecosystems</mark>*. Blockchain forces enterprise architecture and technology innovation leaders to* **rethink the notion of value exchange** *in a world of decentralized trust.*"

- Gartner

# Hype Cycle for Blockchain Business, 2018



**expectations**

- Blockchain Reward Models
- Initial Coin Offering
- Blockchain in Government
- Blockchain Consortium
- Blockchain in Insurance
- Blockchain in Banking and Investment Services
- Blockchain in Supply Chain
- Blockchain
- Blockchain in Logistics and Transportation
- Distributed Ledgers
- Blockchain in Education
- Internet of Things
- Cryptocurrency and Blockchain Regulation
- Blockchain in Life Sciences
- Blockchain in Utilities
- Blockchain in Healthcare
- Things as Customers
- Smart Contracts
- Smart Assets
- Blockchain in Oil and Gas
- Decentralized Autonomous Organization
- Blockchain Business Models
- Ricardian Contracts
- Blockchain in Retail
- Blockchain in Media and Entertainment
- The Programmable Economy
- Cryptocurrencies
- Blockchain in Manufacturing
- Digital/Cryptocurrency Fiat
- Digital Commodity Exchanges
- Blockchain for CSPs
- Green Money
- Stable Cryptocurrency
- Blockchain-Based ACH Payments
- Blockchain for Advertising
- Blockchain for Customer Service
- Complementary Currency

As of July 2018

| Innovation Trigger | Peak of Inflated Expectations | Trough of Disillusionment | Slope of Enlightenment | Plateau of Productivity |

**time**

**Plateau will be reached in:**

○ less than 2 years ○ 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

## gartner.com/SmarterWithGartner

**Gartner**®

" The thing that I often ask startups on top of Ethereum is, 'Can you please tell me why using the Ethereum blockchain is better than using Excel?' And if they can come up with a good answer, that's why you know you've got something really interesting."
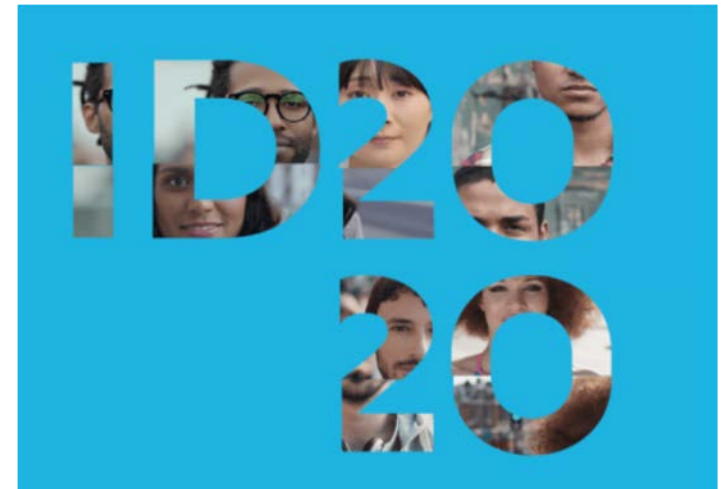- Vitalik Buterin

What says Vitalik?

# HR Use Case:  Candidate Verification

- If it happened, it only needs to be officially verified ONCE:
  - Identity verification
  - Employment and education history
  - Credentials
  - Criminal history

- Token-based system based on value creation
  - Pay to pull
  - Get paid to push



Accenture has joined the ID2020 Alliance with partners like Microsoft to create an open, human-centric approach to identity. The alliance draws on advances in biometrics and innovative technologies and brings together expertise from business, government and non-government agencies. Our experts at the Dublin Innovation Center contribute cross-functional and cross-cultural expertise to drive it forward in collaboration with both UN and other global humanitarian organizations. Get in touch with us.
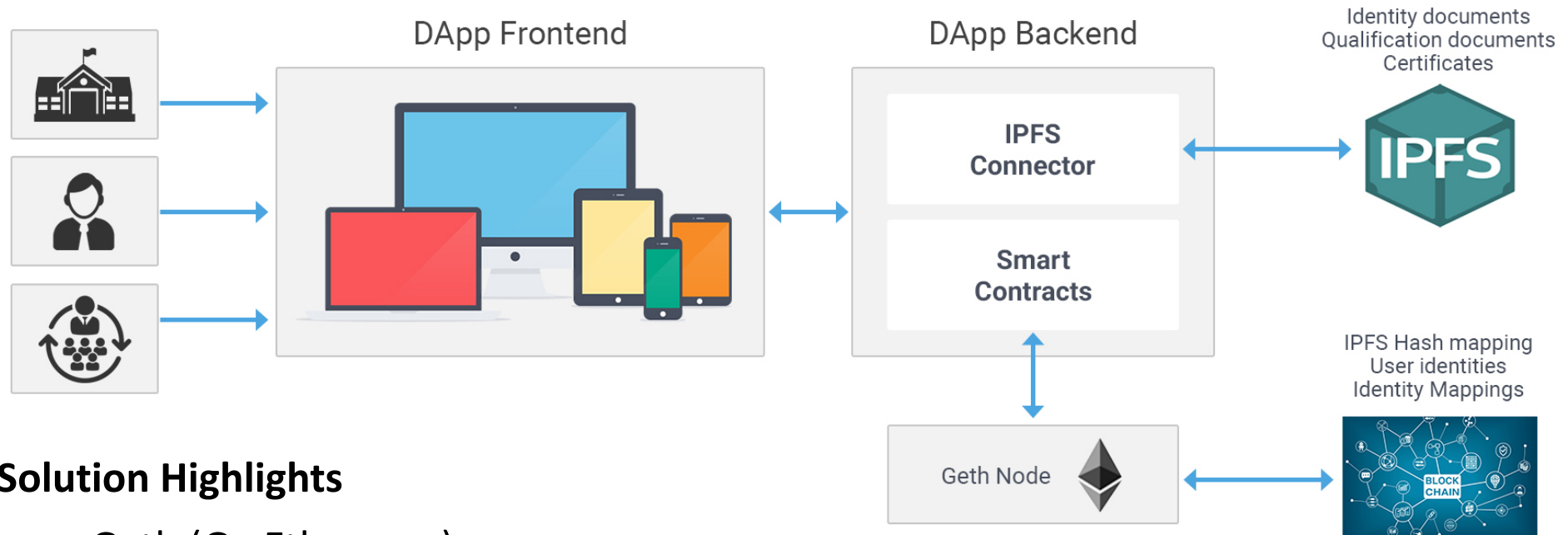
- Challenges in Traditional Workflow:
  - Expensive verification process
  - Ownership of employee data
  - Maintenance of data

- Management of employee data using blockchain – an example workflow:
  - Employer and Employee access
  - Blockchain to save employee data
  - Use of Smart Contracts
  - Who has access to what?

# High Level Architecture

## DApp – Distributed web app

DApp Frontend

DApp Backend

Identity documents
Qualification documents
Certificates

**IPFS Connector**

IPFS

**Smart Contracts**

IPFS Hash mapping
User identities
Identity Mappings

Geth Node

**Solution Highlights**

- Geth (Go Ethereum)
- IPFS 0.4.10
- Meteor

# Verified Profiles



*Start-ups are going it alone, finding early adopter partners to join their networks, or trying to propagate their blockchain as industry standard…*

# Credential Verification



*Point solutions can be quickly adopted but how will they tie into broader blockchains?*

# Considerations

- Adoption – legacy systems with data silos; "chicken and egg"
- Industry coordination – currently there are no standards
- Technology – "normal" issues like scaling, etc.
- Legal (e.g., FCRA) – who has jurisdiction over a blockchain?

*This technology inherently needs an **industry consortium approach***

# Consortium Approach

- Blockchains are <u>decentralized</u>

- Blockchain networks are launched by *anchor participants*

- A consortium is needed to:
  - Bring together interested parties
  - Define a block standard
  - Determine how to interoperate with other blockchains
  - Provide best practices for implementation

# Evolution

- We are in a period of transition:
  - Old Guard:  centralized; "social waste"
  - Disruptors:  will still need oracles and agents to feed data possibly even leveraging the Old Guard
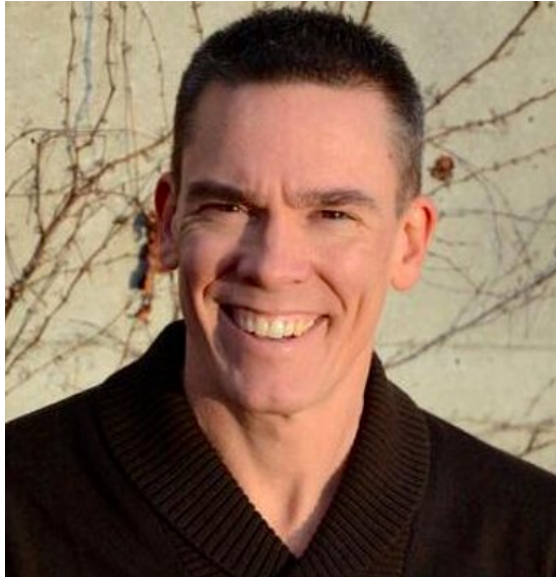  - Sources of Truth will publish directly to blockchain

# Thanks!

**Rick Barfoot**

CTO, HRNX Integrations

rick.barfoot@hrnx.com

**Mahesh Karade**

Associate GM, Harbinger Group

maheshkumar@harbingergroup.com