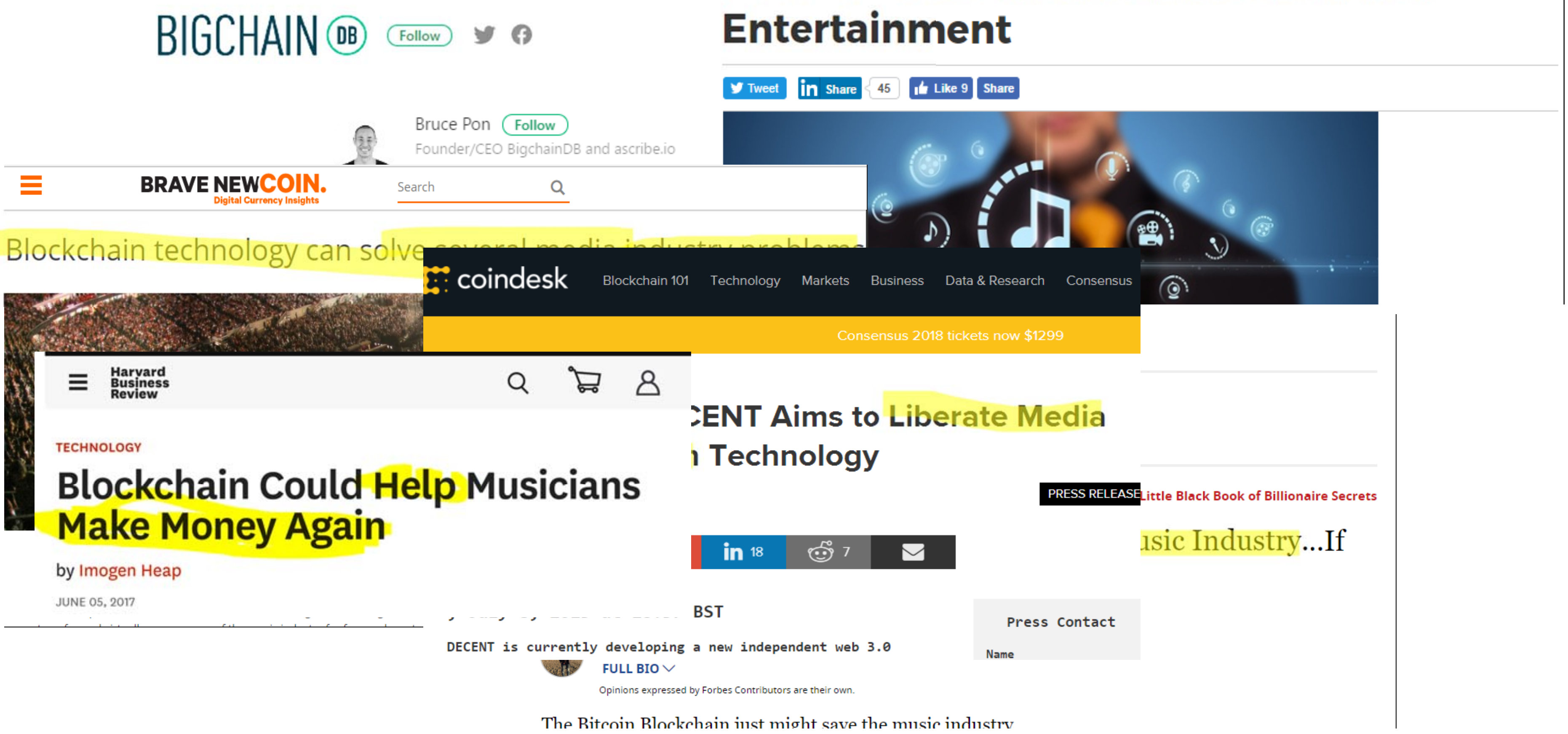
Is Blockchain the Savior of the Media Industry?

ERIC DIEHL

VP, Security and Media Technologies

REALLY?



BIGCHAIN DB Follow

Bruce Pon Follow

Founder/CEO BigchainDB and ascribe.io

BRAVE NEWCOIN. Digital Currency Insights

Search

Blockchain technology can solve several media industry problems

How Blockchain will Transform Media and Entertainment

Tweet | Share 45 | Like 9 | Share

coindesk | Blockchain 101 | Technology | Markets | Business | Data & Research | Consensus

Consensus 2018 tickets now $1299

CENT Aims to Liberate Media
n Technology

PRESS RELEASE

in 18 | 7

BST

DECENT is currently developing a new independent web 3.0

Press Contact

Name

Harvard Business Review

TECHNOLOGY

Blockchain Could Help Musicians Make Money Again

by Imogen Heap

JUNE 05, 2017

Little Black Book of Billionaire Secrets

usic Industry...If

FULL BIO

Opinions expressed by Forbes Contributors are their own.

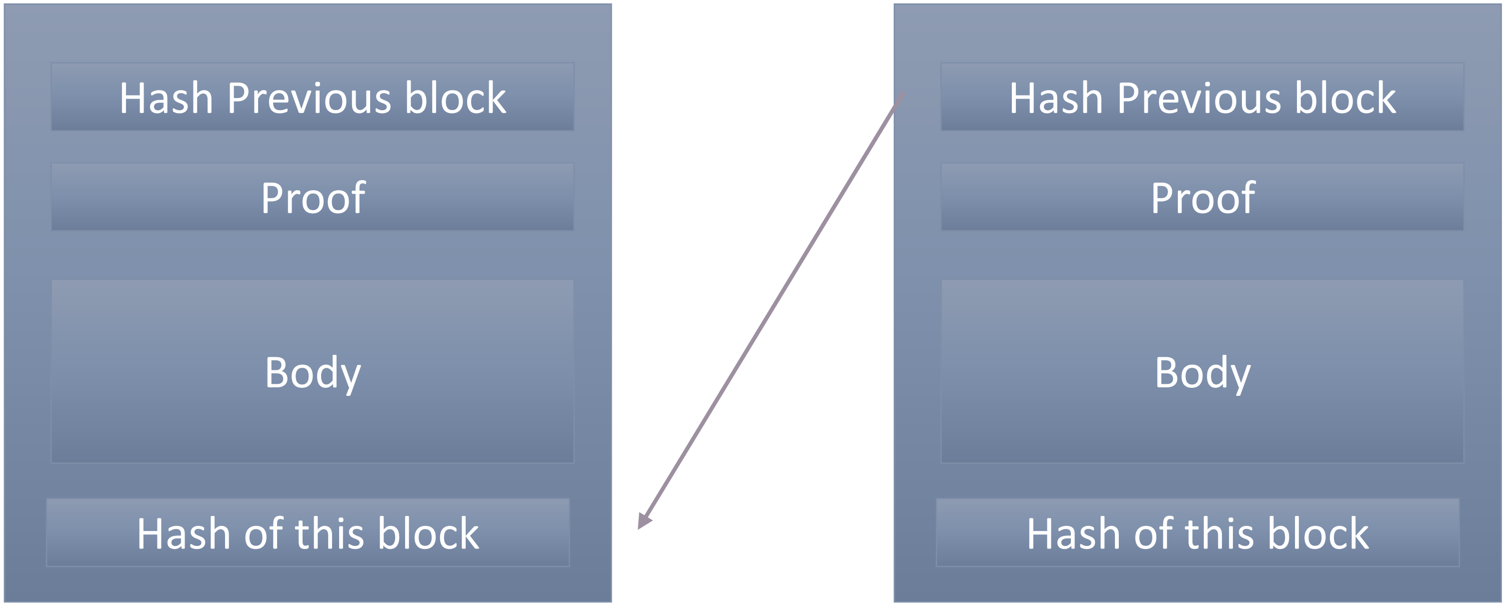
The Bitcoin Blockchain just might save the music industry

Agenda

- Blockchain 101
- Mythology
- Consensus?
- Smart contract?

Blockchain 101

Basic Block Structure



Hash Previous block

Proof

Body

Hash of this block

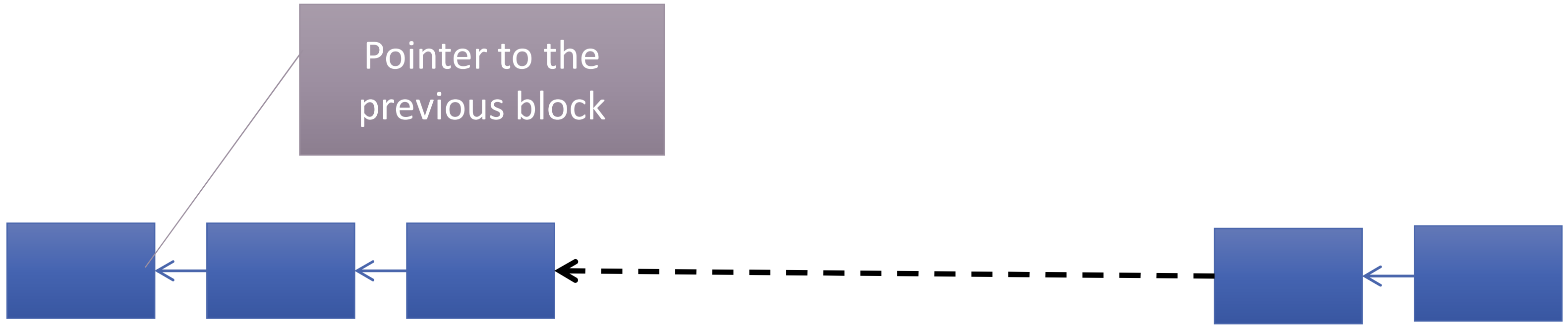
Hash Previous block

Proof

Body

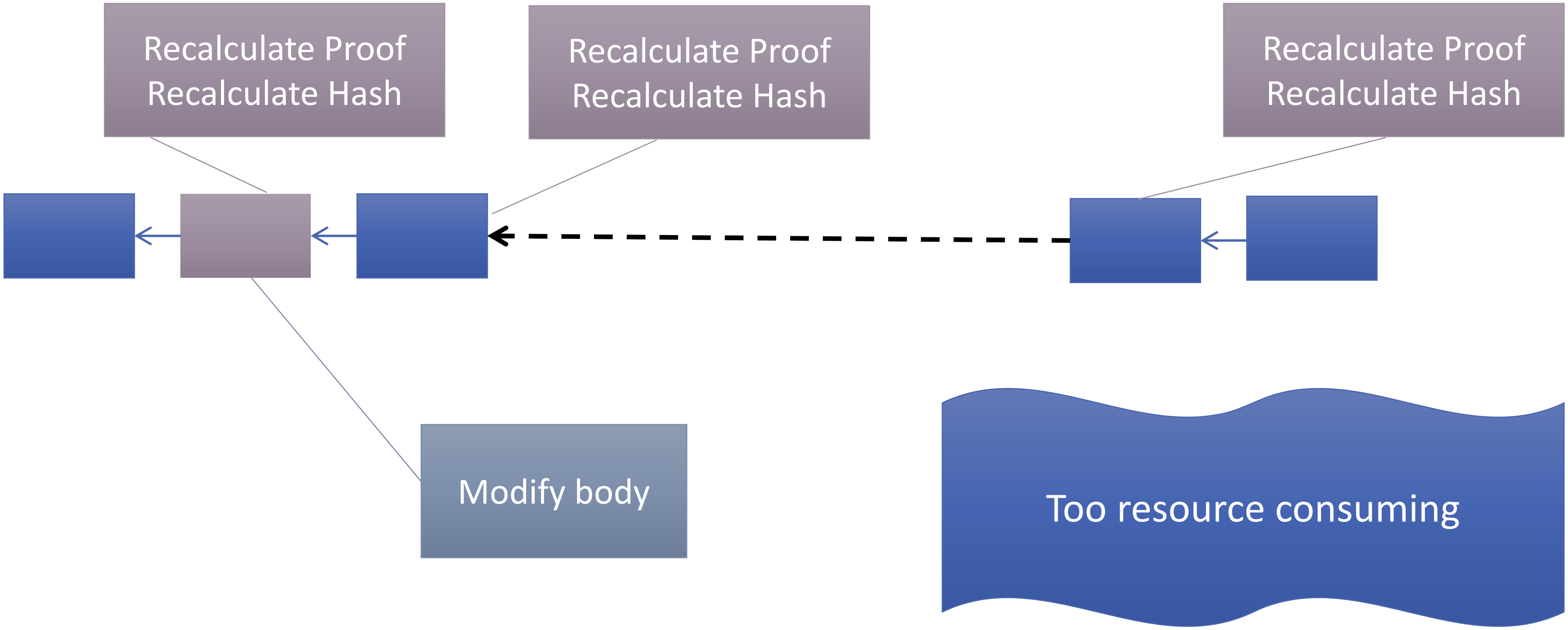
Hash of this block

A Time-Ordered Chain



Pointer to the previous block

A Time-Ordered Chain Immutable



Recalculate Proof
Recalculate Hash

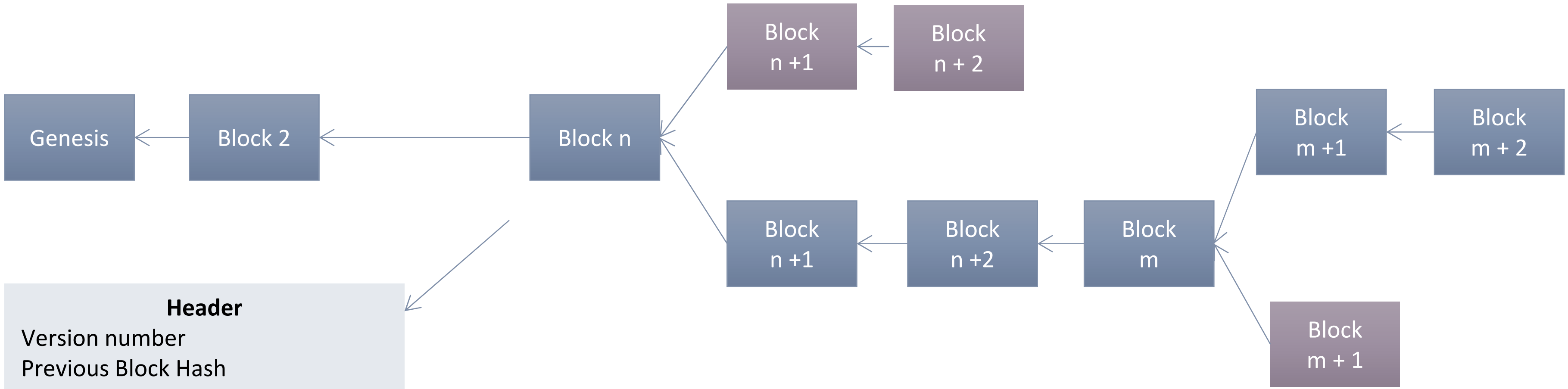
Recalculate Proof
Recalculate Hash

Recalculate Proof
Recalculate Hash

Modify body

Too resource consuming

Bitcoin Structure



Header

Version number
Previous Block Hash
Transaction Merkle Root
Timestamp
Difficulty Target
Nonce

Body

Transaction 1
Transaction 2
….

Input

Previous Transaction Hash
Sender’s Public Key
Signature by sender

Output

Value
Recipient's public key

Characteristics of Blockchain Ledger

- **Immutable**
  - Cannot modify the stored blocks
  - Self protected
- **Perfect ledger structure**
  - Ledger of timestamped transactions
  - Ledger of sequential transactions
- **Control point**
  - Addition of a new block to the chain
  - Who is the authority?
    - The public, i.e. permissionless
    - Set of trusted entities, i.e. permissioned

Some Advantages

- **Integrity**
  - Digital signature offers the same feature
- **Non tampering**
  - Linked chain
  - Distributed block chain
- **Chronological registration**
- **Distributed**
- **Undeniability and transparency**

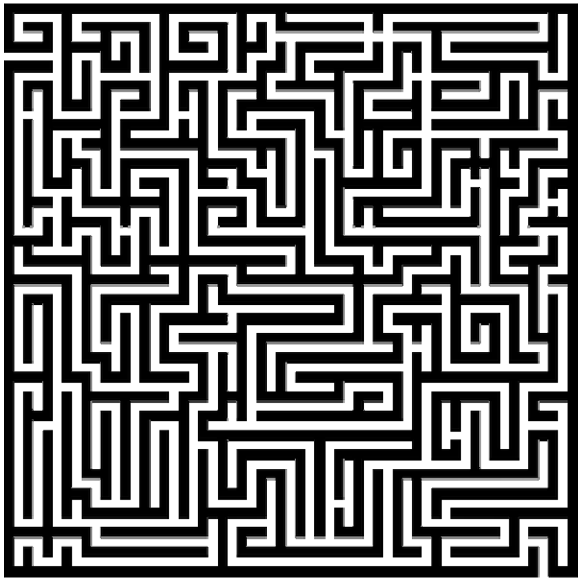
Some Disadvantages

- **Size of the ledger**
  - linear increase with size O(n)
- **Latency in transaction validation**
  - Especially if permissionless distributed block chain
    - Bitcoin has a 50 mn latency
- **Transparency**
  - When confidentiality is needed

Mythology

Some Remarks

- **Block chain**
  - Ledger of chronological transactions
    - Verification by navigating the list
  - Difficult to fool
- **Bitcoin introduces some complexity**
  - ANY BODY should be allowed to write to the chain block
  - No centralized power
- **This complexity may not be needed in all cases**

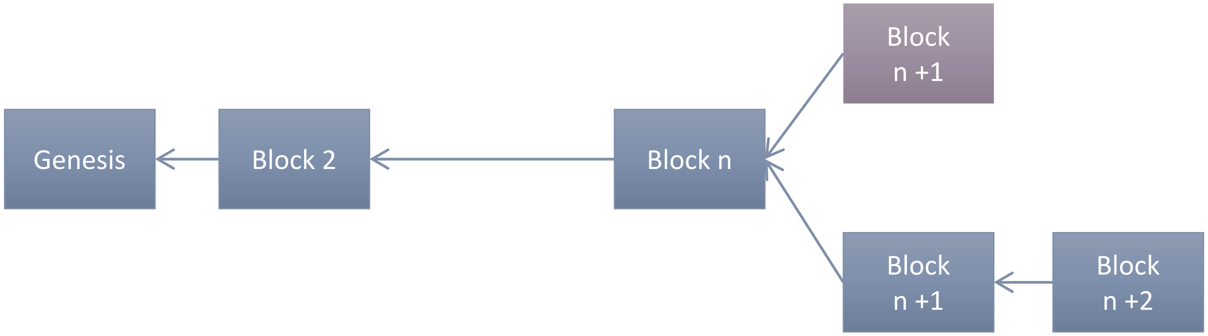


Some Misconceptions

- **Blockchain ≠ Bitcoin or cryptocurrency**
- **Blockchain does not need to have distributed permissionless consensus**
  - Cryptocurrency uses public distributed consensus
  - Land registry does not use public validation
- **Blockchain does not need to be public**
- **Blockchain does not need mining**
  - Proof of Work is only needed for permissionless blockchain
- **Blockchain is not necessary slow and with latency**
  - Bitcoin handles 7 transactions per second
  - Permissioned blockchains can be faster.

Consensus?

Problem



TWO PROBLEMS:

- How is a transaction validated?
- How to synchronize the distributed ledgers?

Four Different Models

- **Proof of Work**
- **Proof of Stack**
- **Byzantine Fault Tolerance**
- **Federated Byzantine Agreement**

Proof of Work

- **Solve the equation**
  - *Target* is defined by Authority
  - *Hash* = SHA-256
- **Difficult to solve**
  - Brute force calculation only
- **Easy to verify**
- **Challenge adjusts the average time to solve the equation**
  - Number of miners
  - Total calculation power

$$Target \geq Hash(B_i|x)$$

Proof of Work

- **Why does it work?**
  - Computationally costly to validate
  - Reward the validators
  - The likelihood that an attacker controls large chunk of the validators is small
    - Mining pools?
- **Pros**
  - Permissionless system
- **Cons**
  - Lot of wasted resources
    - Power consumption of Ireland!
  - Latency
  - 51% attack
  - Large network of miners needed

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf.

Proof of Stake

- **Next block generator is polled deterministically with a function of its wealth (i.e., stake)**
- **If you own *n*% of the coins, you may expect to mint *n*% of the blocks**
- **Examples; PPCoin, Ethereum…**
  - Coin age = amount x holding period
  - Bid coin ages

$$Pr_{gen}(Alice) = f\left(Wealth(Alice)\right)$$

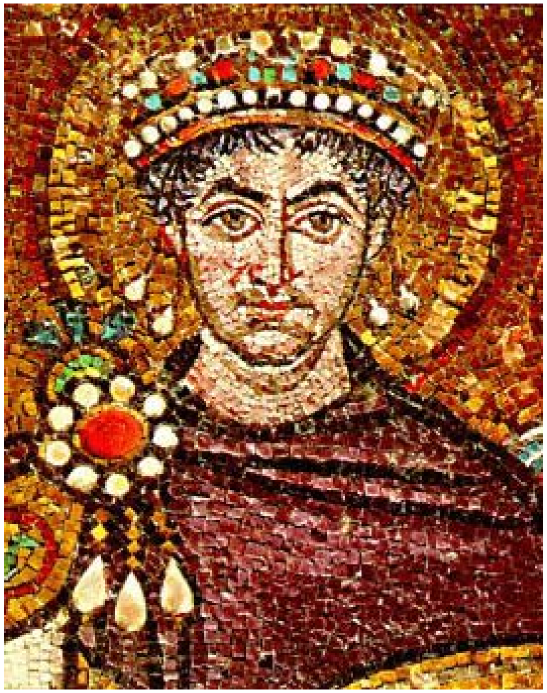
Proof of Stake

- **Why does it work?**
  - the more you own of the system, the more you are expected to defend it
- **Pros**
  - Permissionless system
  - Less consuming than PoW
- **Cons**
  - Weaker trust model
  - Nothing at Stake attack
  - No established formally proven protocol
    - No strong theory
  - Latency

King, Sunny, and Scott Nadal. “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” August 19, 2012. https://peercoin.net/assets/paper/peercoin-paper.pdf.

Byzantine Fault

- **Byzantine Fault = any failure of the system**
  - Involuntarily such as a crash
  - Voluntarily such as a malicious behavior
- **Byzantine fault tolerant system survives in case of Byzantine fault**
  - *n* nodes
  - *f* ill-behaving nodes
  - *n-f* well-behaving nodes
  - Optimal n=3*f*+1



Practical Byzantine Fault Tolerance (PBFT)

- **Why does it work?**
  - Built to be resilient up to a given level
- **Pros**
  - Simple and robust
  - Well adapted to known set of trusted entities
  - Trust is not linked to resources
- **Cons**
  - Not flexible
    - Pre-established list of participants
  - Sybil attack
  - All entities have the same trust level

Castro, Miguel, and Barbara Liskov. “Practical Byzantine Fault Tolerance.” In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*. New Orleans, USA: USENIX Association, 1999. https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance

Federated Byzantine Agreement (FBA)

- **A quorum slice for node *v* is a set of nodes sufficient for *v* to decide that v decides to agree**
- **A quorum is a set of nodes necessary to reach an agreement**
  - In PBFT, any $2f + 1$ nodes form a quorum
- **A FBA system can guarantee agreement if and only if any of 2 quorums share a node**
- **A two-step validation process**
  - Commitment ballot
  - Confirmation phase

Federated Byzantine Agreement (FBA)

- **Why does it work?**
  - Formally proved
  - Distributed Byzantine decision
- **Pros**
  - Open membership
  - Each node decides who it trusts
  - Low latency
- **Cons**
  - Need to reach quorum intersection
  - Complex negotiation protocol

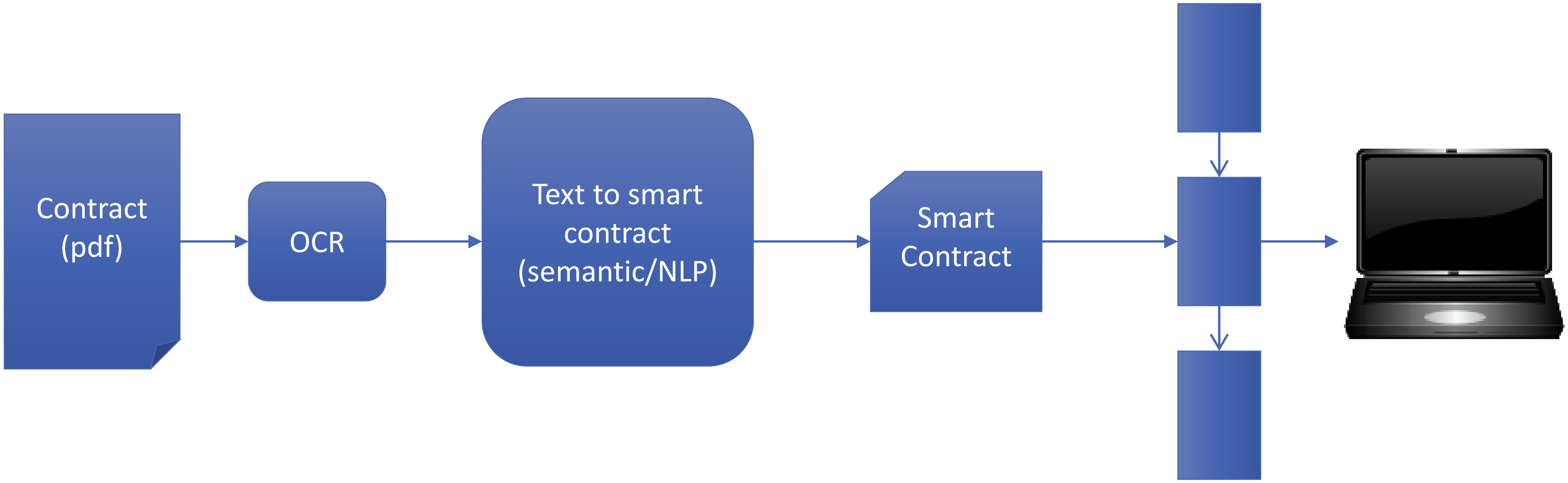
MAZIERES, DAVID. “The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus,” July 14, 2015. http://www.the-blockchain.com/docs/The%20Stellar%20Consensus%20Protocol%20-%20A%20Federated%20Model%20for%20Internet-level%20Consensus.pdf

Smart Contracts?

Smart Contract

- **A piece of software that is executed once a transaction is validated**
- **Some characteristics**
  - Protected in integrity by the blockchain
  - Interpreted language with rather rich expressivity
- **Announced to be THE solution**
  - It is not simple in real world scenario

Theoretical Use Case:
Managing All Contracts by a Blockchain



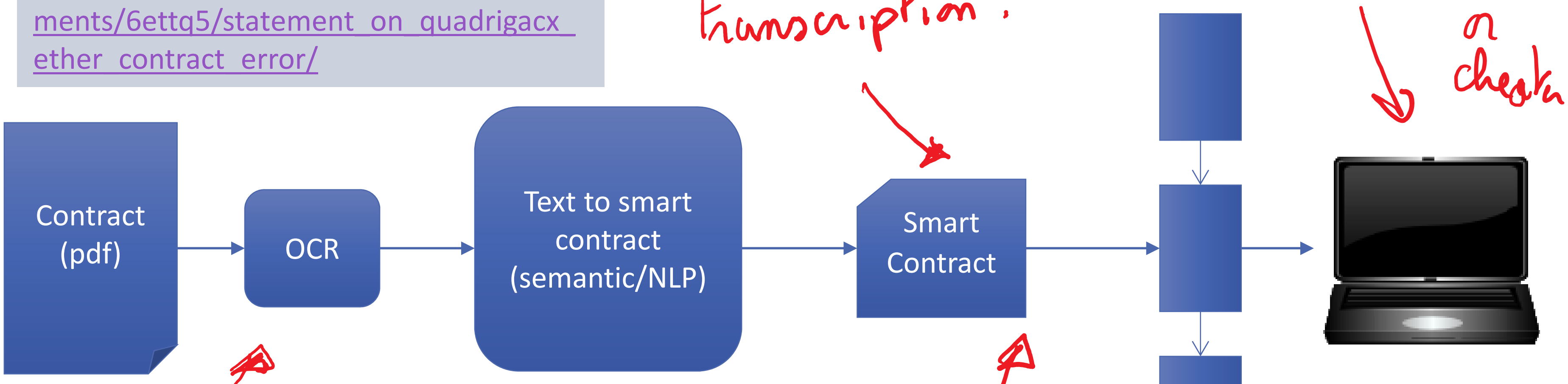
NLP: Natural Language processing

Use Case: What Could Go Wrong?

ETHEREUM JUNE 17
https://www.reddit.com/r/ethereum/comments/6ettq5/statement_on_quadrigacx_ether_contract_error/

Accurate transcription?

No bug in VM or checker?



$10.00 or $100.00

ETHEREUM JUN 16
http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/

No bug in transcription?

Remediation

Hard Fork as a Remediation?

- **Ethereum and DAO**
  - Hard fork on 17th July 2016 to recover the $40M theft from DAO
- **Undermines immutability**
- **Who decides to fork?**

Conclusion

Conclusion

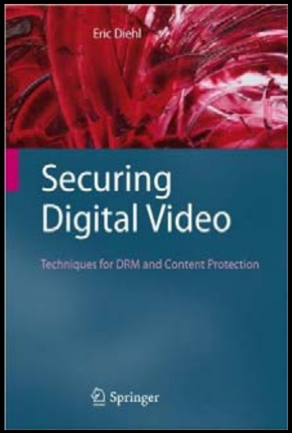
- **Blockchain is a promising technology**
- **Blockchain is larger than Bitcoin or Ethereum**
- **Practical Federated Byzantine Agreement may be a more suitable consensus system for the M&E industry**
  - At least for many scenarios
- **Smart contracts may need some maturity**
  - Tools for formal proof and test
  - Security model

Conclusion: What Next?

- **Better understand the technology**
- **Identify M&E problems that blockchain may solve**
  - Immutability
  - Distributed
- **Design some heuristics to decide when to use blockchain**
- **Experiment**

Thank you for your attention! Merci

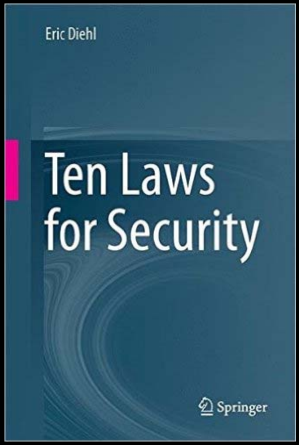
Any questions?


Eric Diehl

Securing Digital Video

Techniques for DRM and Content Protection

Springer


Eric Diehl

Ten Laws for Security

Springer