RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

#RSAC

SESSION ID: GPS-R09B

BEYOND TRADITIONAL PASSWORD AUTHENTICATION: PKI & BLOCKCHAIN

Sid Desai

Head of Business Development
Remme.io
@skd_desai

Agenda

- Our relationship to our digital-selves
- Evolution of Authentication Methods
- PKI-based Authentication
- Blockchain + PKI
- Conclusion

Security first? Think again!

Afterthought?

World's Biggest Data Breaches

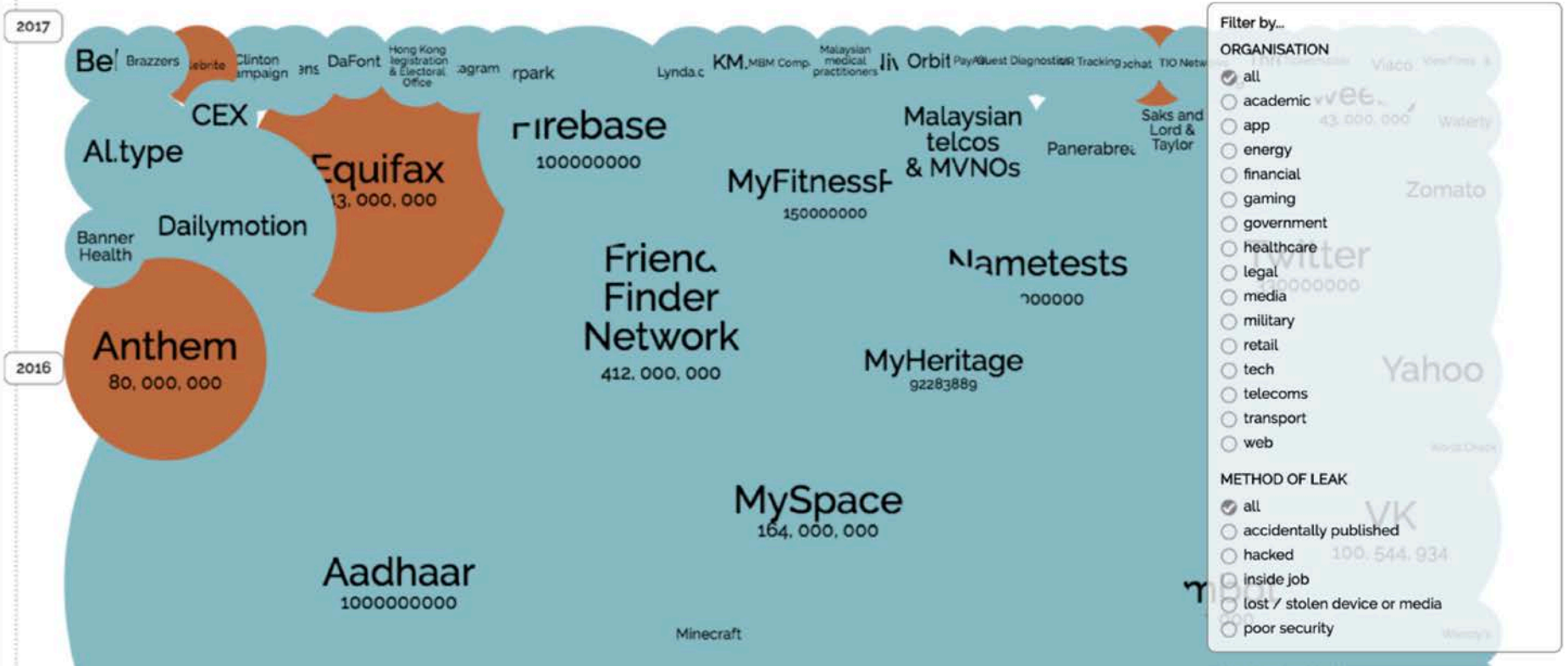
Selected losses greater than 30,000 records

(updated 4th July 2018)

interesting story

YEAR

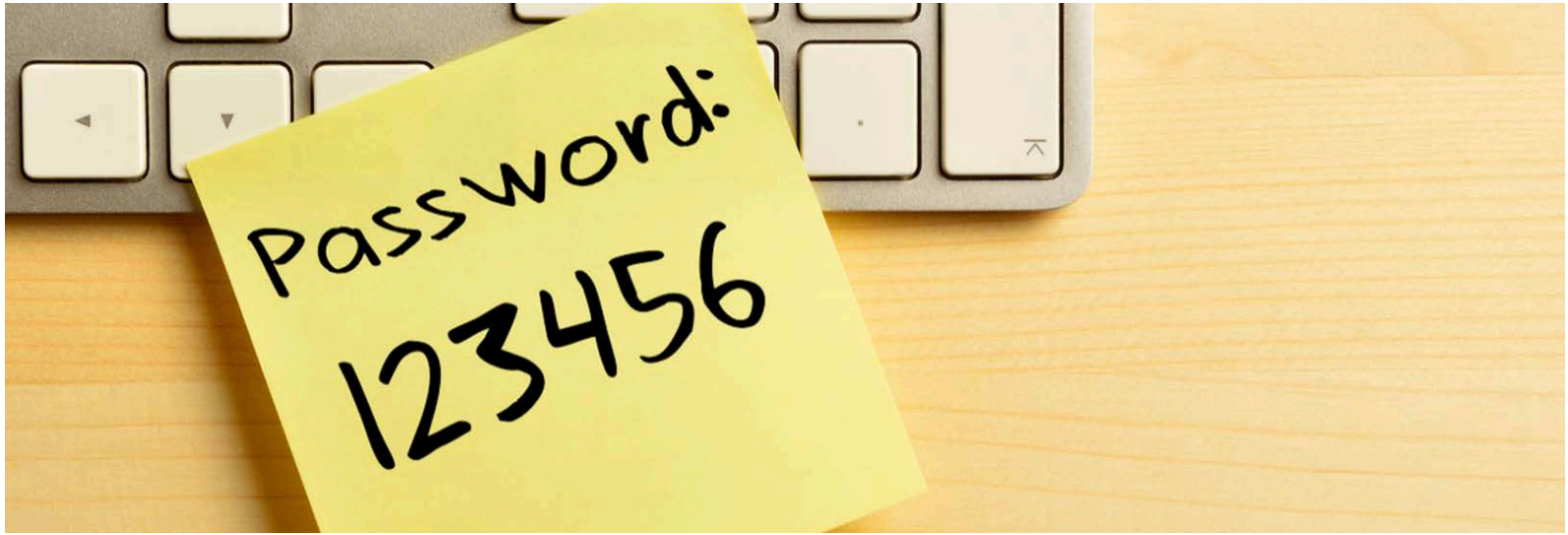
BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY HIDE FILTER



EVOLUTION OF AUTHENTICATION OPTIONS

Authentication Methods

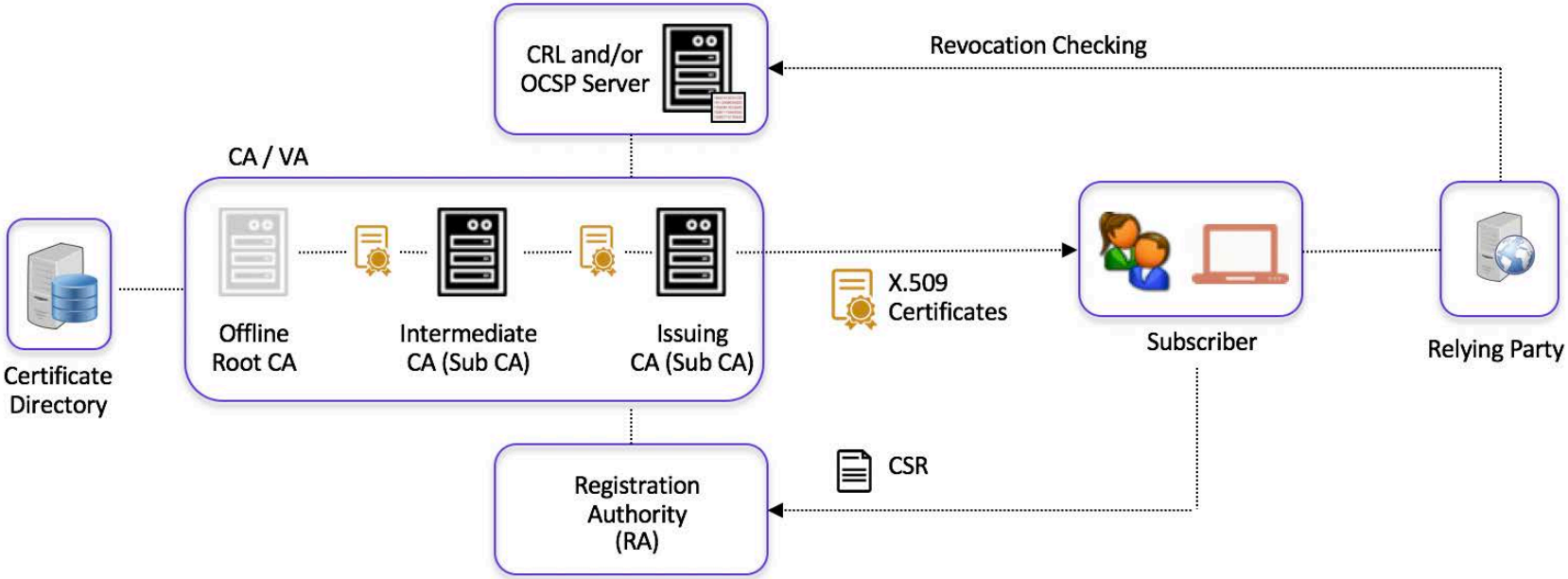
Authentication Methods – Evolution?



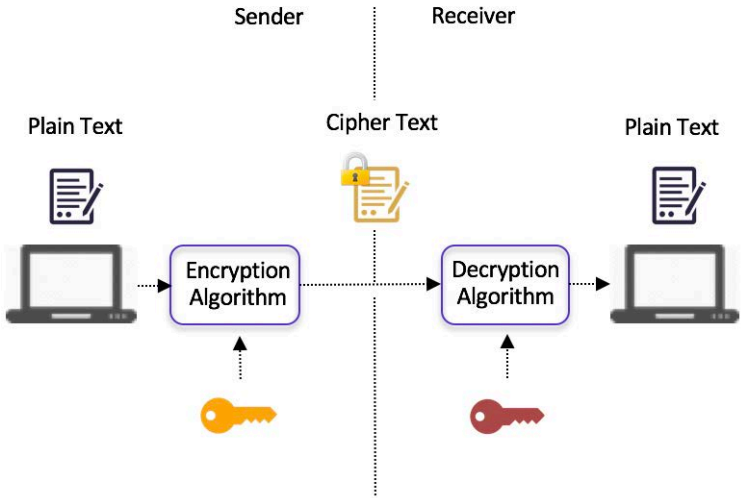
SEE THIS REGULARLY?

PKI-BASED AUTHENTICATION

PKI?

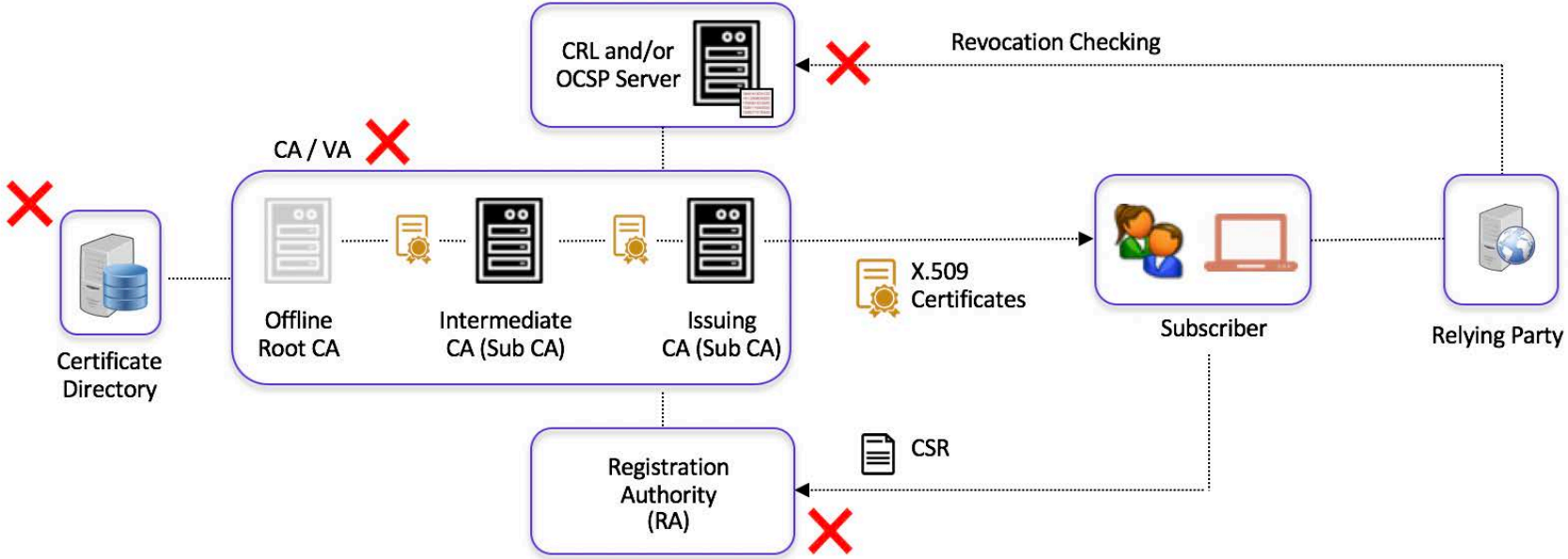

CRL and/or
OCSP Server
Revocation Checking
CA / VA
Offline
Root CA
Intermediate
CA (Sub CA)
Issuing
CA (Sub CA)
Certificate
Directory
X.509
Certificates
Subscriber
Relying Party
Registration
Authority
(RA)
CSR

PKI?



- Powered by asymmetric cryptography
- Most common algorithm: RSA
- Most popular algorithm today: ECDSA
- Public and private keys
- Widely used in SSL, Digital Signatures, Authentication

Traditional PKI Drawbacks



CAs are only as good as their systems, standards, and practices

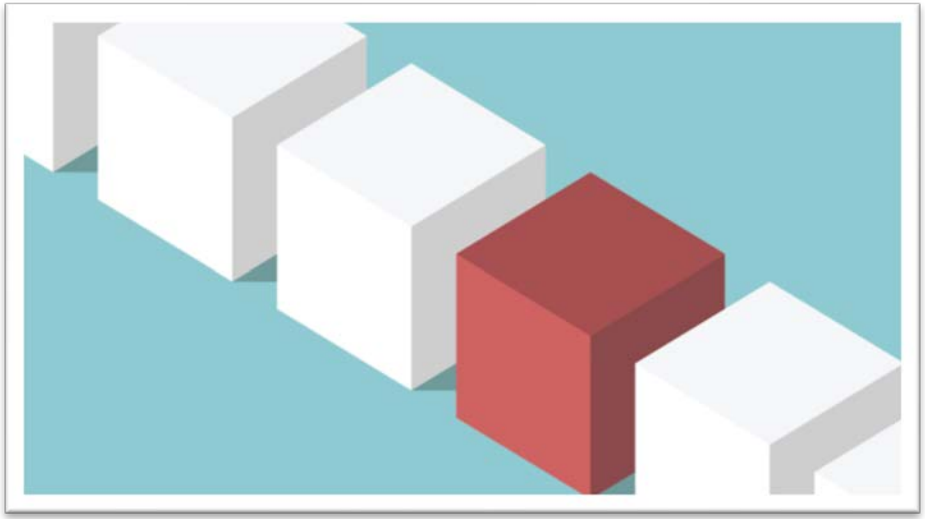
Traditional PKI Drawbacks

- Cryptographic Weaknesses
  - SHA1 already outdated, Quantum computer threats
- CA Issues, Architectural Issues
  - Unauthorized Certificates / CA compromise
  - CA mis-behaviors
  - DoS attacks, Path Validation Errors
- Lifecycle Issues
  - Unchecked Cert Provisions
  - Cert Expiry Control
  - Cert Management

Blockchain?

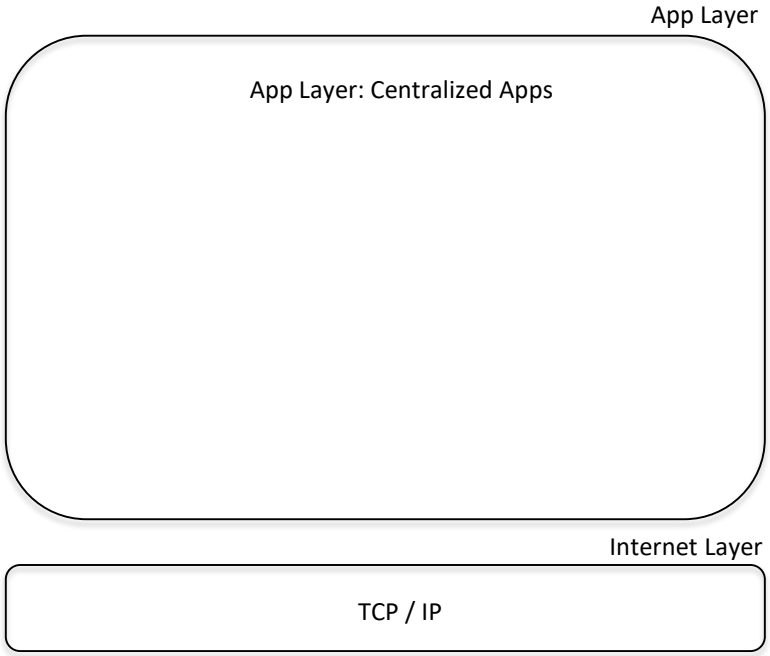

DECENTRALIZATION WILL CHANGE EVERY-THING.
SUCH AS?
WELL... FOR EXAMPLE, UM... THE BITCOIN AND THE ETHEREUM.
DID YOU RECENTLY READ AN ARTICLE?
SOME OF IT.
DILBERT.COM @SCOTTADAMSSAYS
©2018 Scott Adams, Inc./Dist. by Andrews McMeel
6-6-18

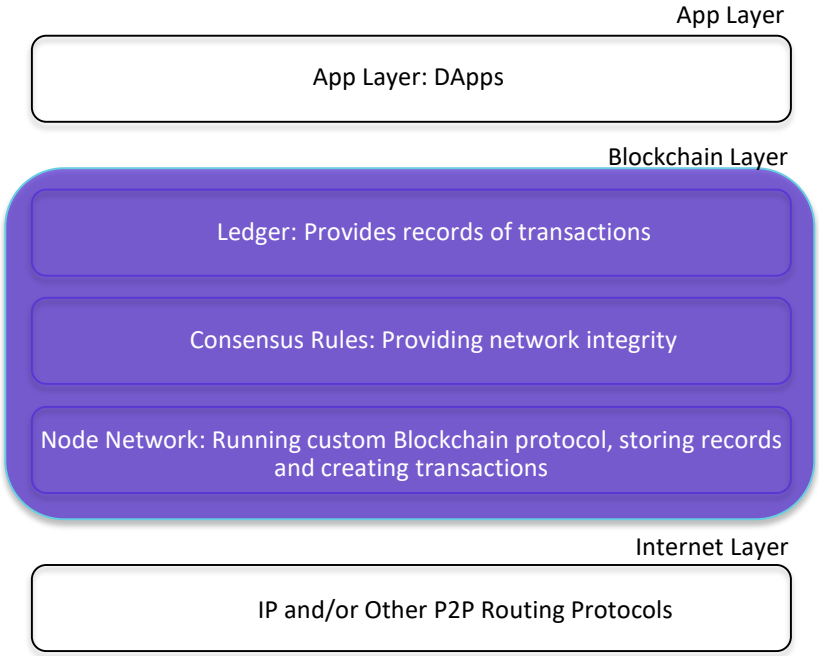
Blockchain?



- Cryptography
  - Integrity, Authenticity, Privacy
- Consensus
  - Decentralized protocol, transaction validators
- Ledger
  - Immutable record keeping
- Business Logic

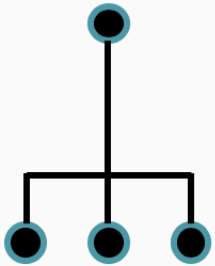
The stack(s)


App Layer
App Layer: Centralized Apps
Internet Layer
TCP / IP


App Layer
App Layer: DApps
Blockchain Layer
Ledger: Provides records of transactions
Consensus Rules: Providing network integrity
Node Network: Running custom Blockchain protocol, storing records and creating transactions
Internet Layer
IP and/or Other P2P Routing Protocols

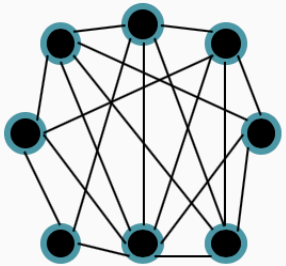
BLOCKCHAIN + PKI

Blockchain & PKI



Trust-by-Authority

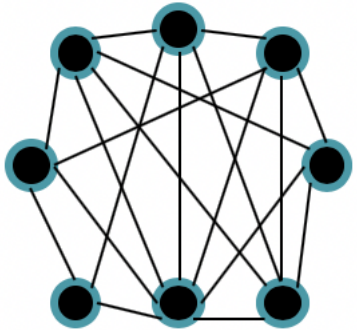
VS.



Trust-by-Computation

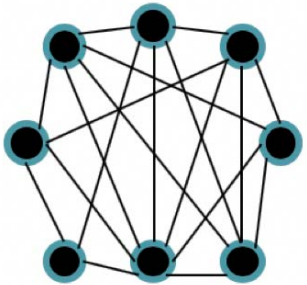
Blockchain & PKI

- Operated by a decentralized authority
- High Availability
- No or reduced* DoS possibility
- Resistant to unwanted modifications
- Can scale
- More opportunities for customizations (custom attributes)
- Quasi-anonymity since identities are represented as numbers

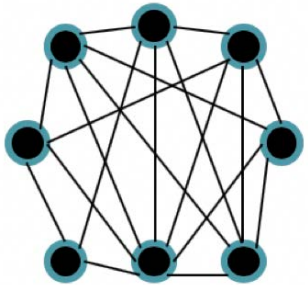


Trust-by-Computation

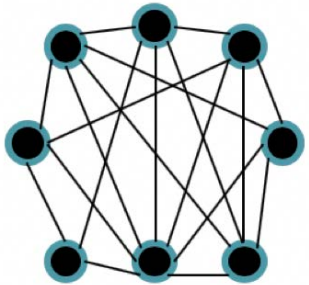
Consensus in a blockchain powered PKI



Proof Of Work



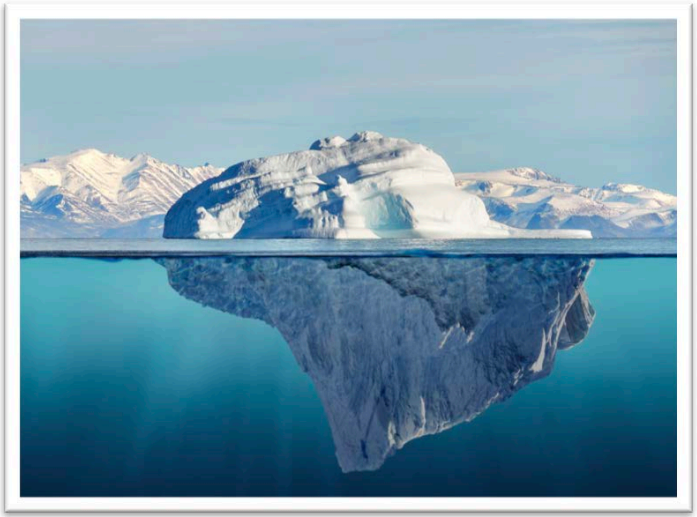
Proof Of Stake



Proof Of Service

Energy Use	High	Low	Low
Centralized/Decentralized	Tends to Centralize	Users remain in control of tokens	Users remain in control of tokens
Reqd. Tools	Mining Equipment	No Equipment	Some Equipment
Security	High	Normal	Normal

Blockchain & PKI



Cons

- Ledger control - if someone gets control of >50% mining power
- Still dependent on same algorithms/hash-functions as traditional PKI
- Could be wasteful unless optimized
- Compatibility with existing systems

CONCLUSION

Summary

- Users prefer usability over security
- If you are still using passwords as your primary authentication method, it's time to change that
  - For personal users, add 2FA!
  - For business users, improve your security posture
- PKI is a reliable technology (for the time being), it's the plumbing of the web
- Blockchain enables new trust models
- A combination of Blockchain + PKI addresses many security concerns in the traditional authentication space

Apply What You Have Learned Today

- Next week you should:
  - For your existing applications and/or systems, start reviewing your authentication policies and procedures
- In the first three months following this presentation you should:
  - Verify & Identify all weak links in your authentication methods. Replace Passwords!
  - Prioritize use-cases and identify gaps in your existing authentication initiatives
  - Consolidate and do a “clean-up” of your current PKI assets, certificates - if you are already using them
- Within six months you should:
  - Upgrade your legacy PKI implementations, consider computational-trust PKI over authority trust
  - Focus on lifecycle management of certificates and keys