AN INTRODUCTION TO BLOCKCHAIN

NOVEMBER 2017

RYAN R. FOX
MARC G. SMITH

- BLOCKCHAIN EXPERT CONSULTING
- TECHNICAL ARCHITECTURE & DESIGN
- BUSINESS IMPACT ANALYSIS
- PROOF-OF-CONCEPT & PILOT PROJECT MGMT
- EDUCATION & TRAINING

Ryan R. Fox | ryan@vativ.io | Boston

- Blockchain Professional
- Professional Scrum Master

Marc G. Smith | marc@vativ.io | Minneapolis

- Transaction Processing / Business Process Management expert
- Enterprise software leader: IBM, Lombardi, Trilogy

3 QUESTIONS TO GET STARTED …

1

What are some business operations that rely on trusted 3rd parties?

Some examples?

- Banking & payments … *banks*
- Securities trading … *brokerages*
- Real estate … *title companies*
- Voting, taxes … *governments*
- Royalties … *publishing houses*
- Healthcare claims … *benefits administrators*

3 QUESTIONS TO GET STARTED …

2

What are some issues with these business scenarios that rely on intermediaries?

Some examples?

- Slow … *e.g., 1-3 days to settle transactions*
- Costly … *transaction fees can be significant*
- Disputes … *due to lack of transparency & tracking*
- Security … *open to hacking & unauthorized access*
- Fraud … *open to identity theft, forged transactions*

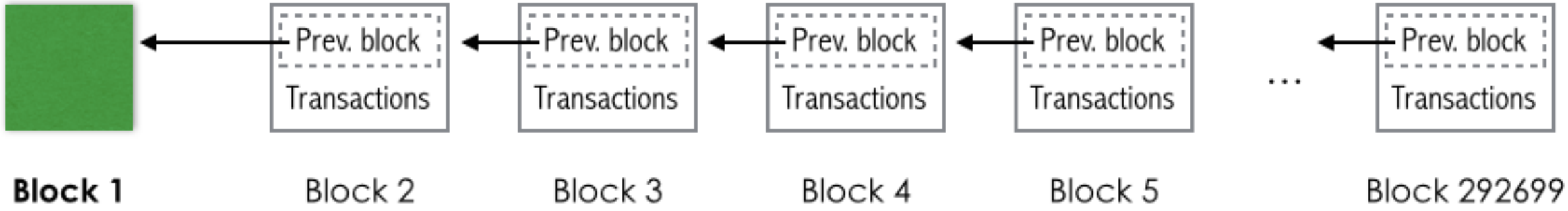
3 QUESTIONS TO GET STARTED …

3	**What if there was "a better way" that relied on technology vs. trusted 3rd parties?**

Blockchain technology *was invented to replace the need for trusted 3rd parties.*

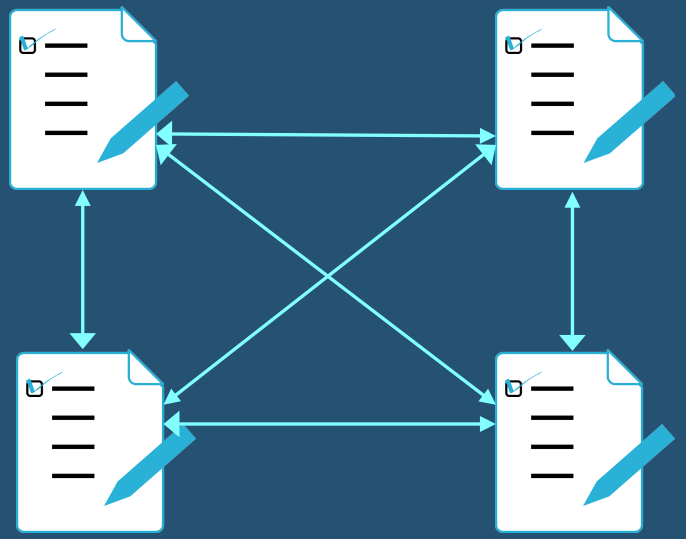
WHAT IS A BLOCKCHAIN?

Transaction Log



Distributed

Replicated



Very Secure

WHAT IS A BLOCKCHAIN?

A very secure, distributed, replicated transaction log:

- digital ledger of asset ownership & exchanges
- openly-shared, append-only “single version of the truth”
- not owned & managed by a “trusted 3rd party”
- nearly “hack proof” using cryptographic technology

COURSE OUTLINE

DAY 1

Blockchain Basics

- What is a Blockchain?
- Origins
- State of Blockchain Today
- Concepts – User Point of View
- Concepts – System Point of View
- Example Use Cases
- Live Demos
- Q&A

DAY 2

Deeper Dive

- Cryptographic Signing
- Consensus Protocols
- Scaling / Performance
- Smart Contracts
- Off-chain Work / Assets
- Oracles / Cryptlets
- Platform Comparison
- Q&A

DAY 3

Hands-On Lab

- Blockchain-as-a-Service on Azure
- How to set up the network
- Dashboard / controls
- How to code smart contracts
- Executing transactions
- Examining results
- Q&A

BLOCKCHAIN BACKGROUND

ORIGINS IN BITCOIN

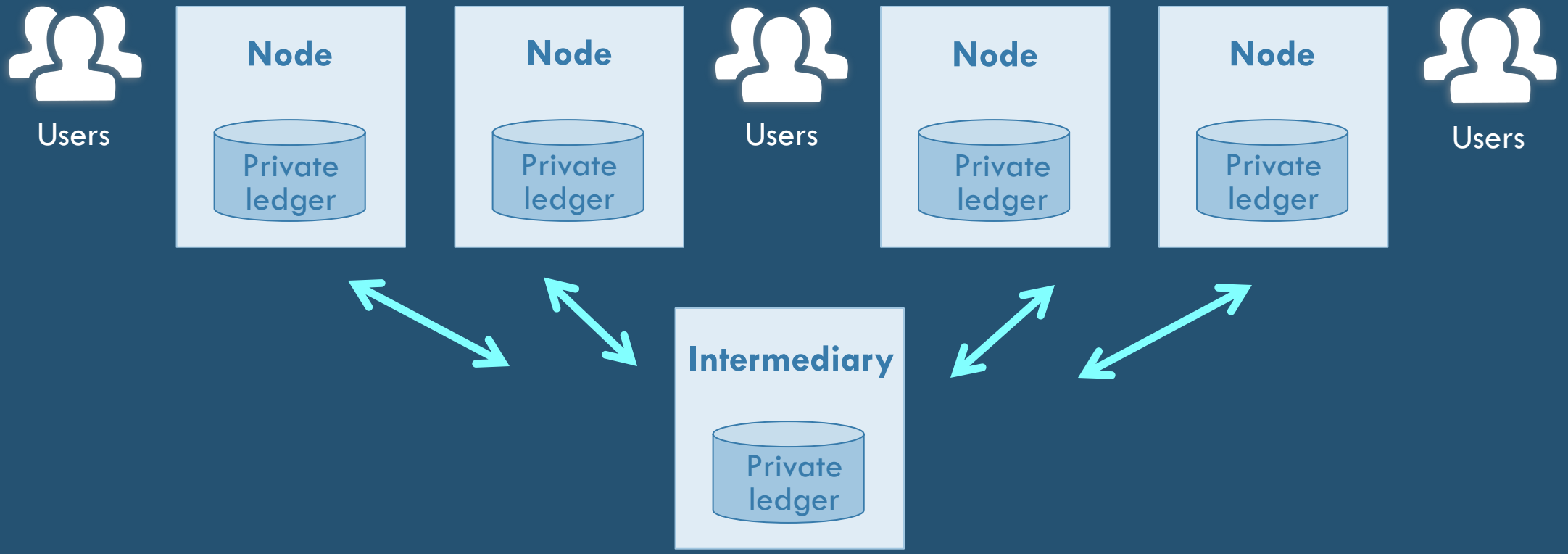
"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

- Satoshi Nakamoto, 2008

"Bitcoin: A Peer-to-Peer Electronic Cash System."
https://bitcoin.org/bitcoin.pdf

THE WORLD BEFORE BLOCKCHAIN

Multiple parties transacting business on a network …

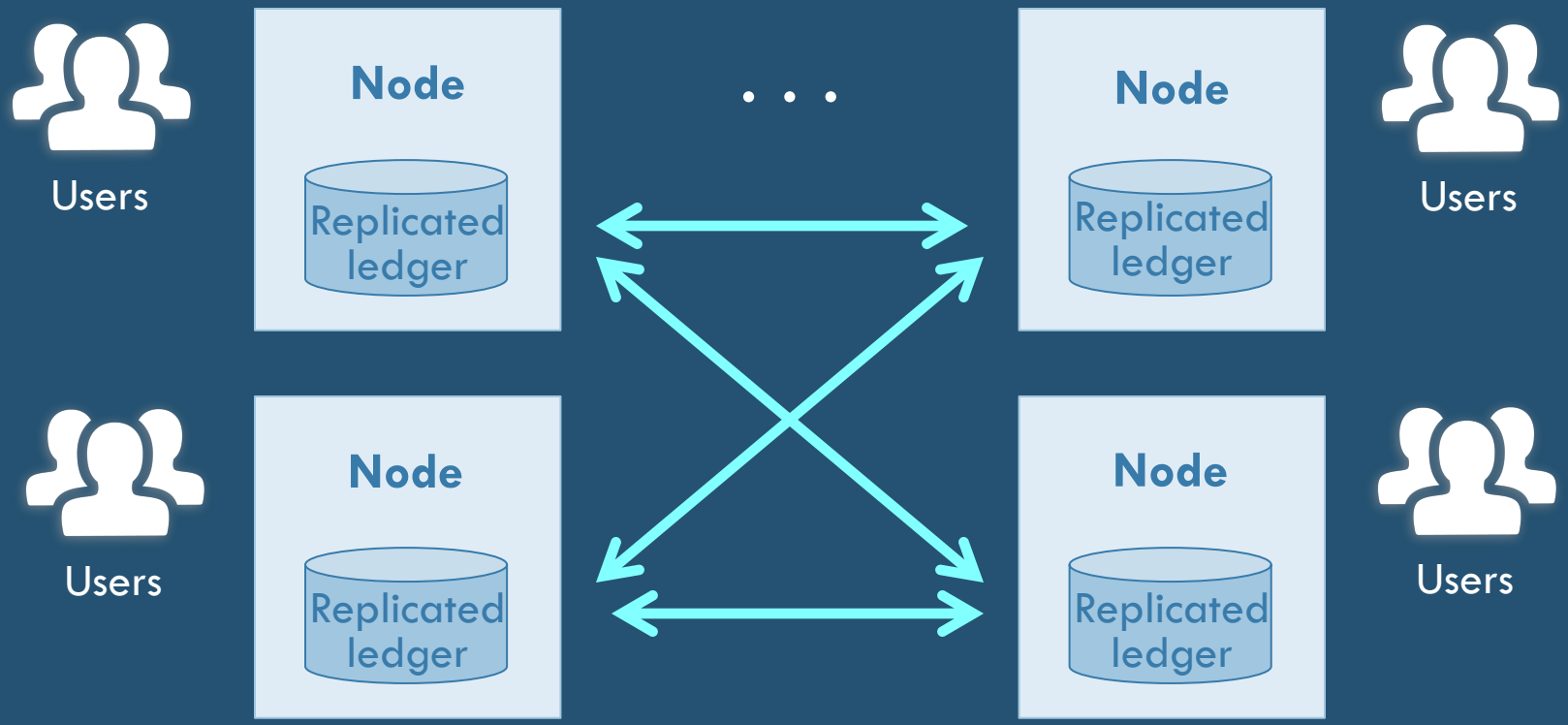


Inefficiencies / Delays
Extra Transaction Costs
Security Exposures

… through 3rd-party intermediaries
(banks, brokerages, clearinghouses, etc.)

A BLOCKCHAIN IS A NEW KIND OF TRANSACTION LEDGER

Multiple parties transacting business on a network …



No Intermediaries
No Delays
Secure by Consensus

… sharing & co-validating a replicated, cryptographically-secure ledger

BLOCKCHAIN EVOLUTION

"Distributed Ledger Technology (DLT)"

- **Blockchain 1.0**
  - Bitcoin – system for digital cash exchange
- **Blockchain 2.0**
  - Platforms for "Distributed Apps" – Ethereum, Quorum, …
  - Smart Contracts – programmable business logic for transactions
  - Configurable consensus algorithms
- **Blockchain Enterprise**
  - Enterprise application platforms – Hyperledger & Sawtooth, Microsoft Coco, EOS.IO, Corda …
  - Scaling, Performance, Interoperability, Integrations
  - Specialized hardware and cloud-computing environments

GOOD QUESTION TO ASK …

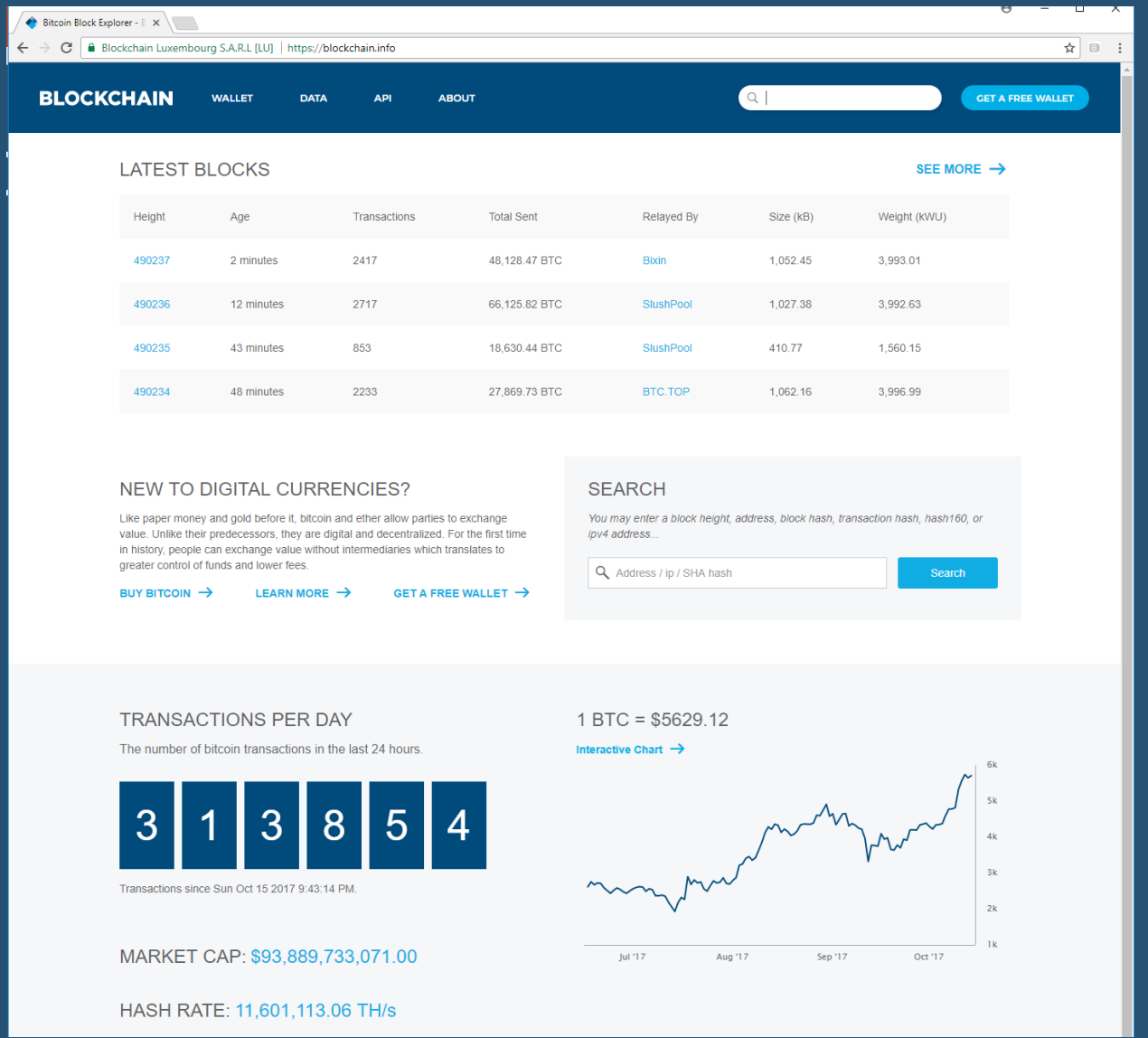
“DO YOU *REALLY* NEED A BLOCKCHAIN?”

WHAT USE CASES ARE WELL-SUITED FOR BLOCKCHAIN?

- Exchange of data / assets between multiple parties across value-chain network
- Siloed systems-of-record across value-chain
- Lack of transparency of exchange / ownership
- Reconciliation of exchanges may be performed by trusted third-party authorities
- Processing today is “manual”, error-prone, time-consuming

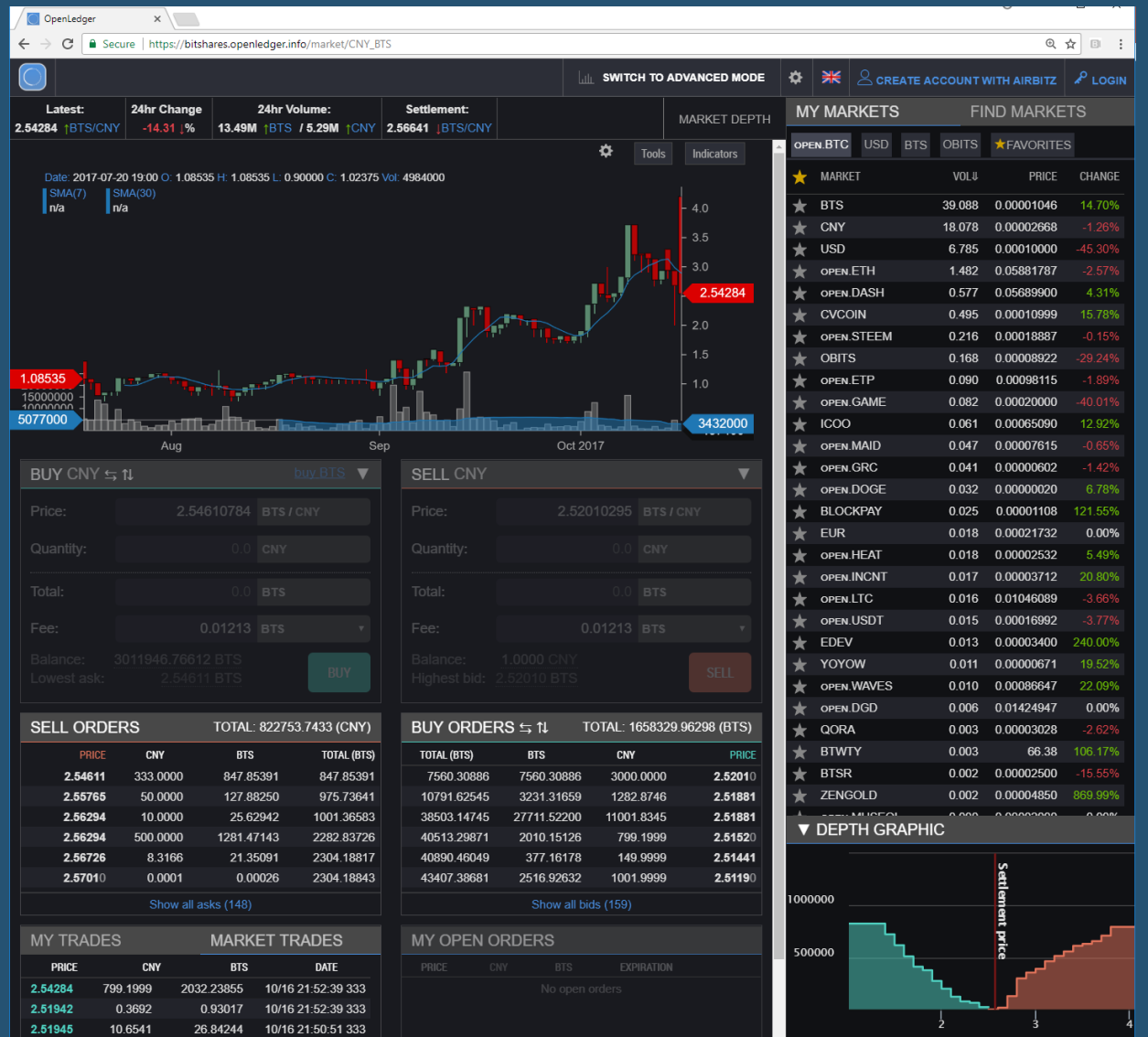
WHAT DOES A BLOCKCHAIN LOOK LIKE?

Digital Currency & Payments



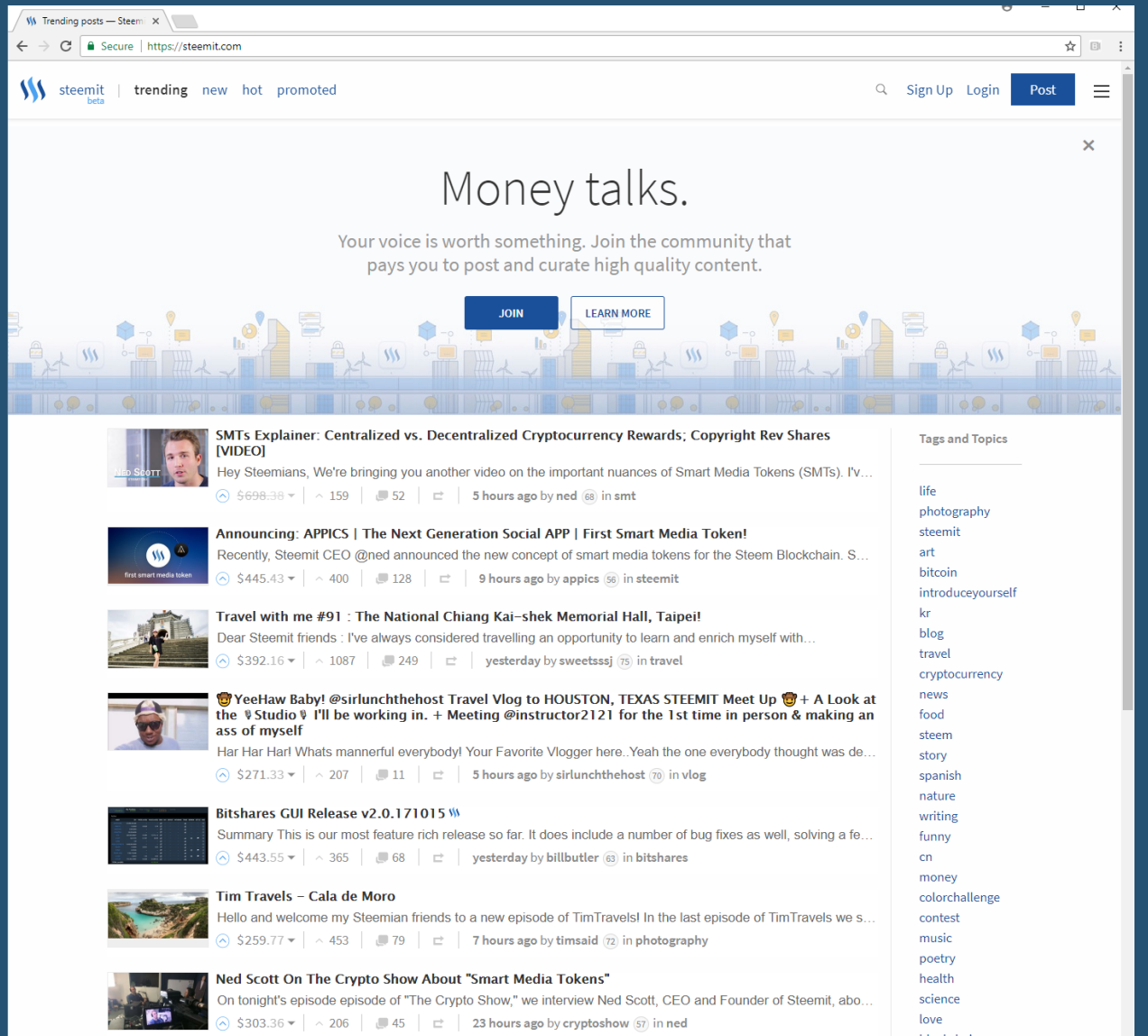
WHAT DOES A BLOCKCHAIN LOOK LIKE?

Digital Exchange Marketplace



WHAT DOES A BLOCKCHAIN LOOK LIKE?

Digital Content Distribution



BENEFITS OF BLOCKCHAIN

Better Security	• Nearly "hack-proof" value transfer using public key encryption & consensus validation
Better Transparency & Trust	• Complete history of transactions, validated and replicated to all participants
Better Efficiency	• Reduce settlement from days → hours/minutes/seconds: No centralized, 3rd-party "middlemen"
Better Integrity	• Avoids missing or duplicate actions … no "double spend"
Better Fault Tolerance	• Many full replicas of ledger across peer-to-peer network

"STATE OF BLOCKCHAIN" (CONSENSUS 2017)

Blockchain is Taking Off

Lots of investment

- Big-name users
  - Citi, Nasdaq, Fidelity, MetLife, Govt, …
- Investors, large & small
  - VCs, individuals, …
- Software vendors, large & small
  - IBM, MSFT, startups, …
- Consultants, large & small
  - PwC, KPMG, Cognizant, …

“STATE OF BLOCKCHAIN” (CONSENSUS 2017)

Blockchain is Taking Off

Blockchain is Still Complex

Lots of new Blockchain concepts & lingo

- Need to learn a new “mental model”

Lots of different Blockchain / DLT variations

- Not just one thing to learn

Sophisticated technology – for developers

- Lots of coding
- Few if any business-friendly tools

"STATE OF BLOCKCHAIN" (CONSENSUS 2017)

Blockchain is Taking Off

Blockchain is Still Complex

Blockchain is Still Emerging

- Outside of the Bitcoin universe, many people still haven't heard of / don't understand Blockchain
- The industry is still in the "creative thinking" phase vs. "convergent thinking"
  - New inventions, startups, announcements, investors, …
- Performance / scalability / cost is a big concern
- Usability / manageability is a big concern
- Lots of experimentation vs. real production systems

→ 2017:	"Year of the Trailblazers"
2018 – 2020:	"Real" Adoption Ramp Up
2020 – 2022:	"Mass" Adoption
202x:	Latecomers / Followers

Now is the time to get ahead of the wave …

BLOCKCHAIN AT LOCAL COMPANIES

UNITEDHEALTH GROUP® / OPTUM®	Rajeev Cyrus, Director of Blockchain Platform and Applications Development Jeremy McNevin, SW Engineer Blockchain Technology (IBM HyperLedger)
usbank	Christopher Swanson, Program Mgr, Enterprise Blockchain R&D Karina Taylor, Business Intelligence Strategy
ADVANTUS® | CAPITAL MANAGEMENT	Lisa Perrin, Investment Technology Consultant, *Securian Blockchain Committee*
Medtronic	Timothy Paffel, Sr Prin IT Technologist (has done a Blockchain POC)
LAND O'LAKES, INC.	Jonathan Brandt, Executive Project Consultant
bluestem brands, inc.	Jared Olhoft, Software Engineer (in 2015 had an LLC focused on Cryptocurrencies)
THOMSON REUTERS	Joseph Raczynski, Technology Manager & Blockchain Evangelist
TARGET	Andrew Schneider, Sr UI Engineer (interested in Blockchain & cryptocurrencies)

QUESTIONS?

BLOCKCHAIN CONCEPTS – USER POINT-OF-VIEW

Alice

Bob

Charlie

Mallory

WHAT'S IN YOUR WALLET

- Drivers License
- SSN Card
- Checkbook

Identity

Transferability

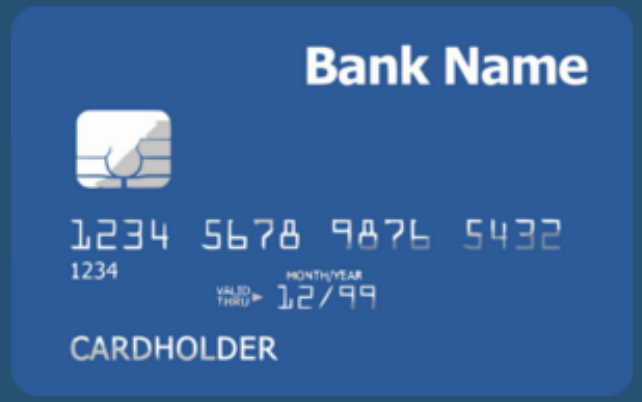
Validity

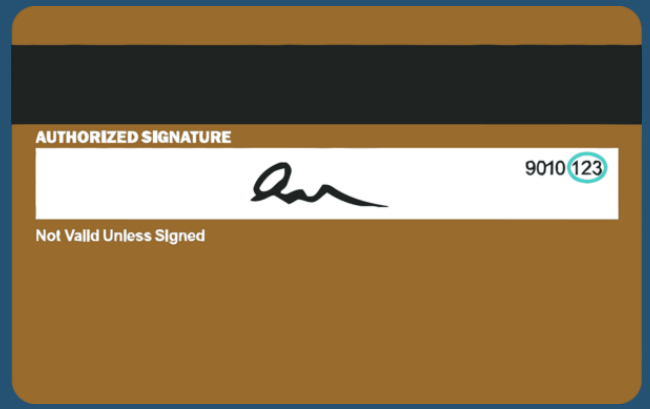
WHAT'S IN YOUR WALLET

NUMBER OR CODE	DATE	TRANSACTION DESCRIPTION	PAYMENT, FEE, WITHDRAWAL (-)		✓	DEPOSIT, CREDIT (+)		$ BALANCE	
	3/1/17	Beginning Balance						973	82
2115	3/1/17	Brightview Apts - Rent	425	00				548	82
DC	3/2/17	McDonald's	8	75				540	07
ATM	3/2/17	Cash Withdrawal	60	00				480	07
AP	3/3/17	Verizon - Phone Bill	70	05				410	02
AD	3/3/17	ABC Company - Paycheck				1,025	57	1,435	59
FT	3/4/17	Transfer to Savings	100	00				1,335	59
2116, TD	3/5/17	Red Cross Donation	50	00				1,285	59

Identity Transferability Validity

WHAT'S IN YOUR WALLET





Identity

Transferability

Validity

WHAT'S IN YOUR WALLET

- Drivers License
- SSN Card
- Checkbook
- Bank Card

- Paper Currency

Identity

Transferability

Validity

WHAT'S IN YOUR WALLET

Identity

Transferability

Validity

WHAT'S IN YOUR WALLET

- Drivers License
- SSN Card
- Checkbook
- Bank Card

- Paper Currency
- Coin Currency
- Loyalty Card
- Stock Certificate

Identity

Transferability

Validity

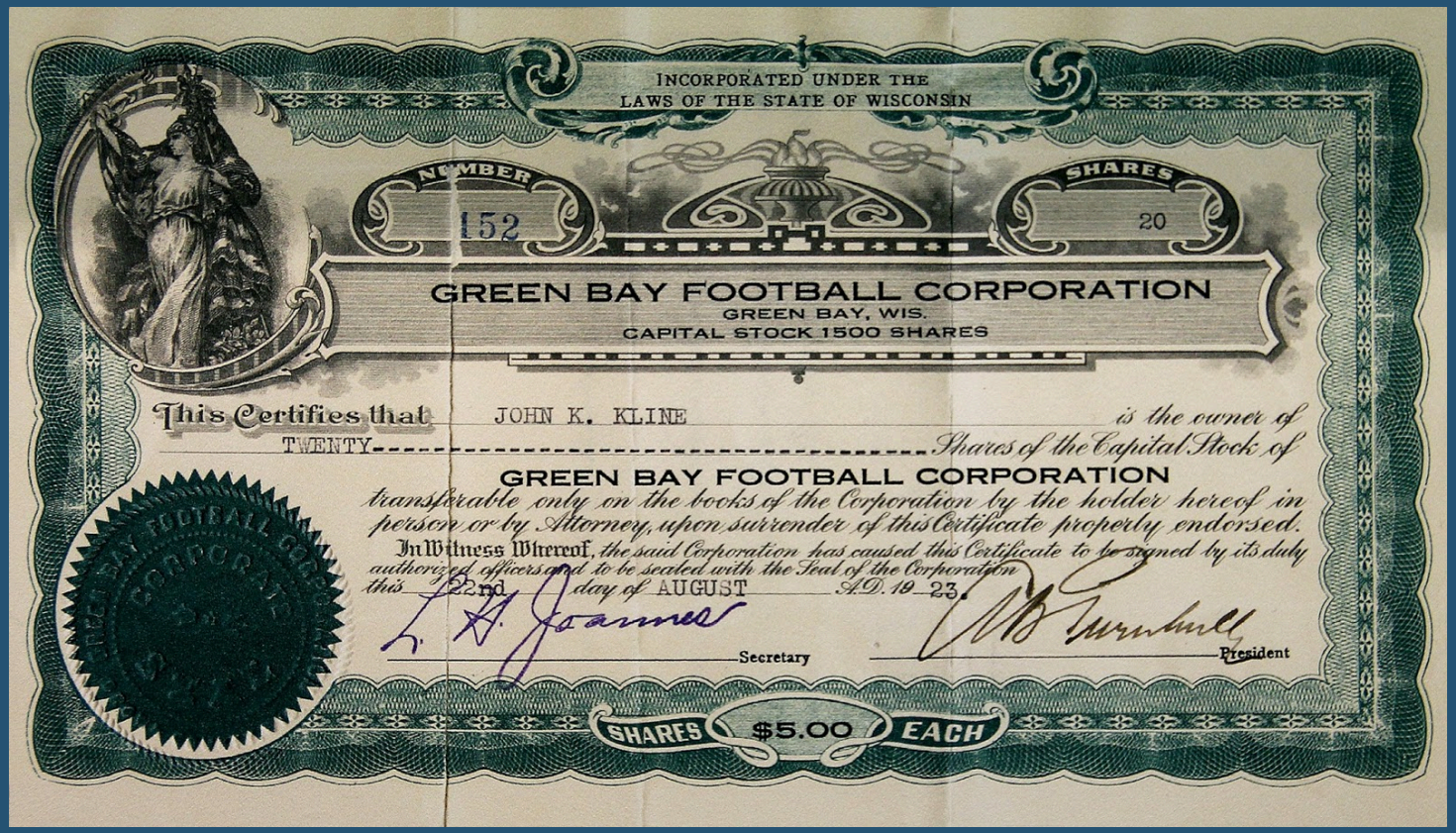
WHAT'S IN YOUR WALLET

Identity

Transferability

Validity

WHAT'S IN YOUR WALLET


INCORPORATED UNDER THE
LAWS OF THE STATE OF WISCONSIN

NUMBER 152

SHARES 20

GREEN BAY FOOTBALL CORPORATION
GREEN BAY, WIS.
CAPITAL STOCK 1500 SHARES

This Certifies that JOHN K. KLINE is the owner of
TWENTY Shares of the Capital Stock of
GREEN BAY FOOTBALL CORPORATION
transferable only on the books of the Corporation by the holder hereof in person or by Attorney, upon surrender of this Certificate properly endorsed.
In Witness Whereof, the said Corporation has caused this Certificate to be signed by its duly authorized officers and to be sealed with the Seal of the Corporation this 22nd day of AUGUST A.D. 19 23.

Secretary

President

SHARES $5.00 EACH

Identity

Transferability

Validity

WHAT'S IN YOUR WALLET

- Drivers License
- SSN Card
- Checkbook
- Bank Card

- Paper Currency
- Coin Currency
- Loyalty Card
- Stock Certificate

Identity Exchange Method Asset Contract

EXCHANGE METHODS

- Cash
- Bank Card
- Loyalty Card
- Foreign Exchange
- Market

TRUST

SHORTCOMINGS OF EXISTING EXCHANGE METHODS

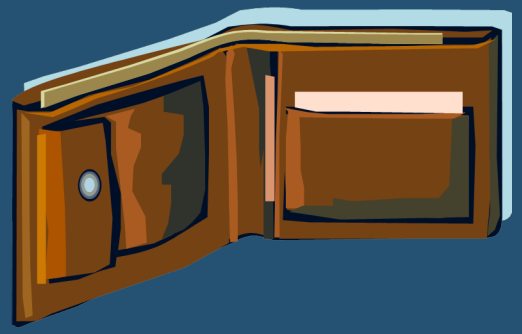
- Cash
- Bank Card
- Loyalty Card
- Foreign Exchange
- Market

- Slow, costly settlement
- Centralized
  - Silos
  - Opaque
  - Trusted intermediaries
- Error, fraud prone

Is there a better way?

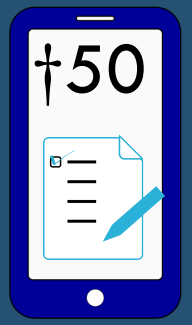
COMPARING PHYSICAL WORLD TO BLOCKCHAIN

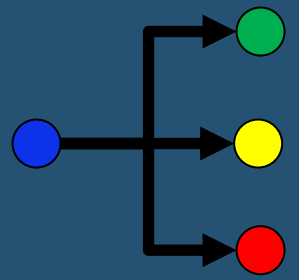
- Physical Wallet
  - Exchange Methods
  - Identities



  - Assets
  - Contracts

- Digital Wallet
  - Exchange Methods
  - Key pairs
    - Private key
    - Public key
  - Digital Assets, Tokens, Coins
  - Smart Contracts



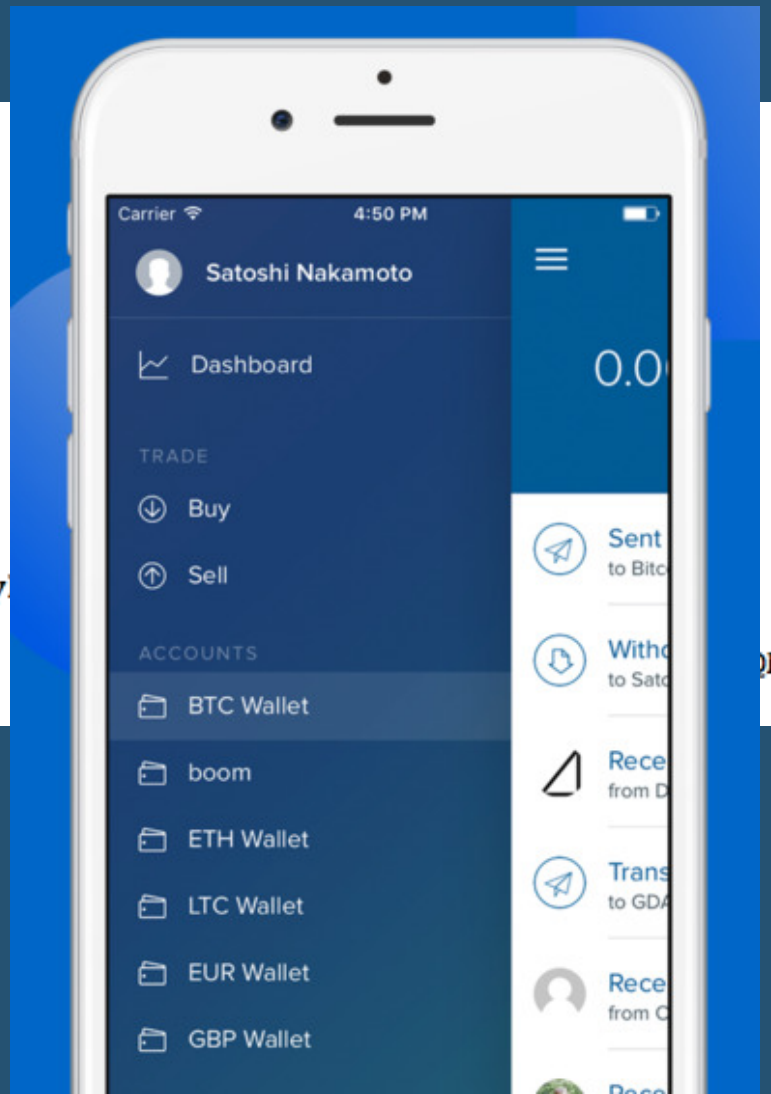


COMPARING PHYSICAL WORLD TO BLOCKCHAIN

Public Address

SHARE

16NZD9iBCbj8NwWrDZnnywpuqTdJtv7y

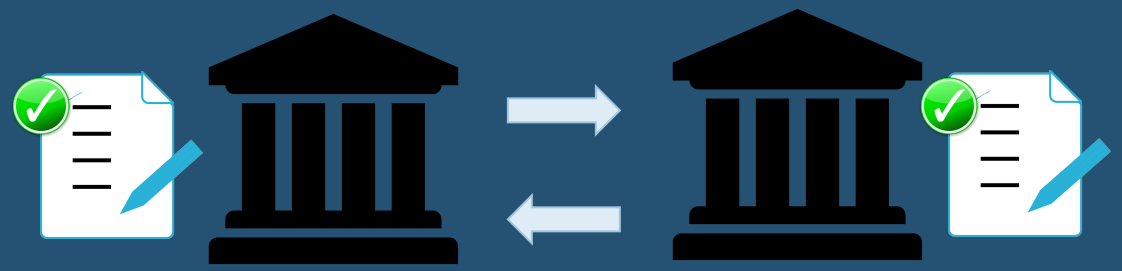


Private Key (Wallet Import Format)

SECRET

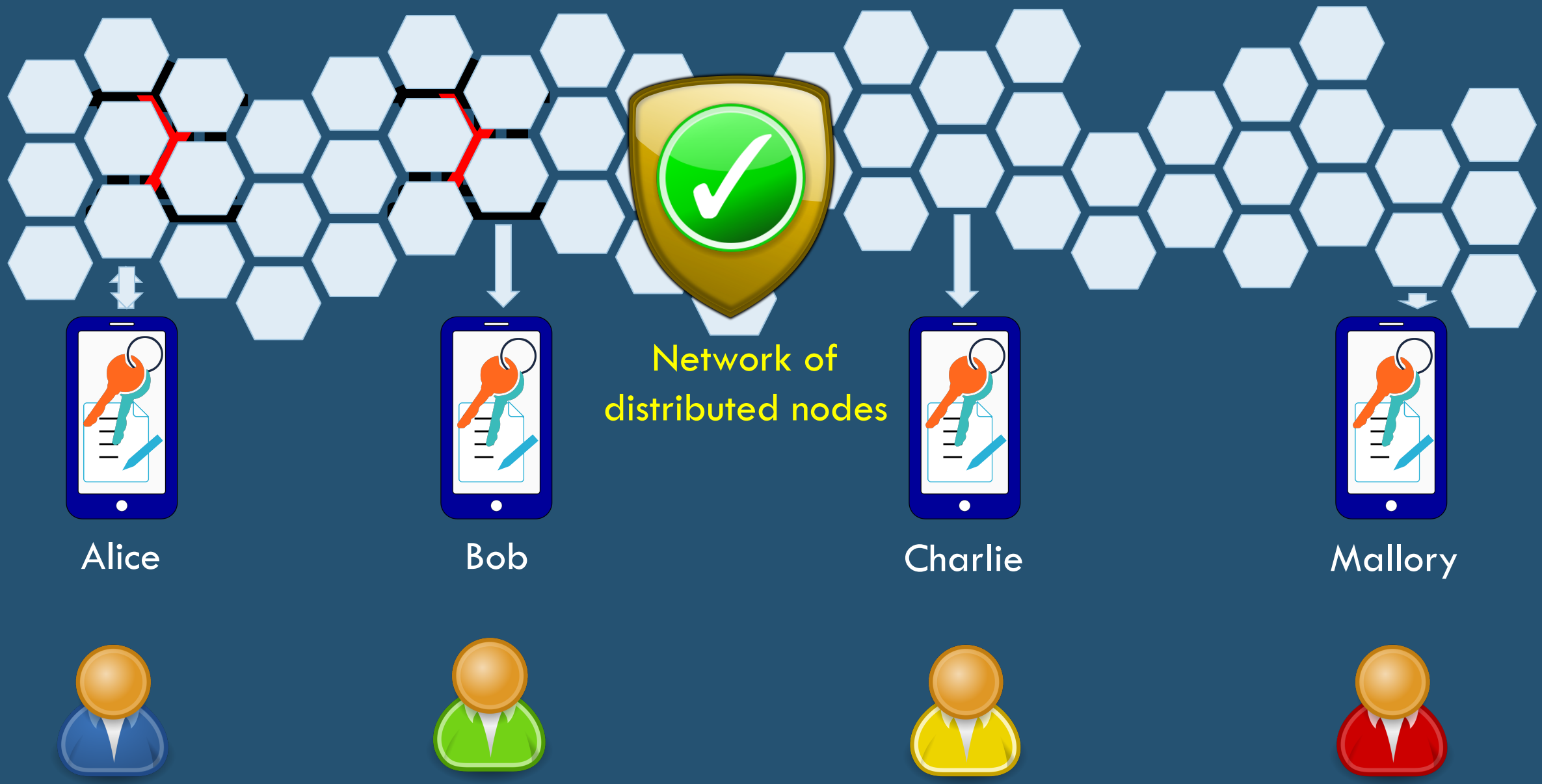
MezBd53zTHp7urRrqC75GG7f5vaEuXgyFfH3DiSg

EXAMPLE: BANKING TRANSFER

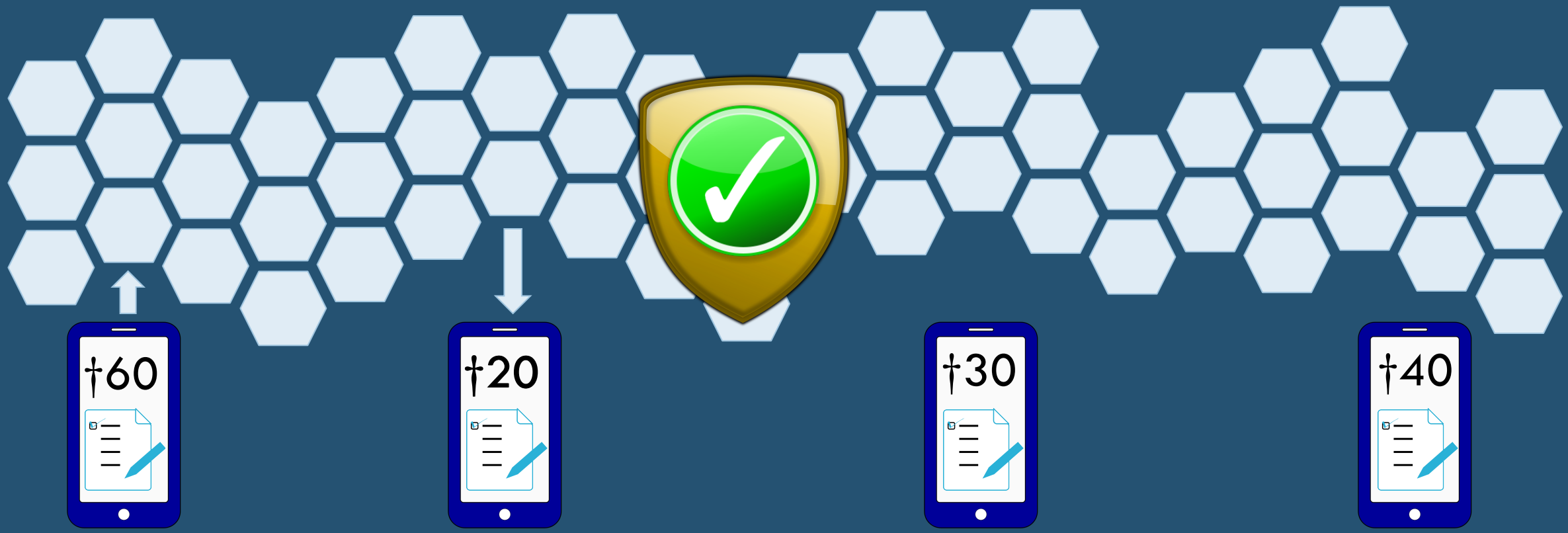


Alice → Bob Charlie Mallory

EXAMPLE: BLOCKCHAIN TRANSFER



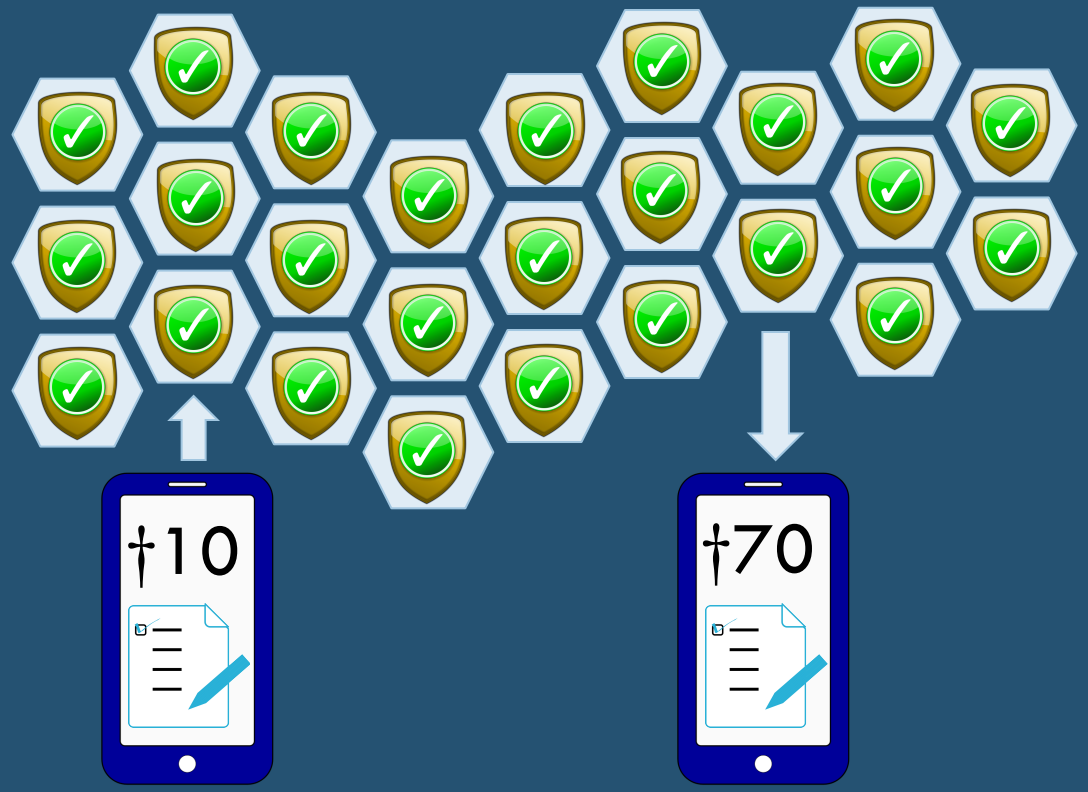
EXAMPLE: BLOCKCHAIN TRANSFER



I ALICE, transfer 30 TOKEN to BOB, signed ALICE

EXAMPLE: NETWORK VALIDATION

EXAMPLE: NODE VALIDATION



Mining Node

[…]

A → B 30 TOKEN

A → B 20 TOKEN

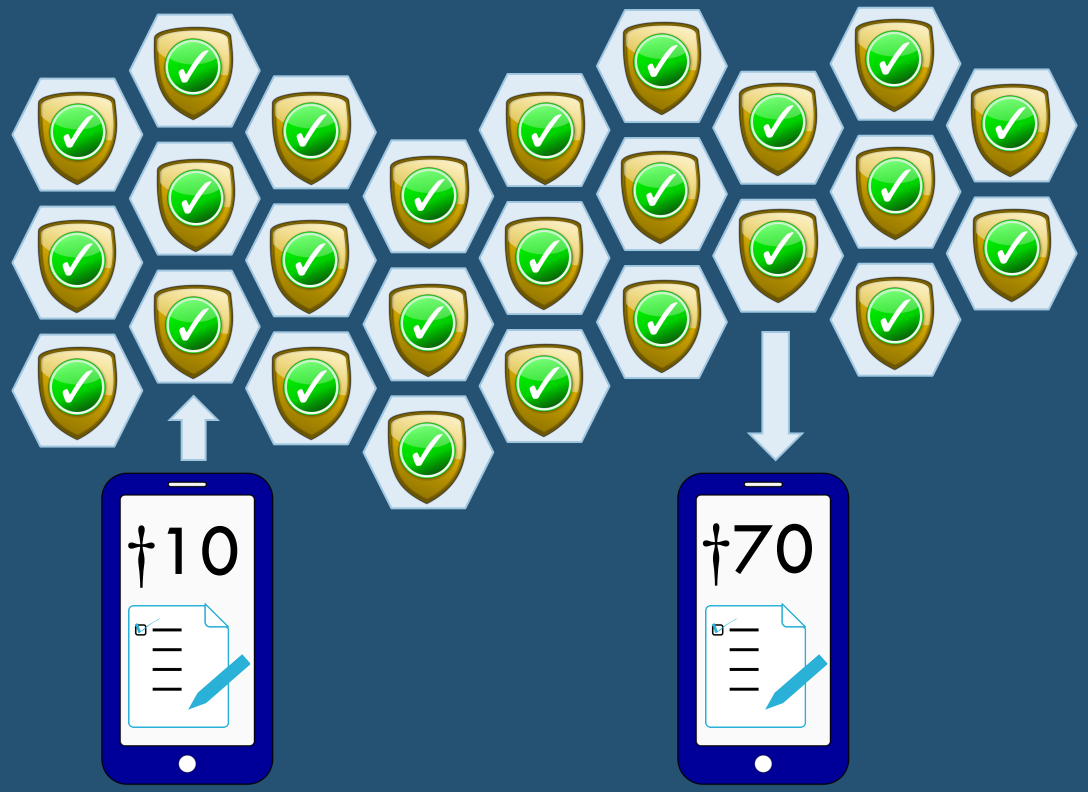
A → B 10 TOKEN ?

Replicated Ledger

Received 10 TOKEN from ALICE

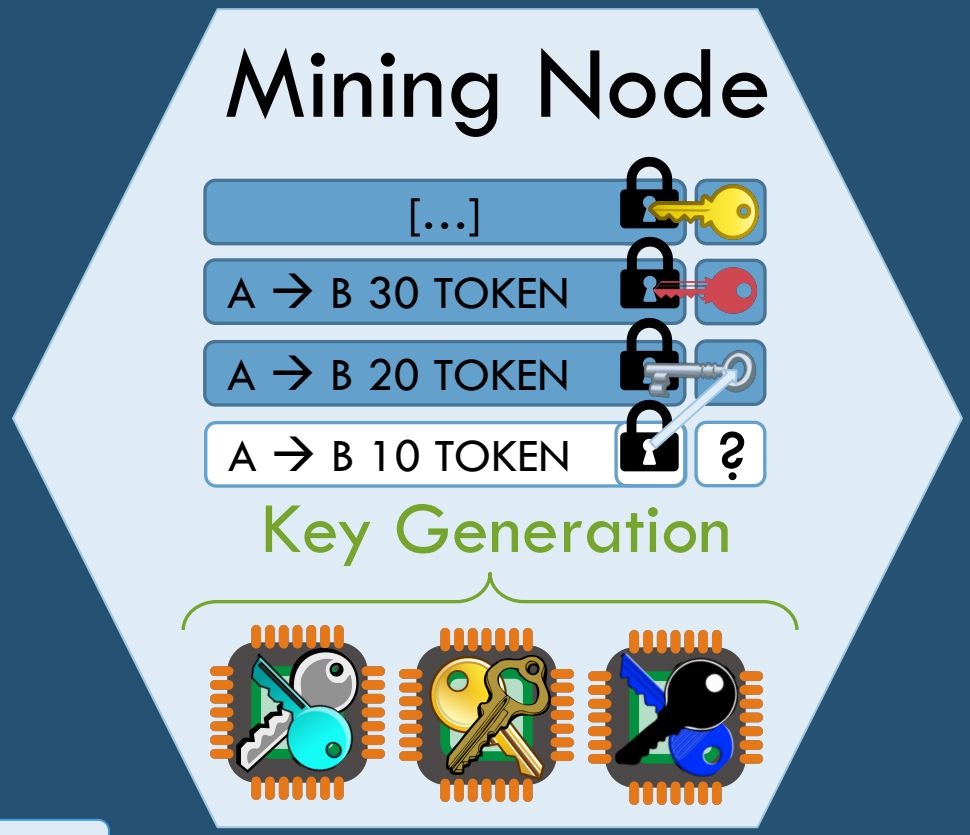
I ALICE, transfer 10 TOKEN to BOB, signed ALICE

EXAMPLE: NODE VALIDATION



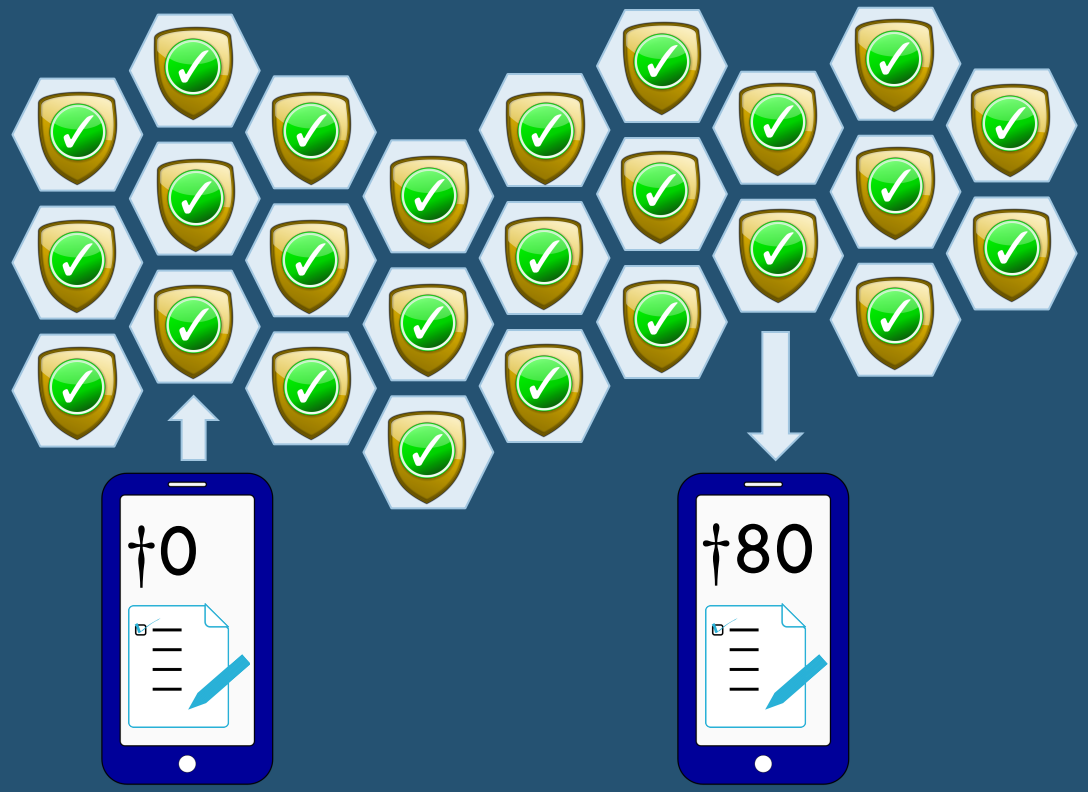
Received 10 TOKEN from ALICE

I ALICE, transfer 10 TOKEN to BOB, signed ALICE



Competition to append valid transactions

EXAMPLE: NODE VALIDATION

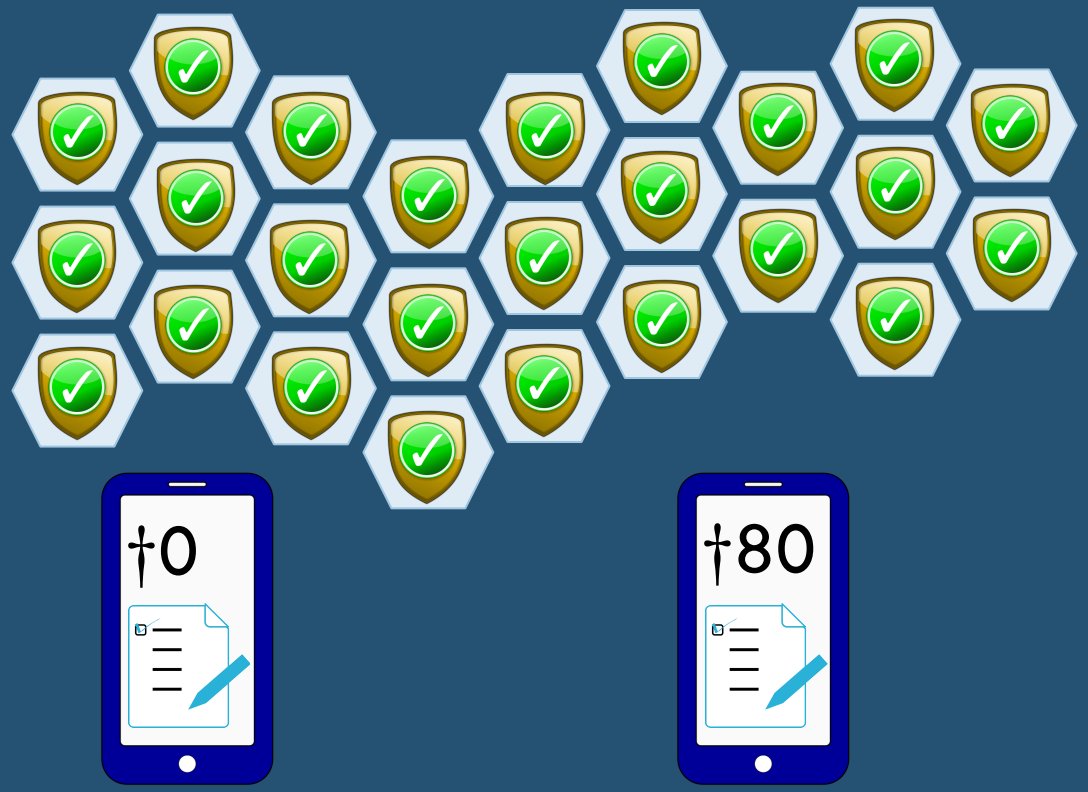


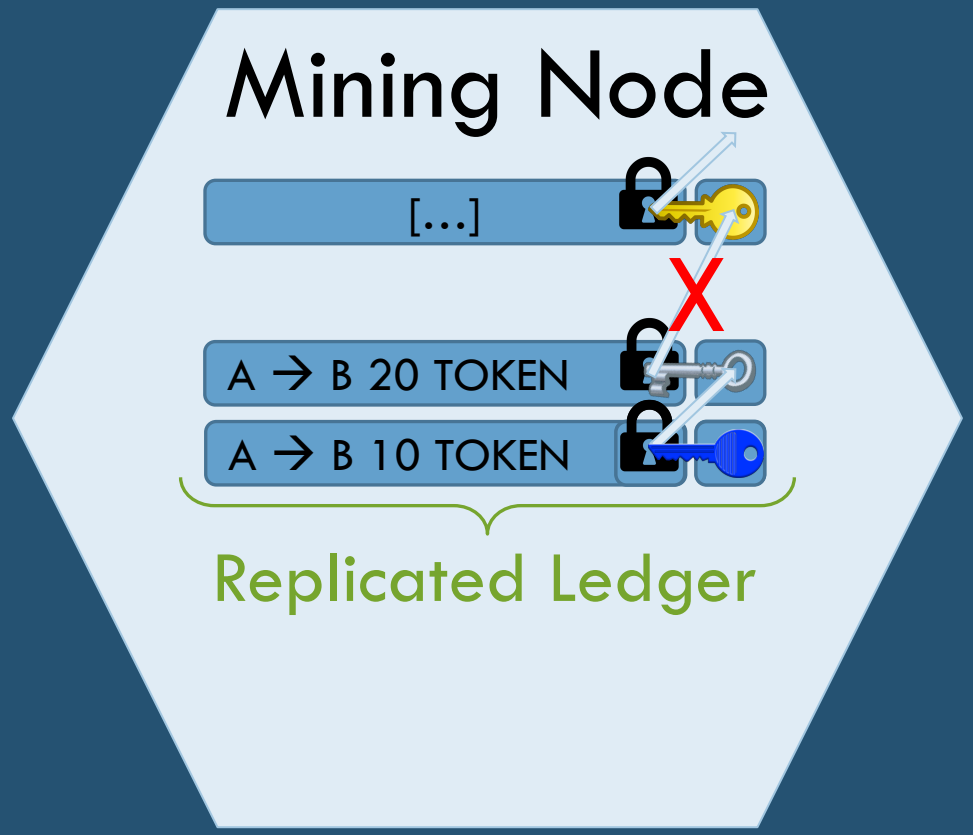
Received 10 TOKEN from ALICE

I ALICE, transfer 10 TOKEN to BOB, signed ALICE

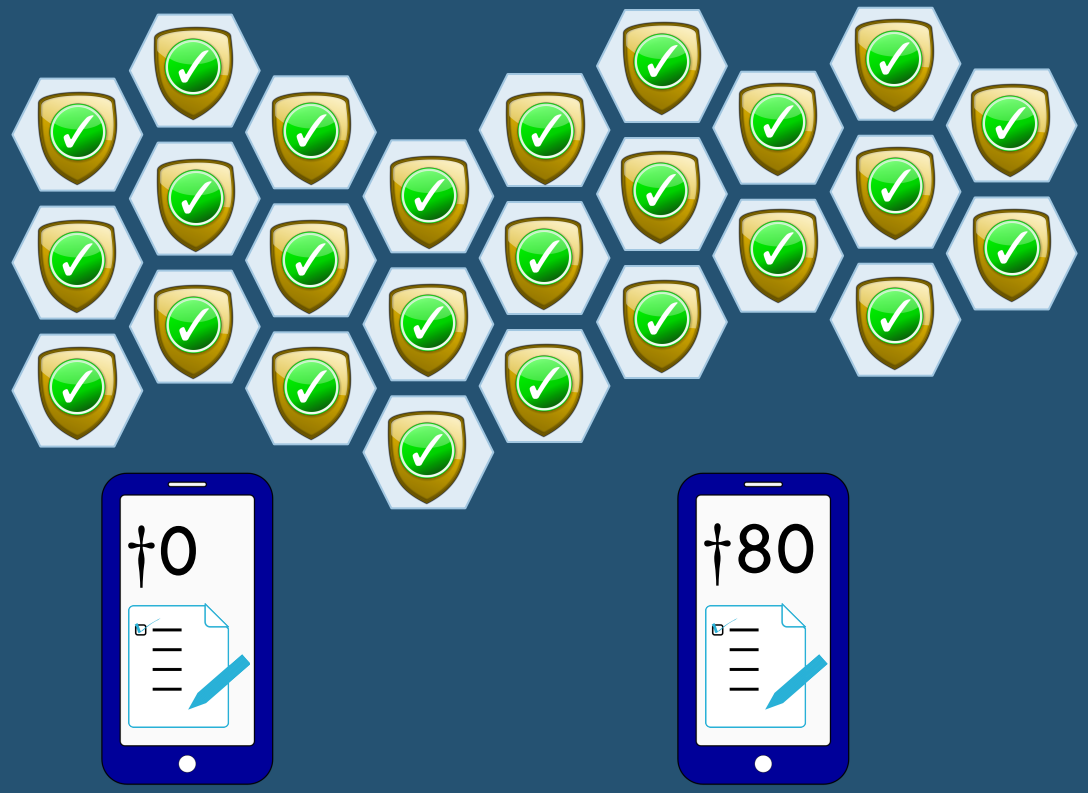
Winning node is rewarded for generating correct key

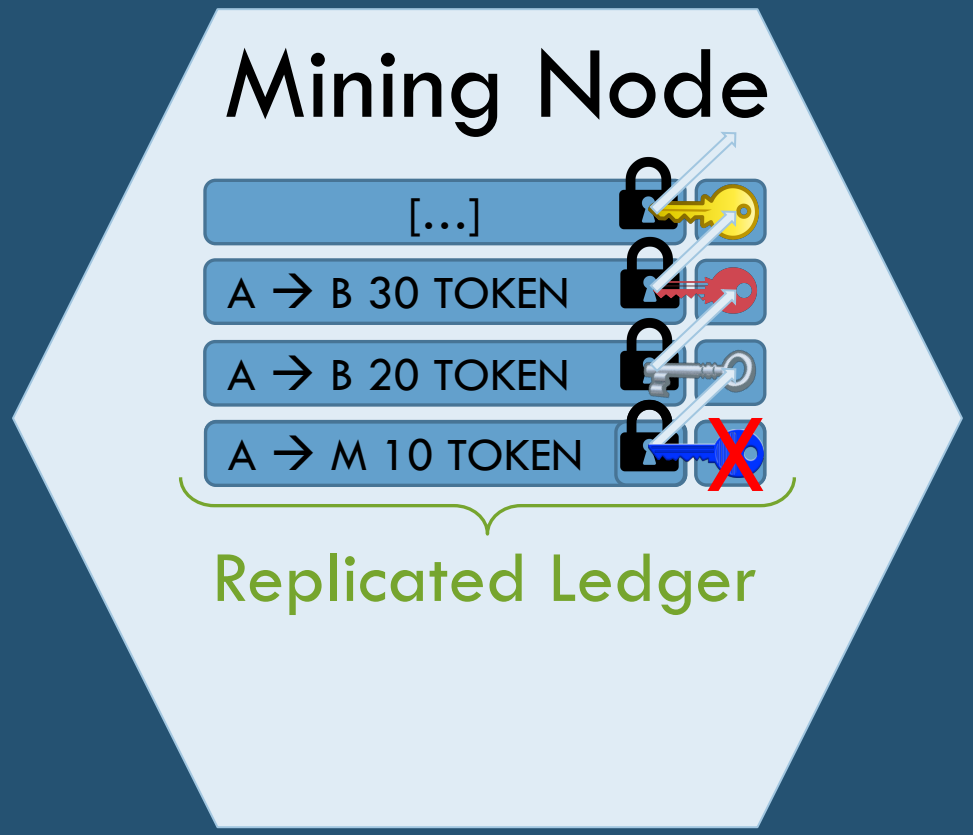
AN IMMUTABLE LEDGER





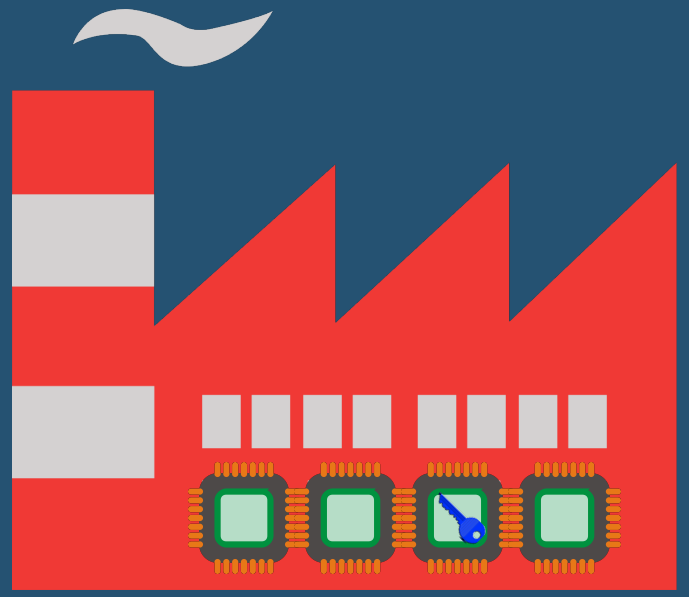
AN IMMUTABLE LEDGER





CONSENSUS METHODS

Proof of Work



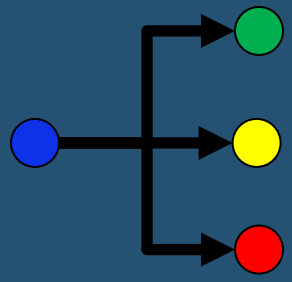
- 1 chance per CPU cycle
- Difficult to compute
- Easy to verify

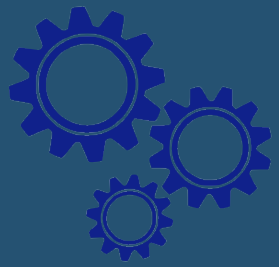
Proof of Stake

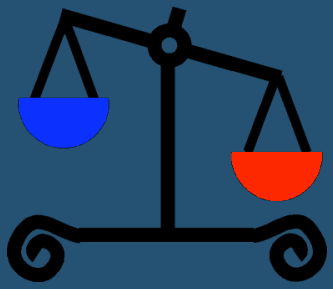
- 1 chance per share
- Deterministic calculation
- Less energy cost

SMART CONTRACTS

Business Logic → Contract Code → Execution → Settlement







FLAVORS OF BLOCKCHAIN NETWORKS

PUBLIC

PERMISSIONLESS

PRIVATE

PERMISSIONED

BLOCKCHAIN TECHNOLOGY STACK

App | App | App

API | API

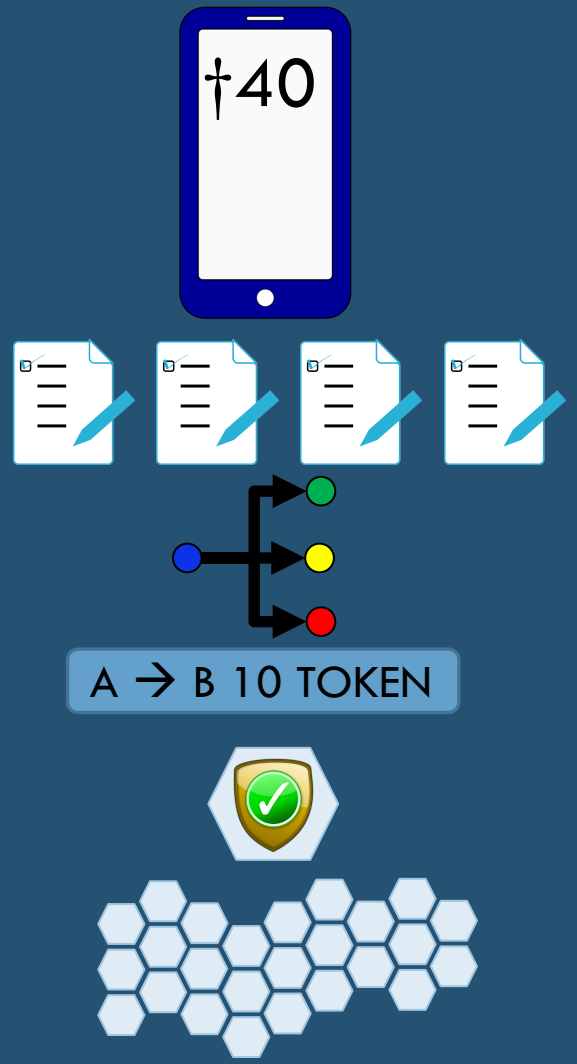
Distributed Ledger

Smart Contracts

Transactions / Messages

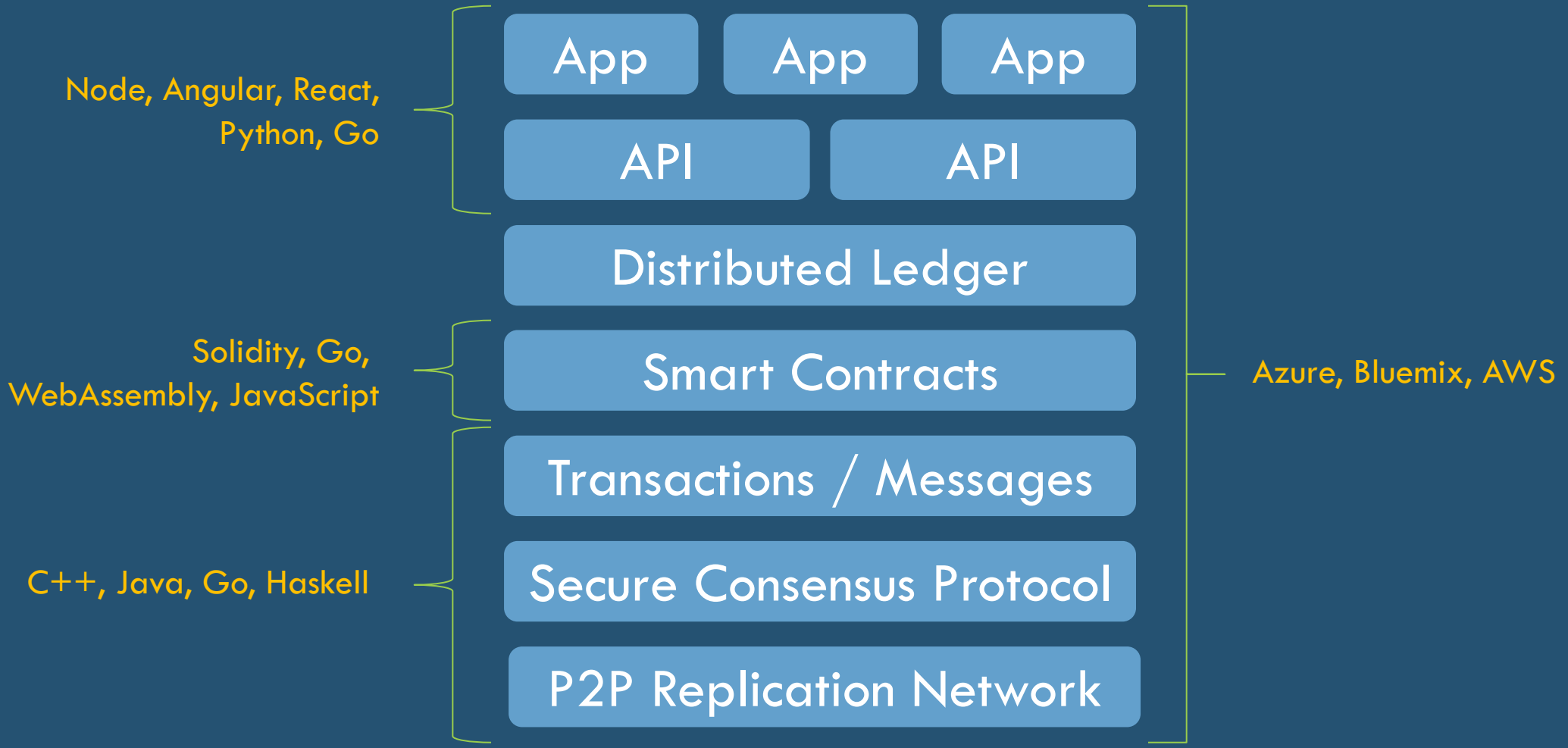
Secure Consensus Protocol

P2P Replication Network



BLOCKCHAIN TECHNOLOGY STACK

Languages and Skill Used by Design Team



QUESTIONS?

BLOCKCHAIN USE CASES / DEMOS

SOME EXAMPLE BLOCKCHAIN USE CASES

Financial Services

- Trading platforms
- Repurchase agreements
- Foreign exchange
- Payment remittance
- Corporate debts & bonds
- Letters of credit
- Digital currencies

Healthcare

- Electronic medical records
- Virus banks
- Seed vault backup
- Doctor-vendor RFP services and assurance contracts
- Blockchain health research commons
- Blockchain health notaries

Insurance

- Peer-to-peer insurance
- Claims processing
- Ownership titles
- Sales and underwriting

Government

- Passports / licenses
- Voting
- Taxes
- Government tender processes

Asset Management

- Device mgmt / IoT
- Capital asset mgmt

Supply Chain

- Manufacturing processes
- Quality assurance

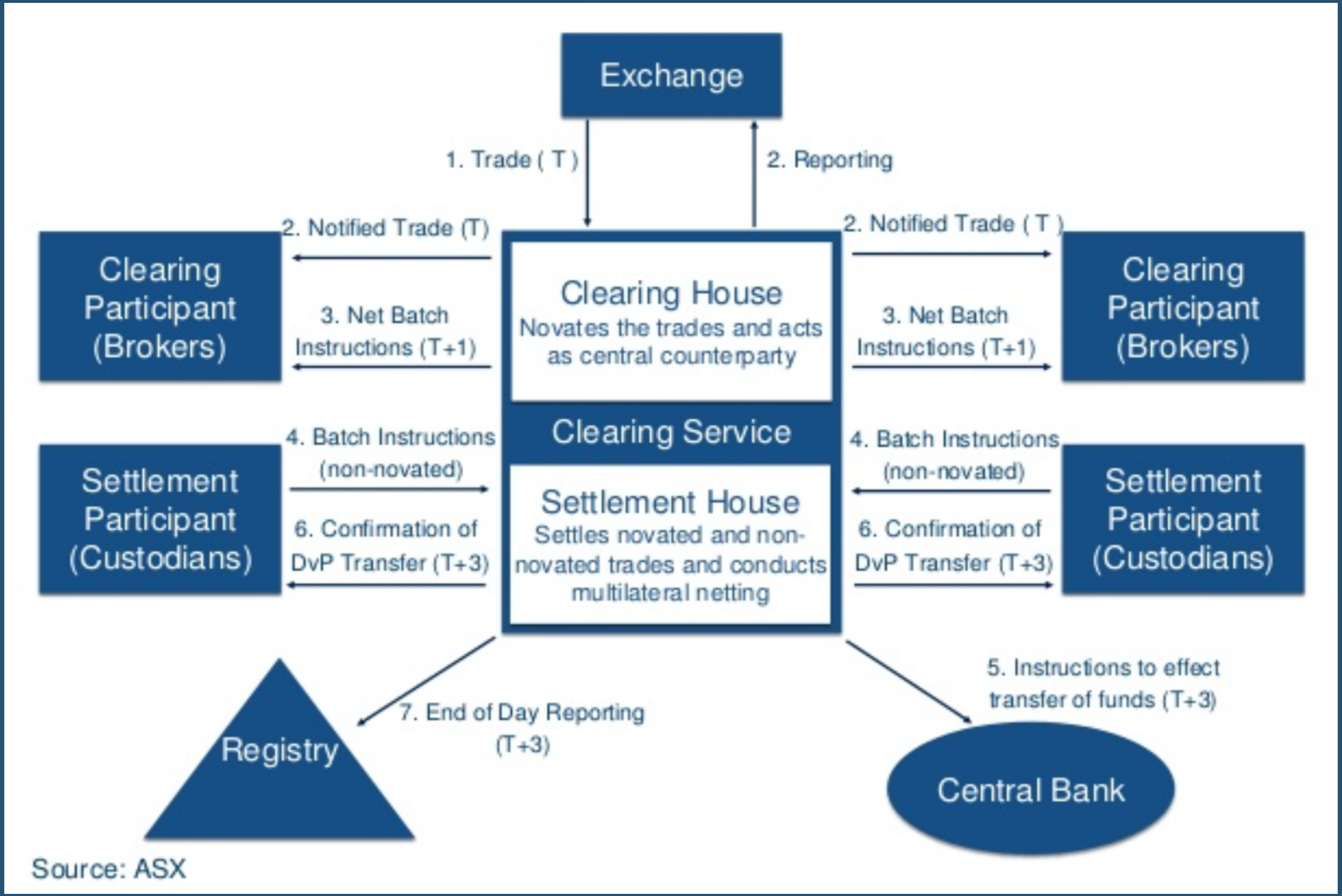
Consumer Marketing

- Loyalty points management

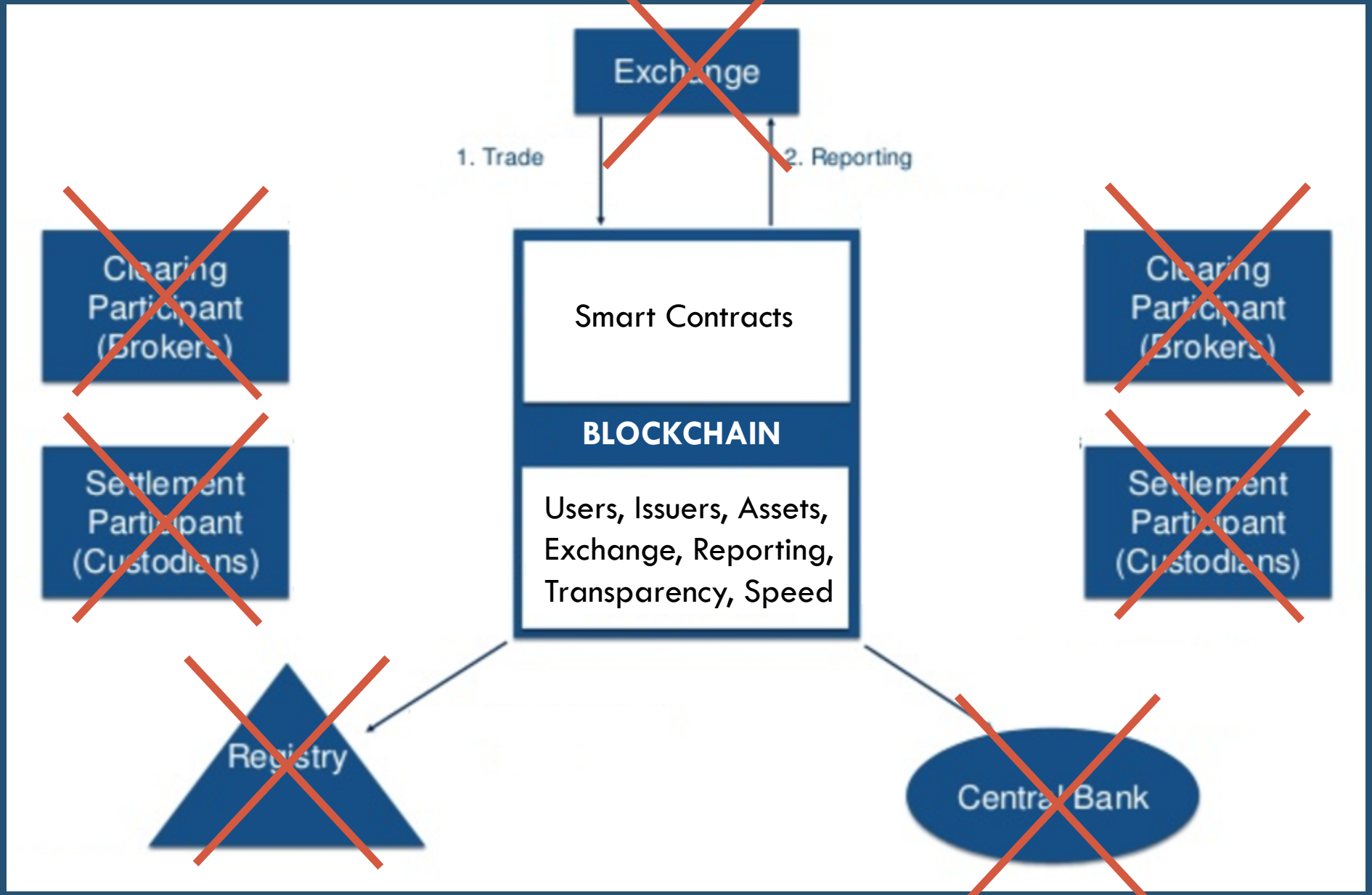
Contracts

- Real estate
- Music
- Royalties

EXAMPLE: TRADE SETTLEMENT (T+3)



EXAMPLE: TRADE SETTLEMENT (BLOCKCHAIN)



DEMOS

BLOCKCHAIN SUMMARY

REVIEW – WHAT WE'VE COVERED IN DAY 1

Blockchain is a very secure, distributed, replicated transaction ledger.

Blockchain / DLT technology is exciting, yet complex, and still evolving.

Blockchain allows a network of parties to track & exchange assets without intermediaries.

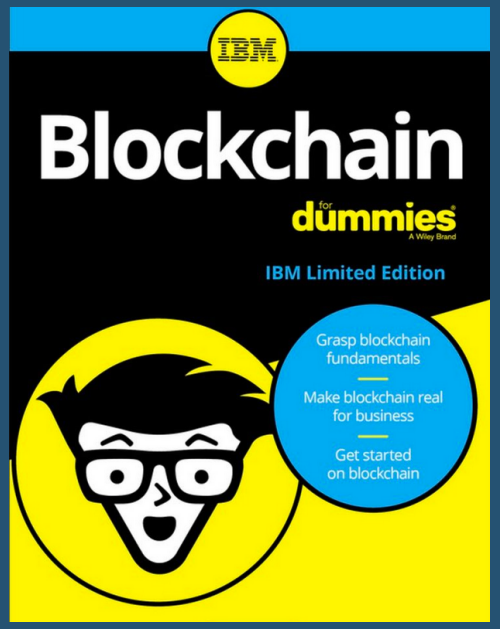
Blockchain uses cryptography and consensus to update the ledger and make it "hack-proof".

Blockchain can support many industry use cases beyond digital currencies.

Now is the time to get ahead of the wave …

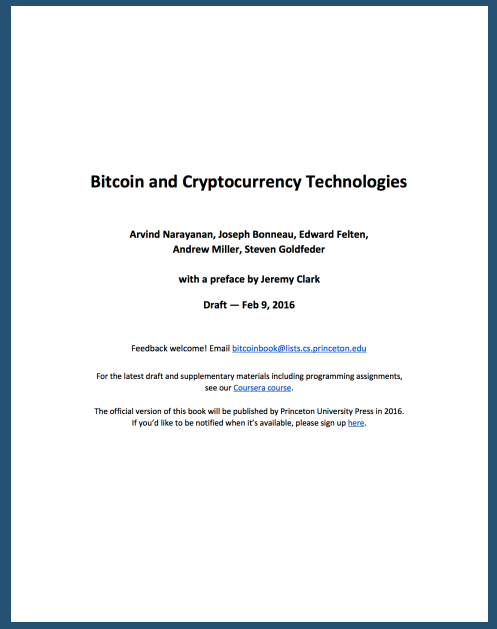
HELPFUL RESOURCES

starter



IBM Blockchain For Dummies

advanced



Bitcoin and Cryptocurrency Technologies

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

with a preface by Jeremy Clark

Draft — Feb 9, 2016

Feedback welcome! Email bitcoinbook@lists.cs.princeton.edu

For the latest draft and supplementary materials including programming assignments, see our Coursera course.

The official version of this book will be published by Princeton University Press in 2016. If you'd like to be notified when it's available, please sign up here.

Princeton Blockchain Textbook & Course

videos

YouTube

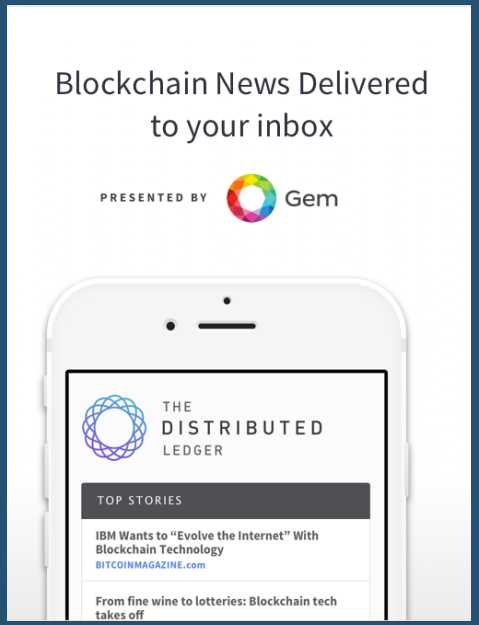
Khan Academy, …

meetups

meetup

Women in Blockchain
Enterprise Blockchain

online news



Distributed.com eMagazine

HELPFUL RESOURCES (LINKS)

starter	IBM Blockchain for Dummies	https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN
advanced	Princeton Blockchain Textbook	https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf
videos	Khan Academy (Bitcoin)	https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking#bitcoin
meetup	Women in Blockchain Meetup (@ Improving)	Contact Barb Gurstelle @ Improving
meetup	Enterprise Blockchain Meetup (@ downtown Minneapolis)	https://www.meetup.com/Enterprise-BlockChain-Meetup/
online news	Distributed.com eMagazine	https://distributed.com/

QUESTIONS?

THANK YOU VERY MUCH!