Patterson Belknap Webb & Tyler LLP

Blockchain: Fundamentals & Opportunities

A primer on its evolution, technological functionality & potential use cases

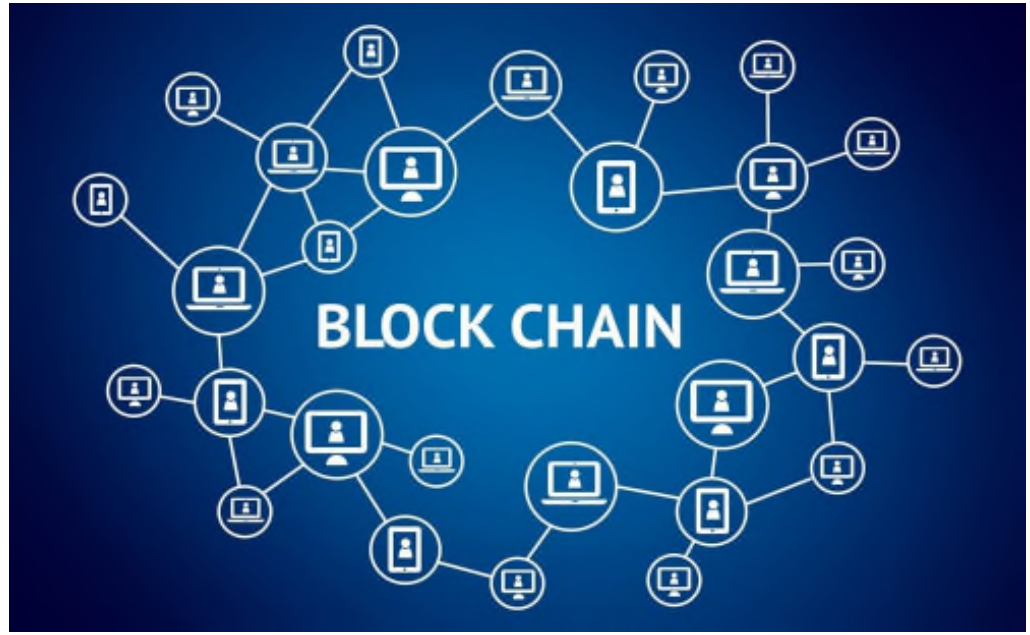
Lewis V. Popovski

Jean-Claude Lanza

pbwt.com

scope

- what's the problem?
- why is blockchain a solution?
- what is blockchain?
  - description
    - characteristics
    - functionality
  - history
  - future
    - general uses
    - specific applications



context

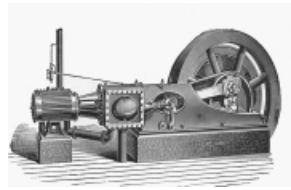
blockchain matters

- invention is proportional to societal gaps of their time
- blockchain is a tool to address the 21st century's gap
- gaps are limitations encountered by society
- pressures on human intuition & outsourced decision making
- importance of institutions - value exchange
- blockchain is the continuation of an evolving human story
- new technological institution that fundamentally changes how we exchange value
- lowers uncertainty using technology alone

necessity & invention provide context

- game-changing inventions
  - 15th cent. – efficient knowledge transfer was impossible until

  - 18th cent. – power generation was predominantly human until



  - up to late 20th cent. – widespread information transfer was difficult until

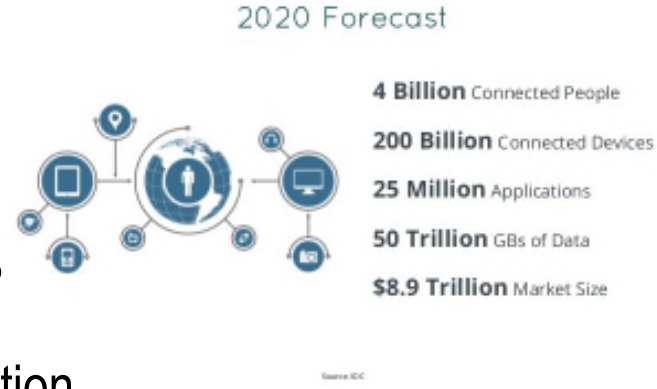
    - knowledge, power, distance … all effectively addressed
    - what is today's (and tomorrow's) gap?

we've got trust issues…

- TRUST - humans need it to transact 
- traditionally, intermediaries are necessary to manufacture trust
  - parties = banks, title companies, vendors, etc
  - tools = errors & omissions insurance, etc
- this gap puts pressure on human intuition & decision making
- leakage 
  - intermediaries charge fees
  - fees leak value from transactions
- lack of trust = intermediaries = costs = leakage = diminished transaction value

trust but verify

- trust isn't enough - verification is needed too
  - if trust is manufactured, need to ensure compliance & legitimacy
  - think "organic", "made in [•]", "conflict-free", "neutral"… do we know for sure?
  - globalism making it extremely difficult to verify
- what's limiting commerce? an inability to verify
- IoT promises staggering growth
  - are human-to-machine transactions trustworthy?
- IoT cannot scale relying on intermediaries for verification
  - can technology help? how?



blockchain is a solution

- if the 21st century's gap is trust…
- because humans are increasingly interacting with machines & each other (IoT)…
- creating a greater demand for trust & verification...
- then, how do we automate verification & build trust?

- blockchain, or distributed ledger technology (DLT)

conceptual definition:	*technical definition:*
blockchain is a software protocol used for recording & transferring data & assets (think SMTP as a protocol for sending email)	blockchain is a tamper-resistant distributed ledger software used for recording & transferring data & assets via the internet, without the need for 3rd party intermediaries

functionality

blockchain: a distributed ledger

- traditionally ledgers were used for internal accounting and by intermediaries to record transactions & ownership
- written ledgers gave way to stand alone databases - such as Excel & SAP
  - did not allow a third parties to easily verify - required time consuming & expensive third party audits
- blockchain = new-age ledger/database
  - distributed—everyone has the same copy of the database
  - complete—everyone can see all transaction histories & their details
    - information is stored in sequential data “blocks” - “blockchain”
  - immutable—very difficult to change verified blocks

the problem:

- Double Spending:
  - anything digital is easily replicated
  - uncertainty as to who rightfully owns a digital asset

the beginning

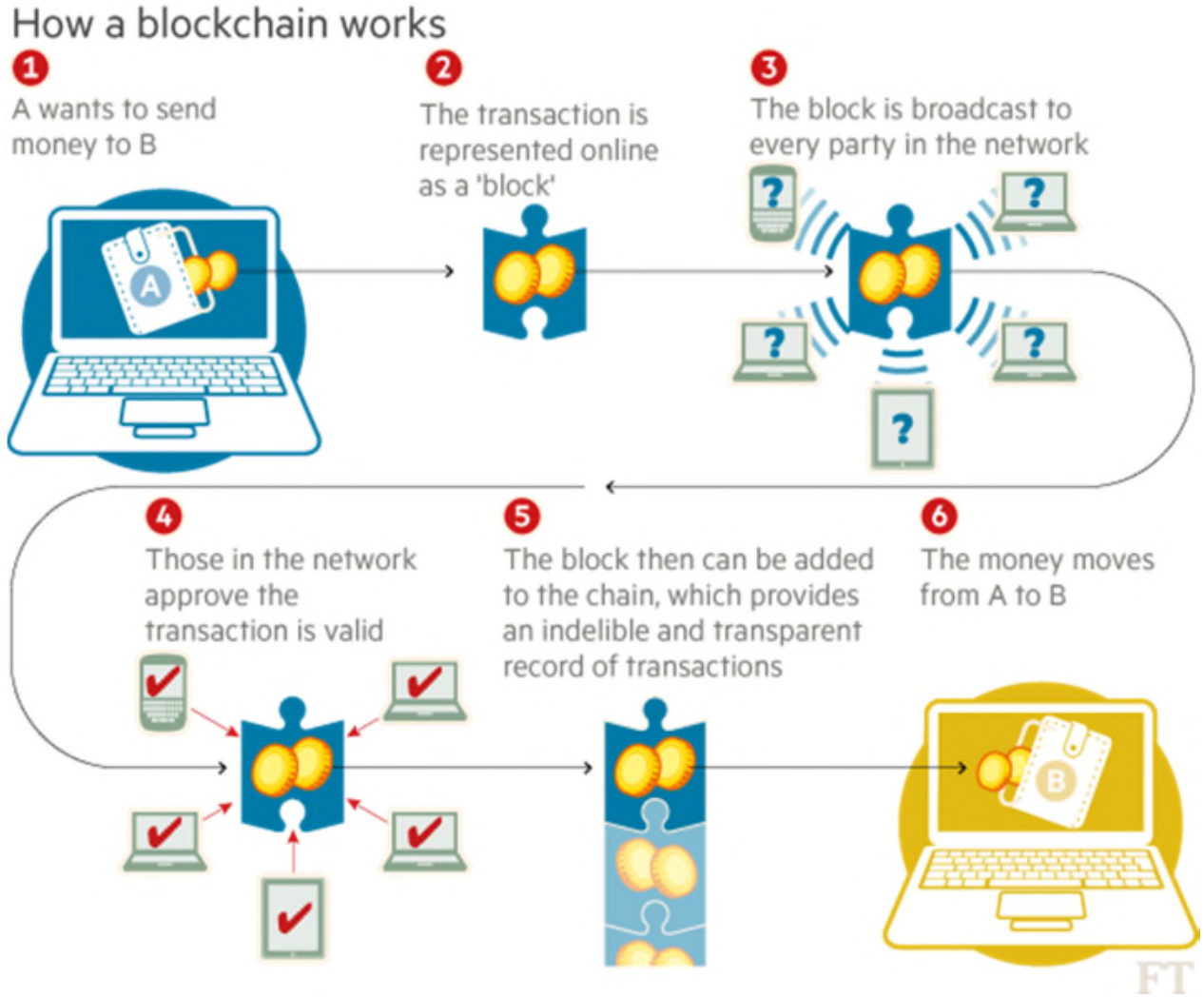
- “Bitcoin: A Peer-to-Peer Electronic Cash System”
  - “Satoshi Nakamoto”

- direct on-line payments without going through financial institutions
  - “An electronic payment system based on cryptographic proof instead of trust”

the solution:

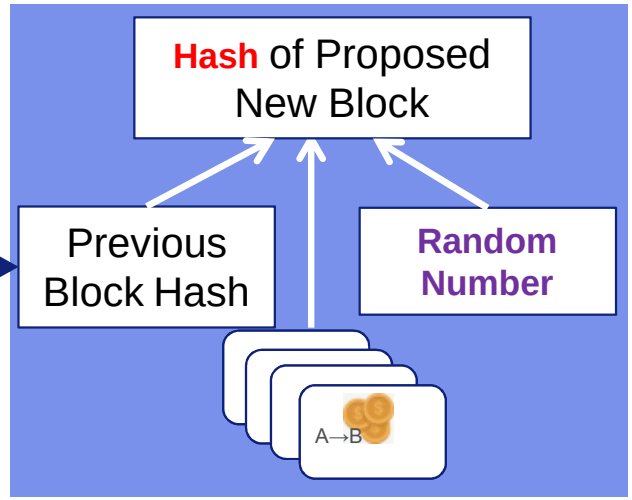
- **Peer to Peer Network**: distributed database
- **Verification** - “Proof of Work”:
  - communal verification of all transactions in a block before block is added to the existing chain
- **Timestamp**: new transactions are connected to & sit on top of all previous transactions forming a time ordered sequence of blocks - blockchain

how it works: overview



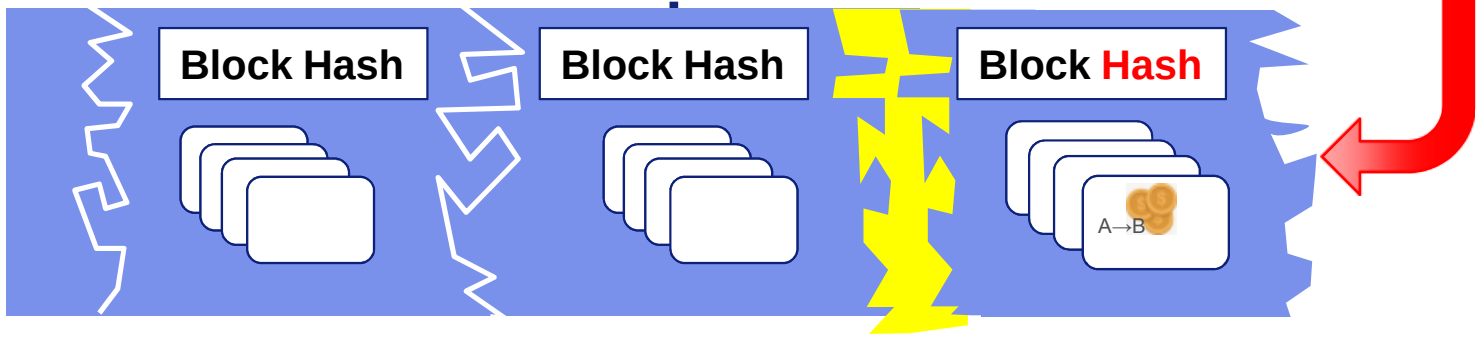
https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64#axzz3qe4rV5dH

proof of work details

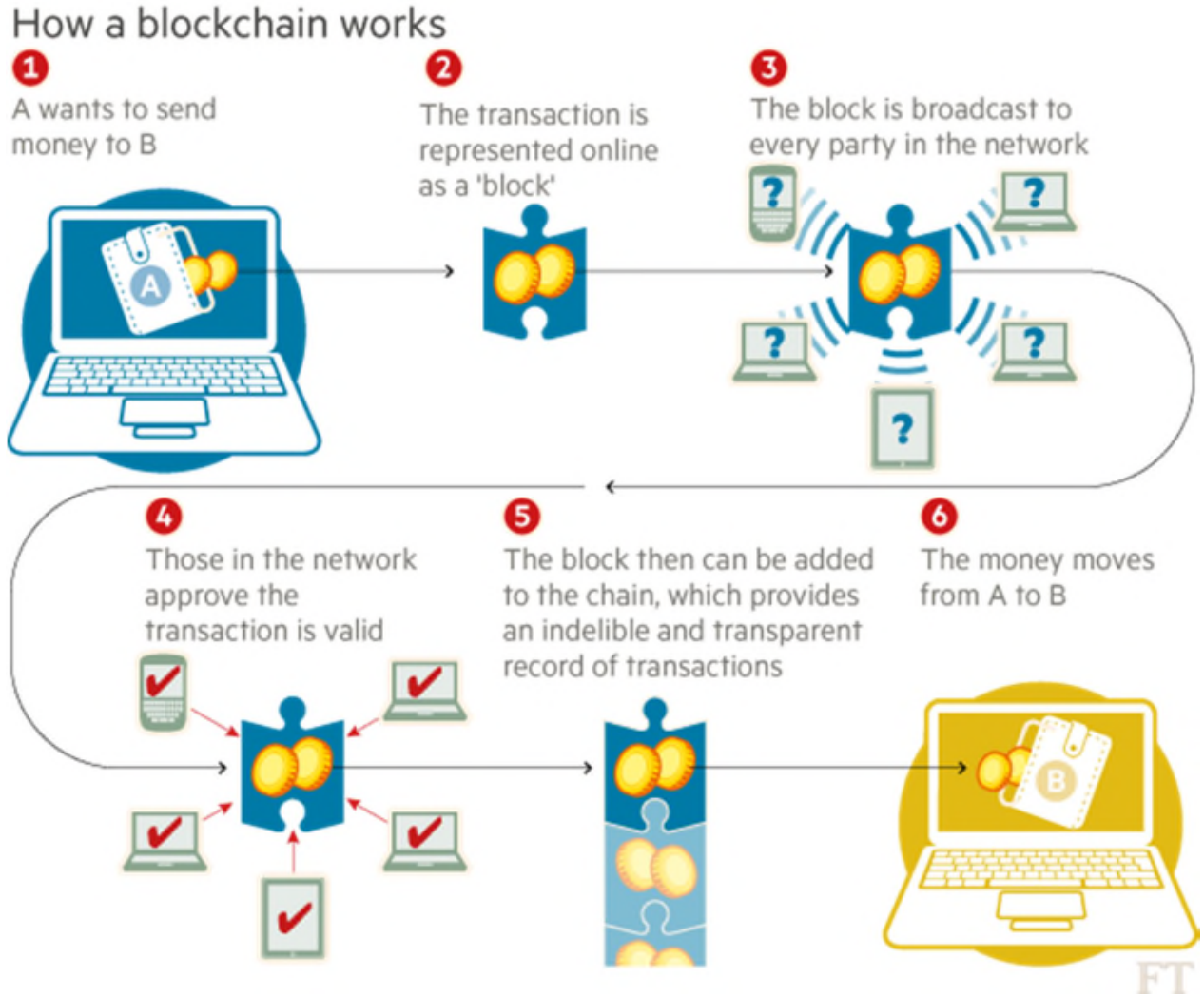


Proof-of-Work Calculation

1) **Pick** new **Random Number**
2) **Compute Hash**
3) **If** (**Hash** < HashMax) **then** broadcast new block
   else repeat from 1)



how it works: overview



https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64#axzz3qe4rV5dH

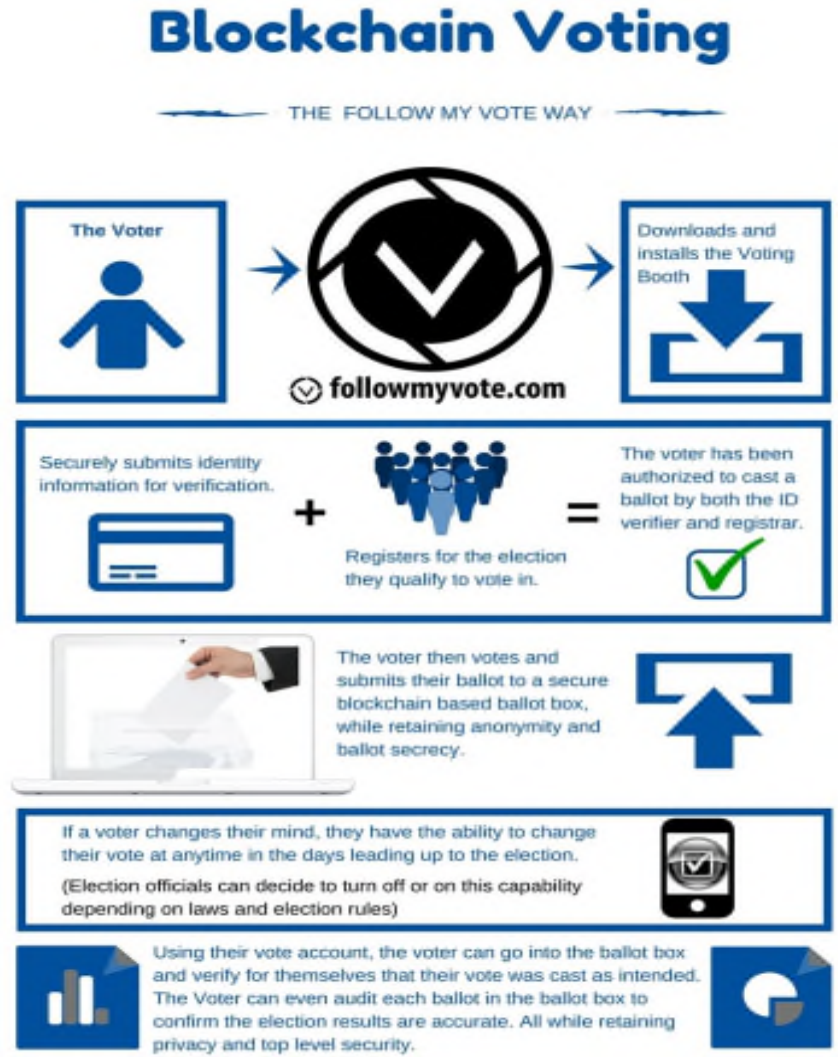
applications

two types of applications

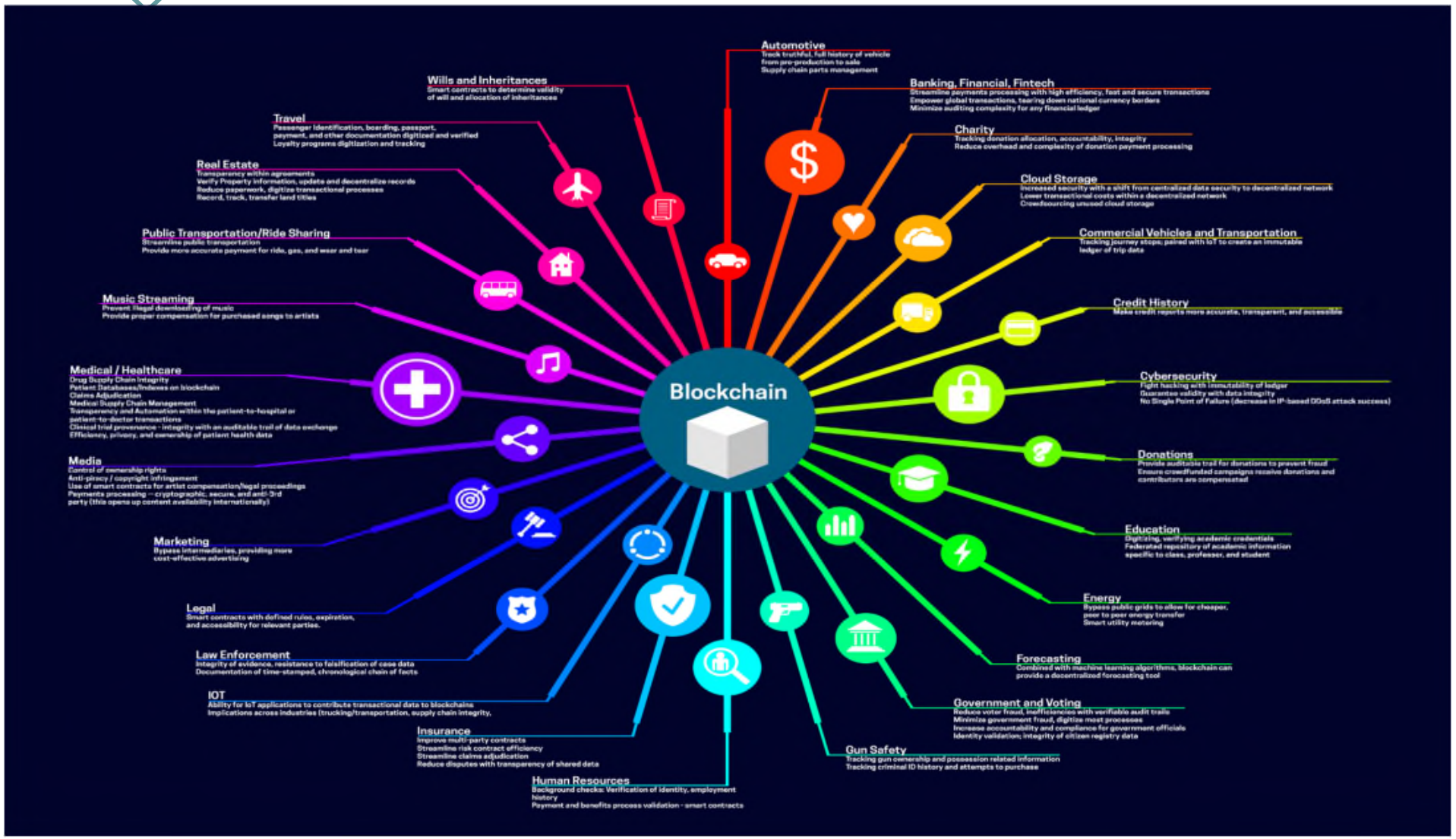
- as a system of record for data
  - digital identification
  - tokenization
  - intra-organizational data management
  - governments
  - financial institutions
  - audit trails
- as an exchange platform for information/value
  - smart contracting
  - automated governance
  - markets
  - clearing & settlement
  - automating regulatory compliance

some early use cases

- property deeds filing & transfer
- letter of credit issuance
- PMI safekeeping & transfer
- supply chain & logistics management
- voter registration, ballot casting & count auditing

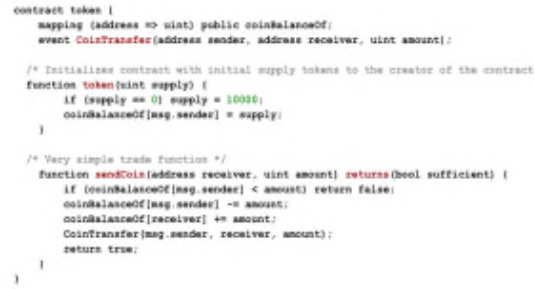


broad spectrum of additional use cases



maybe most importantly for us.... smart contracts

- using blockchain software to model many parts of a contractual arrangements
- self-executing contracts stored on the blockchain with agreement terms between buyer & seller written directly into lines of code
- cold war precedents
  - grew out of academia-driven project to make contracts computable & machine-readable
- number of benefits
- some concerns



```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

  /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

a few open questions (from the growing pile)

- is data on the blockchain admissible as evidence?
- what is the law of blockchains?
- where do transactions executed on the blockchain occur?
- which courts will have subject matter or personal jurisdiction over disputes
- which laws apply?
- where are smart contracts deemed to be transacted?
- who has jurisdiction over decentralized autonomous organizations (DAOs)?
- will pseudonymizing information satisfy data privacy concerns?
- how will the “right to be forgotten” be addressed?
- how to tax an entity that lives on the blockchain?

contacts

Lewis V. Popovski

212.336.2610

lpopovski@pbwt.com

Jean-Claude Lanza

212.336.2022

jlanza@pbwt.com