Challenges and Advances of Blockchain Technologies

Nikolay Pakulin
Pax Datatech, CTO
nikolay@paxdatatech.com

October 31 2018

Bitcoin: A Peer-to-Peer Electronic Cash System

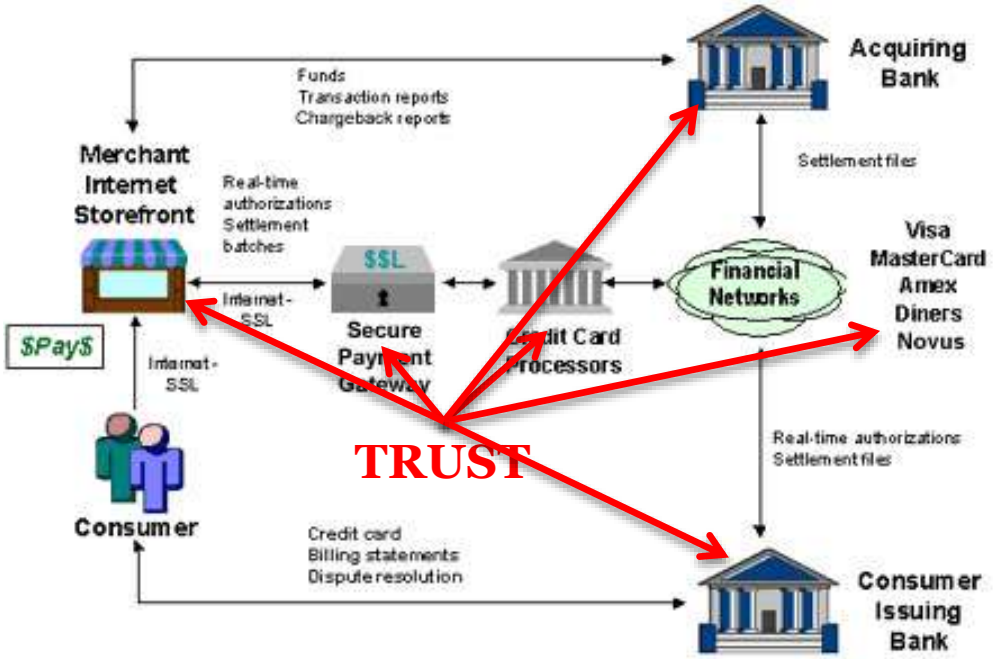
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

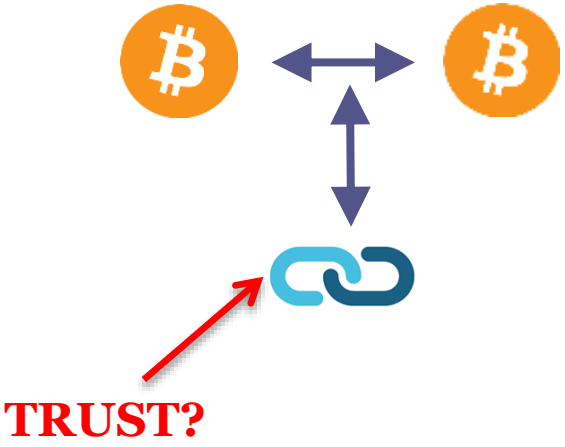
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

Why P2P Electronic Cash?



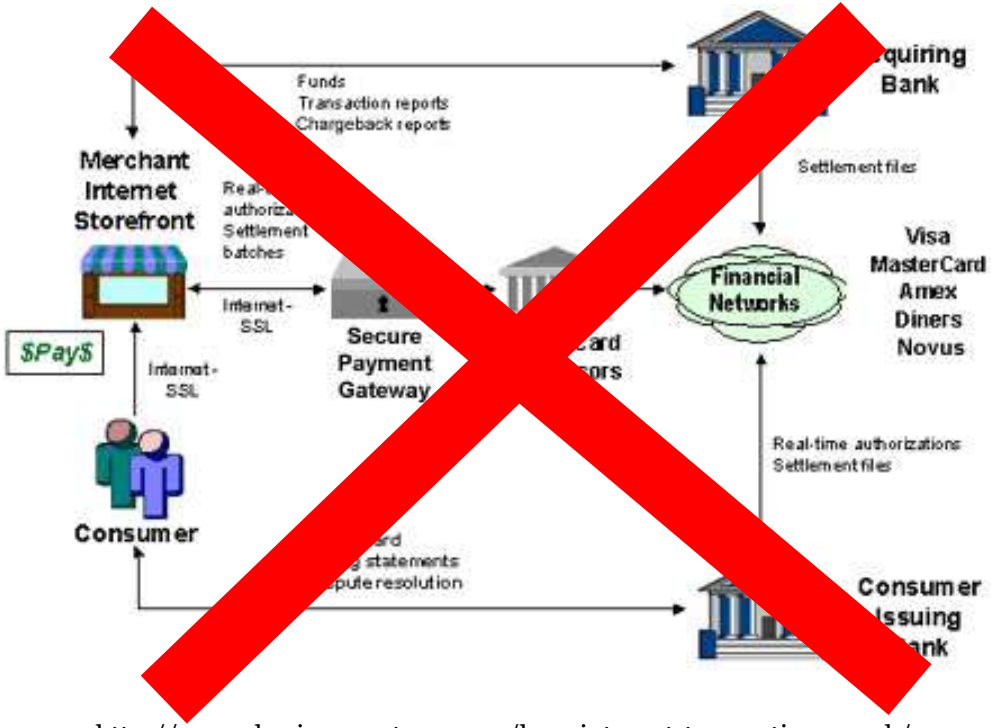


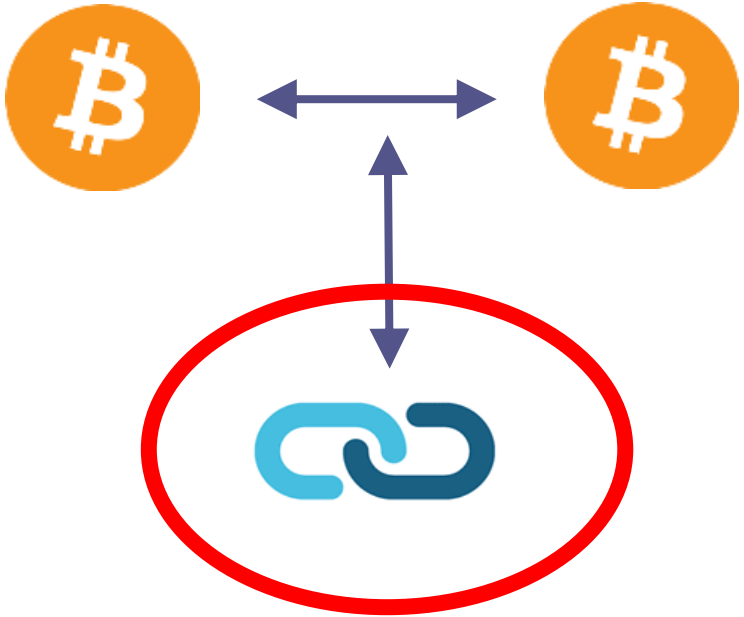
http://sourcebusinesssystems.com/how-internet-transactions-work/

Bitcoin: Trusted history log from untrusted community

- Transaction: Alice claims to send 10 BTC to undisclosed barer
- Community: validates that Alice has 10 BTC
- Assumptions:
  - Community is diverse, mostly unrelated to Alice
  - Little number of cartel, cliques, coordination
  - “Miner game” (PoW) guarantees random selection of block producer

Peer to Peer?

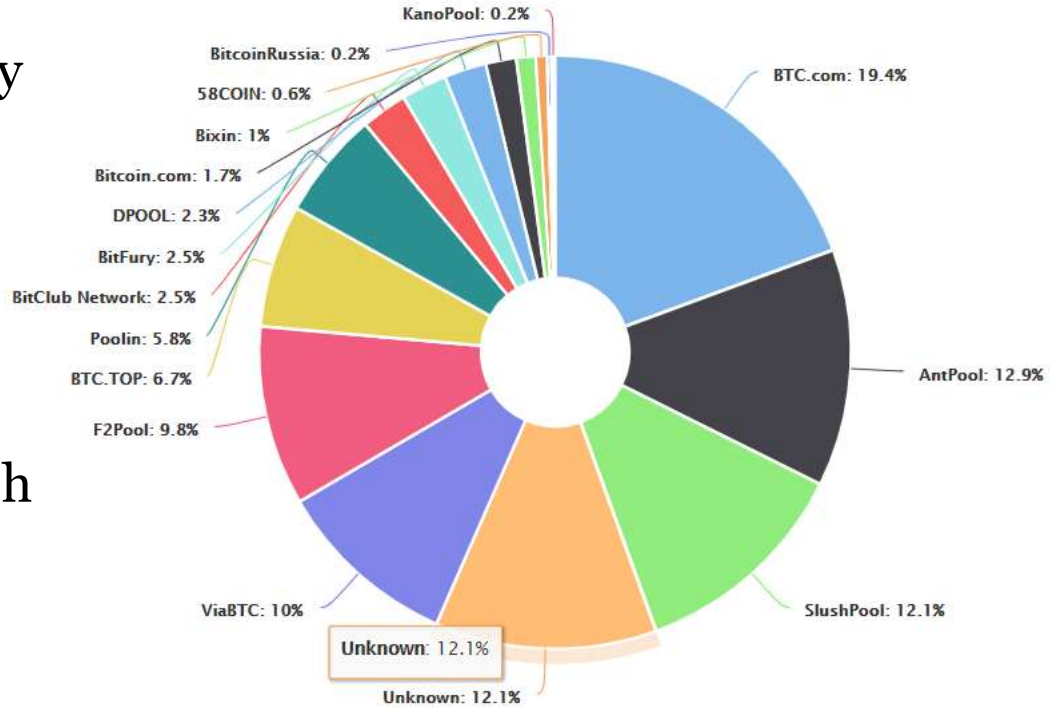




http://sourcebusinesssystems.com/how-internet-transactions-work/

Bitcoin: assumptions failed

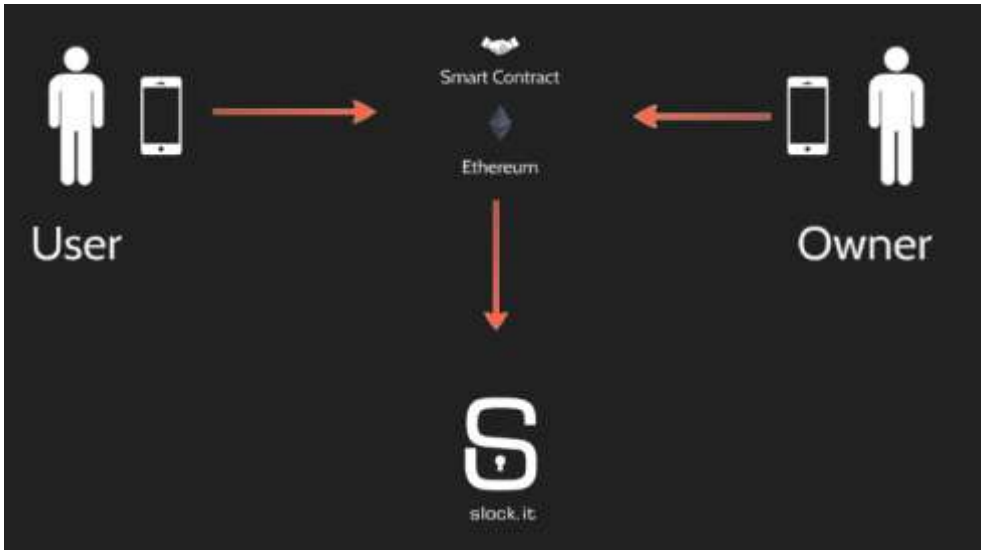
- 80% of blocks constructed by 8 miners
  - BTC.com, AntPool, SlushPool, ViaBTC, F2Pool, BTC.TOP, Poolin, BitClub Network
- Unidentified community: only 12.1%
- Reason – CPU-intensive hash function, easy to parallelize
  - Scrypt, Ethash, … - memory intensive



Still...

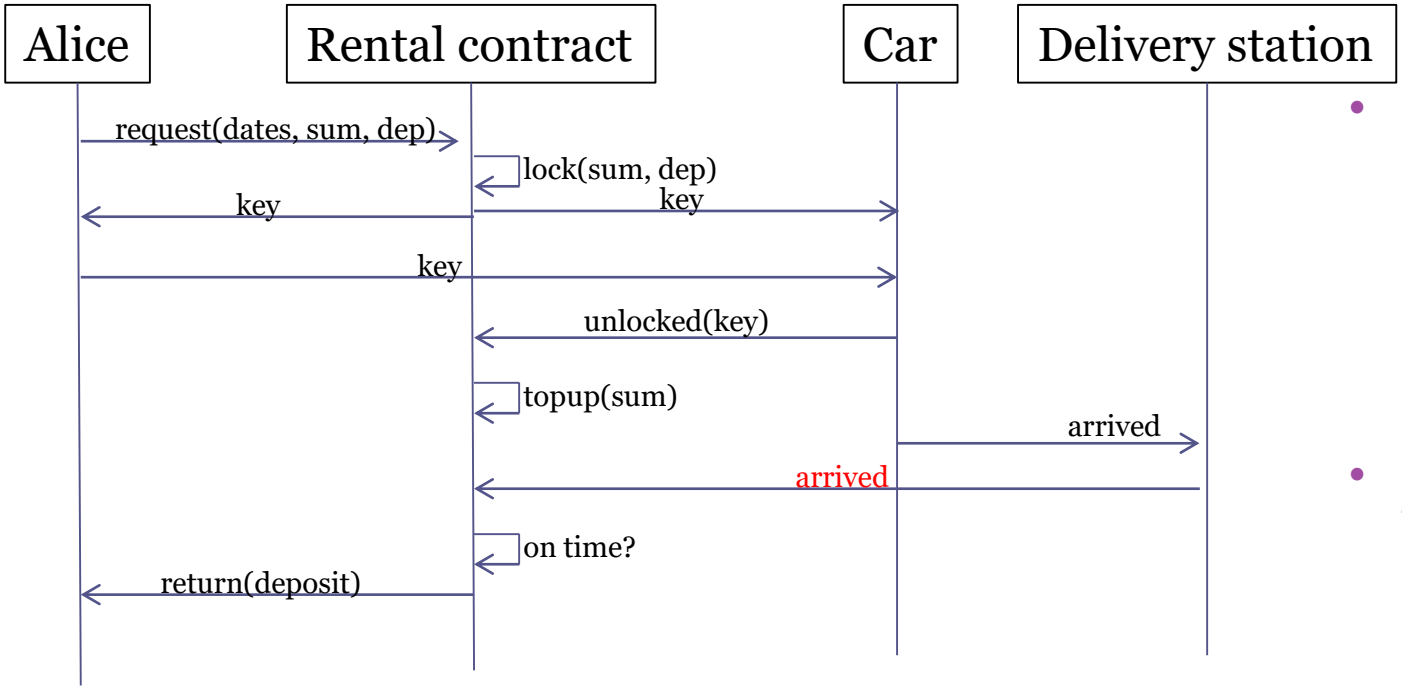
- 39 forks, 6 in Top-20
- Varying in block size, block time, transaction data, emission policy, hashing, privacy
  - ZCash!

“Smart” Contract



- Executed in blockchain
- Triggered by events
- Uses data from oracles
- **Digitalizes relationships between humans**

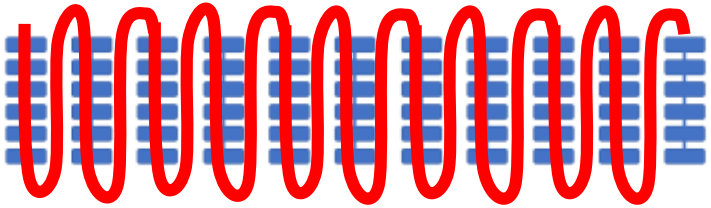
“Smart” contract possible?



- Policy Specification – as old as 1960-s
  - Coding laws, contracts, agreements
  - No major success
- Exceptions – the root of all evil
  - Car integrity?
  - Really car?

Smart contract performance

- Sequential Execution
  - Only one node executes chain code at a time
  - No concurrent execution
- Simple and short chain code)
  - Ethereum: Gas limit
  - EOS: 30 ms execution time



Blockchain Performance - How to Solve?

- Produce blocks faster
  - Bitcoin – 10 minutes, Ethereum – 10-40 seconds, EOS – 0.5 second
- Produce bigger blocks
  - SegWit, off-chain data, gigabytes in size
- Fundamental limit:

$$performance = \frac{1}{time\_per\_transaction}$$

  - Because of sequential execution

Call for dApps

Blockchain Platform

Developers

Smart Contract Development?

- Have you tried Solidity?
- Have you tried to debug Solidity?
- Have you tried to test Solidity?
- Have you tried to read Solidity?
- **Can you trust smart contracts?**

```
PUSH1 0x60
PUSH1 0x40
MSTORE
PUSH1 0x04
CALLDATASIZE
LT
PUSH2 0x006c
JUMPI
PUSH4 0xffffffff
PUSH29
0x0100000000000000000000000000000000000000000000000000
PUSH1 0x00
CALLDATALOAD
DIV
...
```

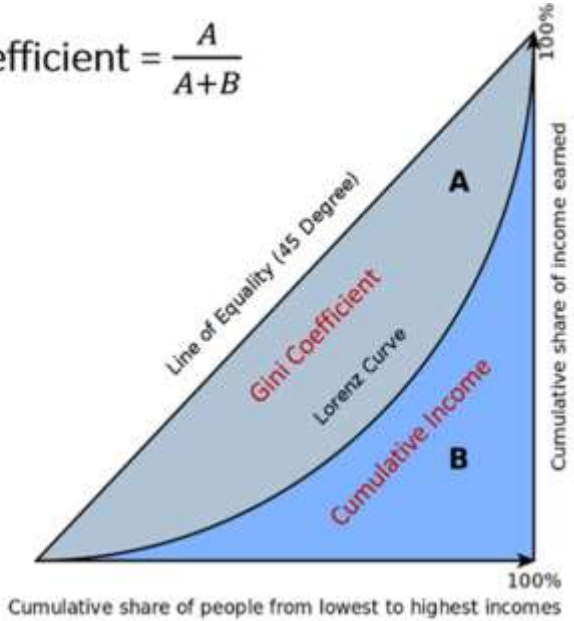
https://etherscan.io/address/0xf97e0a5b616dffc913e72455fde9ea8bbe946a2b#code

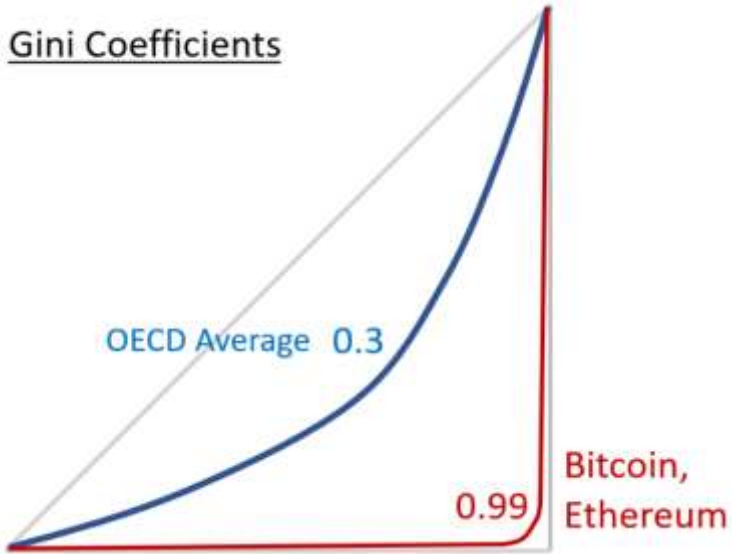
Governance

- Who decides?
  - Bitcoin foundation, Ethereum foundation, Dash main nodes, EOS block builders…
- Who controls?
  - Decentralized? Fair?
- Legislation? Policy Enforcement?
  - EOS case
- Forks?

Rich become Richer

$$\text{Gini Coefficient} = \frac{A}{A+B}$$





The Problems

Problems of Existing Blockchain

Governance

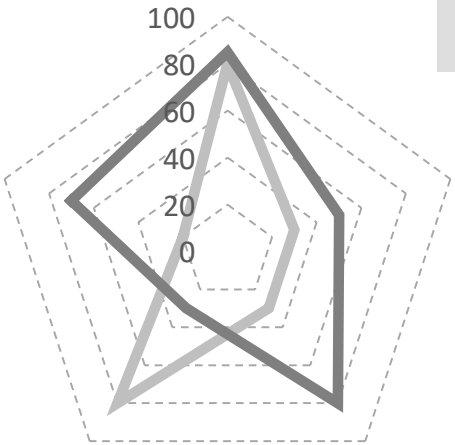
- **Cartel & Bribe (PoS)**

EOS governance has failed, how can any DAO deal with bribe attacks, plutocrats and other risks?

Security

- **Hacks & Thefts**

No good solutions to account security regarding hacks and thefts



Sophisticated dApps

- **No Big dApps**

No large-scale applications yet

Decentralization

- **Recentralization**

The centralization risks in Proof of Stake

- **The Rich Get Richer and The Poor Get Poorer**

Bitmain and affiliate pools have 53% of all bitcoin hashpower

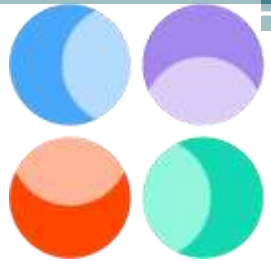
Scalability

- **Slow Transaction Speed**

dApps do not work well with 5-10 sec of blockchain latency

- **Expensive Transaction Cost**

PoW is burning billions of dollars every year

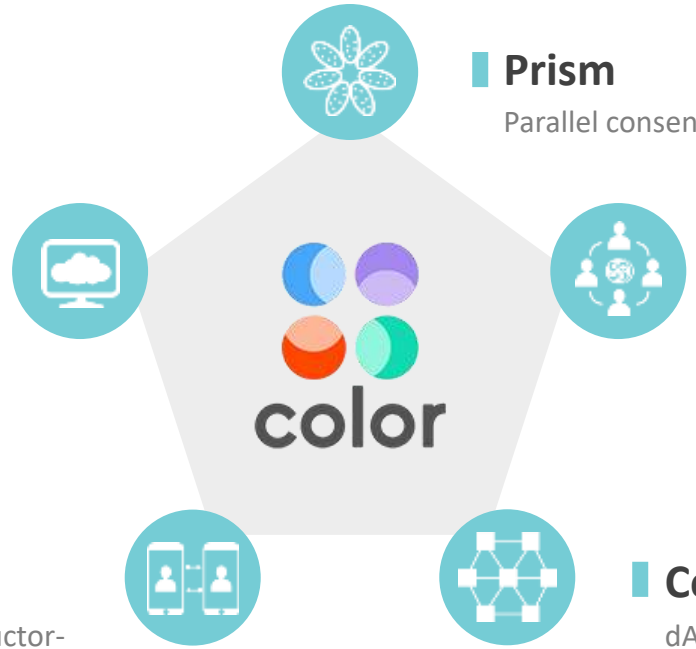


color

Trying to Answer

Color – multiaspect project of Pax Datatech (Seoul, Korea)

How It Works



Prism

Parallel consensus algorithm

Color Spectrum

Two-tier data processing technology

Pixel Program

Color Coin distribution program

Color Pay

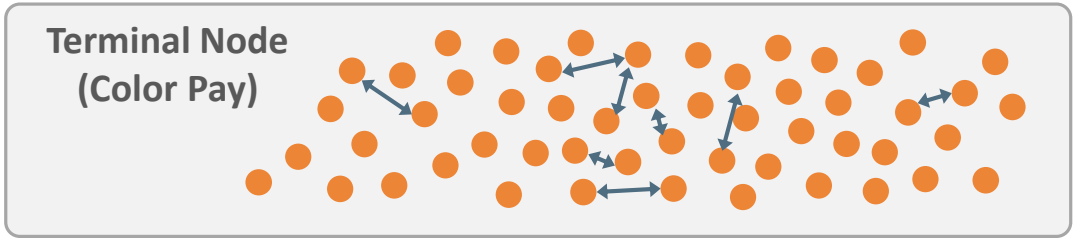
Unhackable semiconductor-based payment system

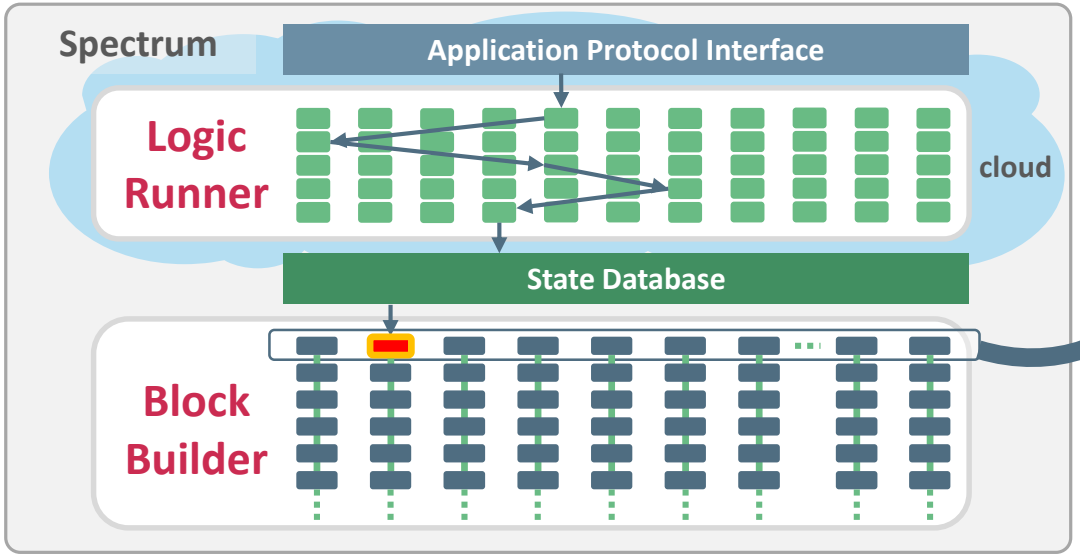
Color Coin

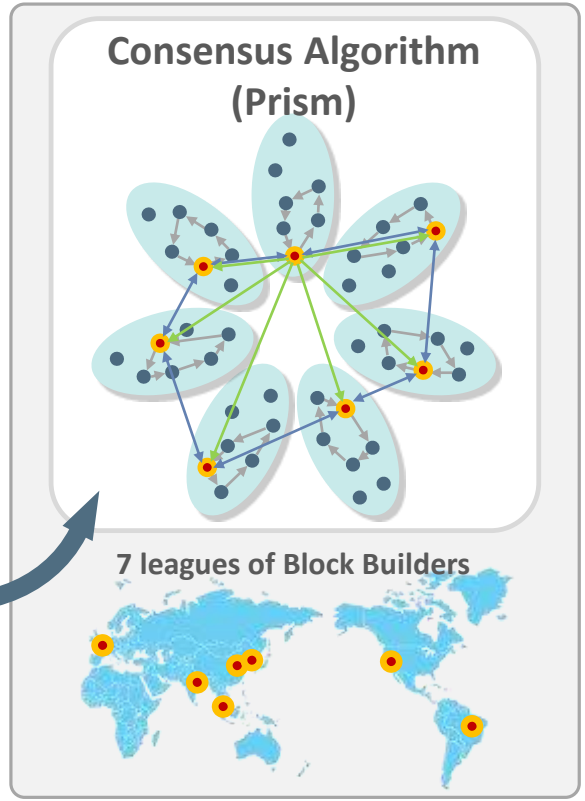
dApp Ecosystem of using a single currency(COL)

Color Spectrum

Color Spectrum is essentially the engine and core technology that enable both the consensus and dApp development on top of the Color Platform via a programming language agnostic development environment.

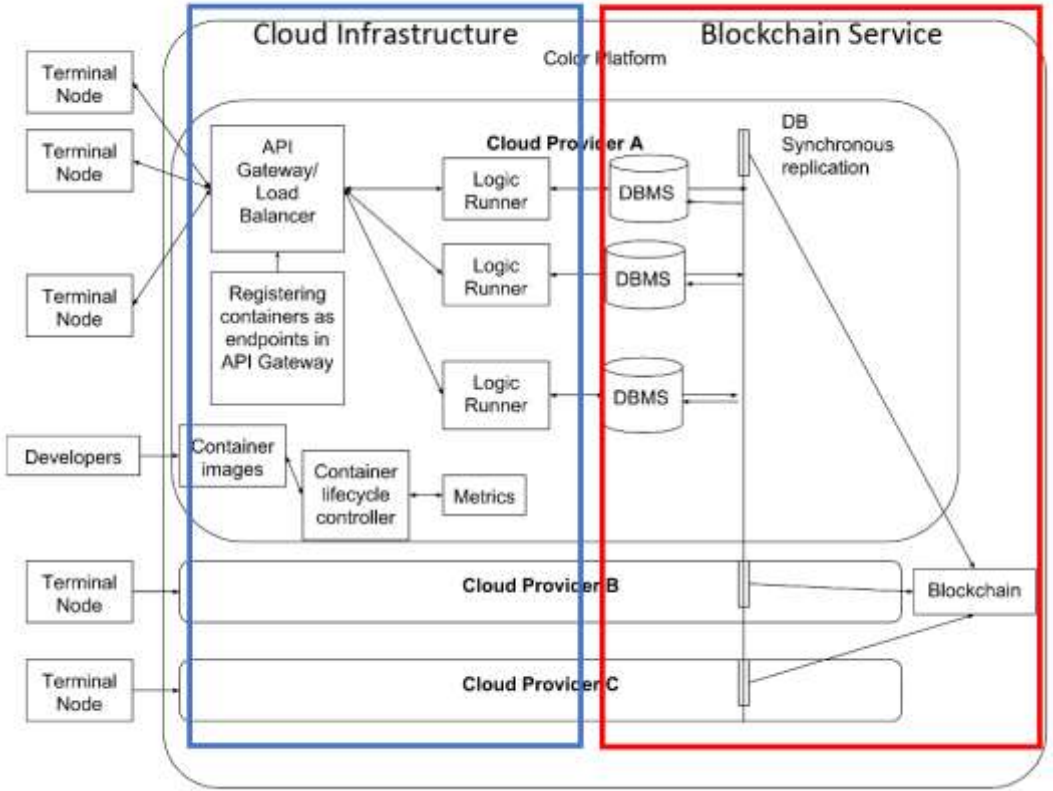






Color Spectrum

Color Spectrum takes the best of both worlds: **Cloud and Blockchain**



Cloud: orchestrates Logic Runners, manages resources, enables **high performance** parallel execution

Blockchain: stores data and result of execution, enables **coin and economy**

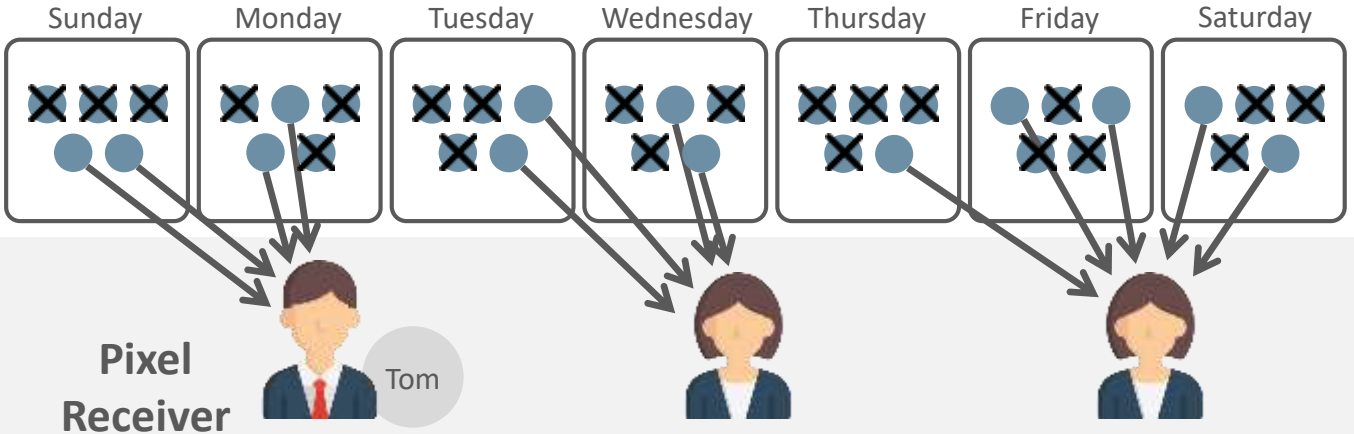
kubernetes

Pixel Program

Pixels are a conditional sharing mechanism aimed to disincentivize hoarding, promote giving, and increase the circulation of the Color Coin to grow the number of ecosystem participants organically.

Pixel Giver

Daily 5 Pixels are Created to Every KYC'ed Wallet.
Non Gifted Pixels are Nullified After 24 Hours.

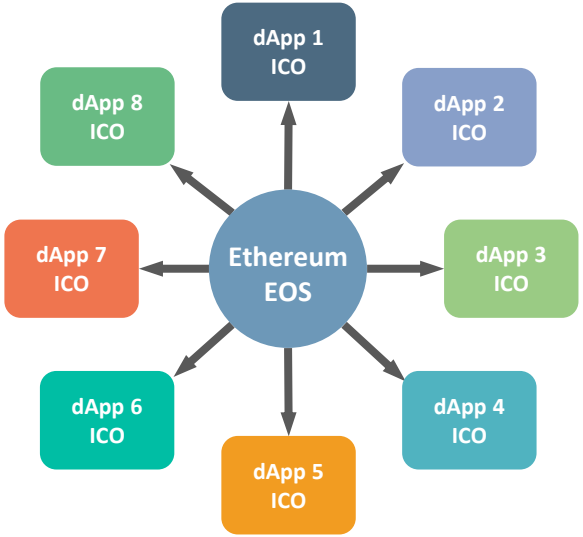


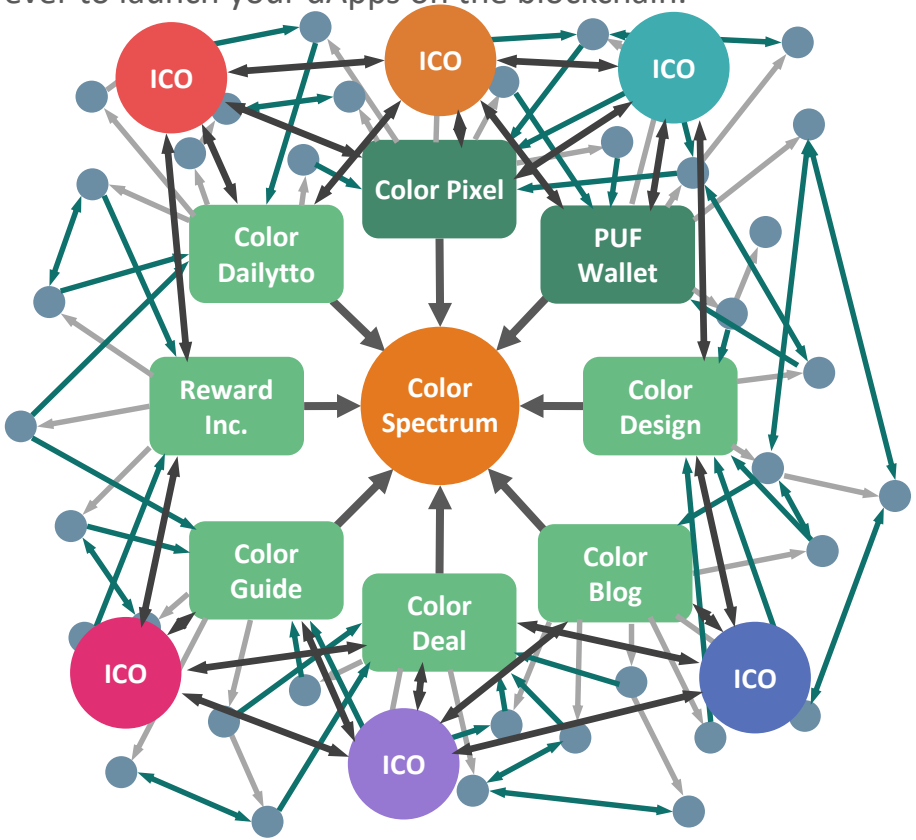
Received Pixels Convert to Color Coin Weekly Proportionally

$$\frac{\text{Pixel Received by Tom}}{\text{Total Number of Pixel Received by All Wallets}} \times \text{Weekly Issued 200,000 COL} = \text{Number of COL Tom Will Receive}$$

dApp Ecosystem

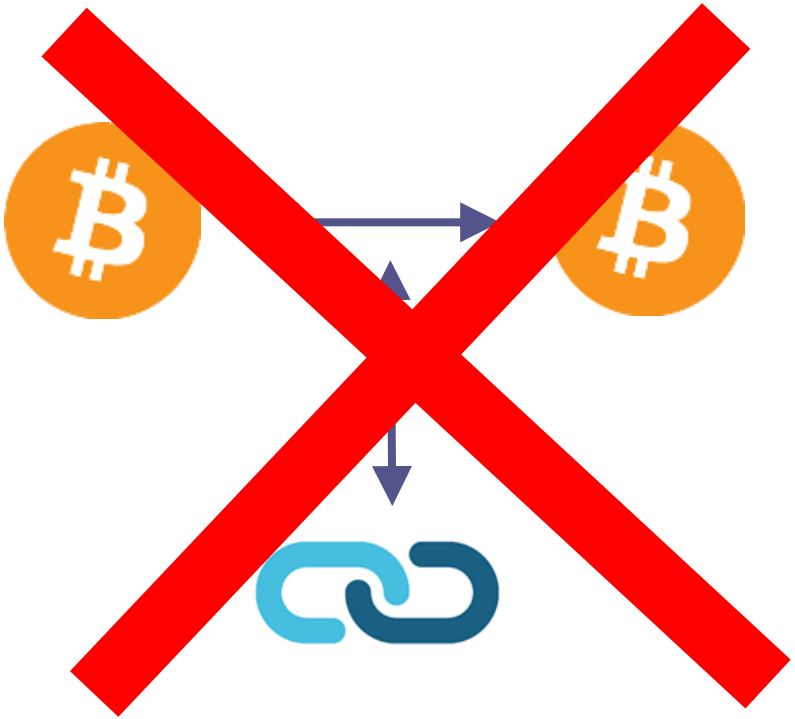
The dApp ecosystem will be powered by migrating existing successful applications to the blockchain, as well as making it easier than ever to launch your dApps on the blockchain.

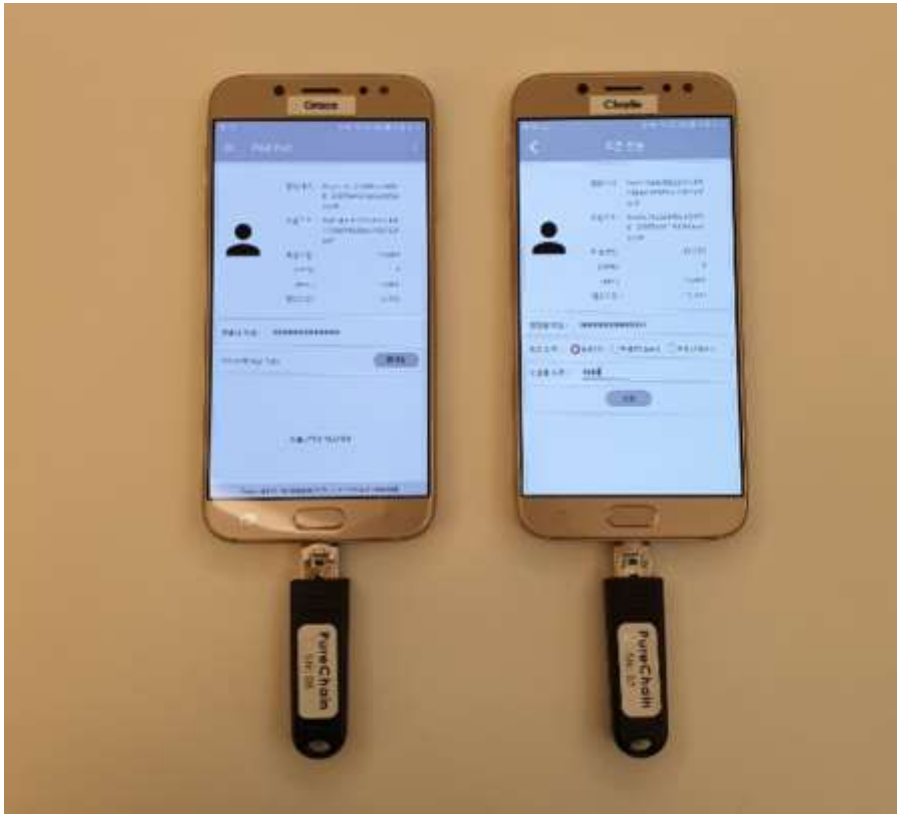




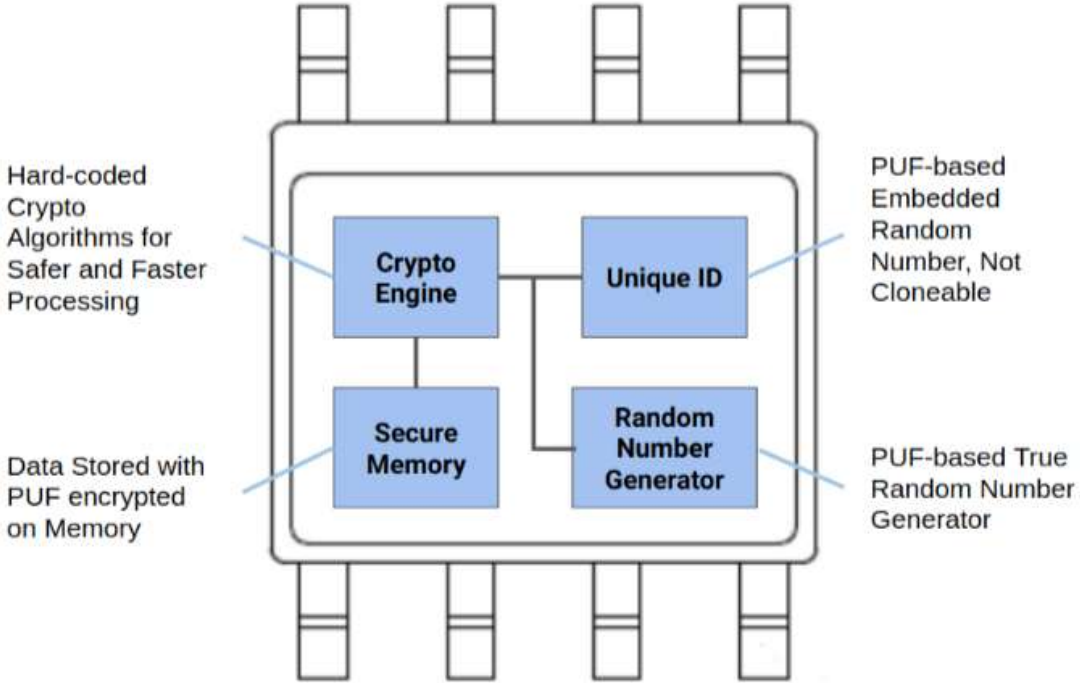
Color Pay

The true **Peer to Peer** digital currency





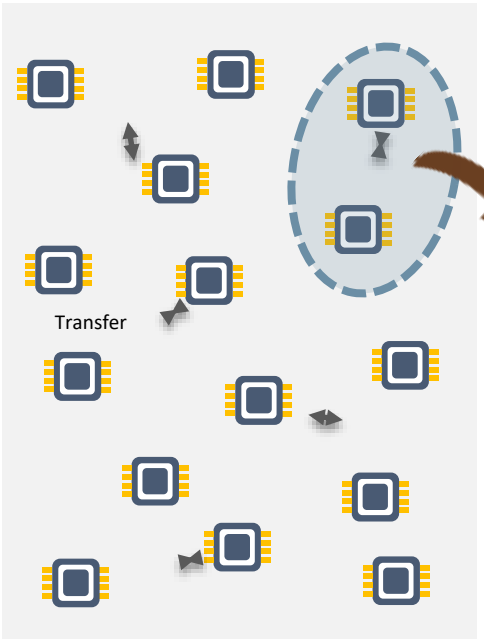
PUF Chip



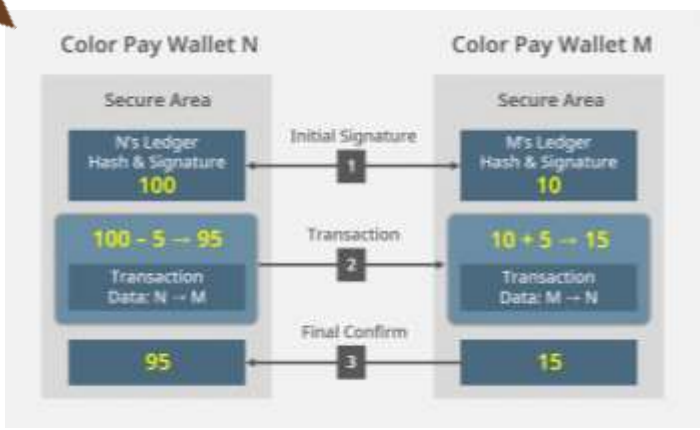
[Figure 2] PUF Chip internal structure

Color Pay

Color Pay is a payments network that combines unclonable hardware chips with a robust payment network that is both fast, and secure. It integrates hardware to improve both scalability and security.

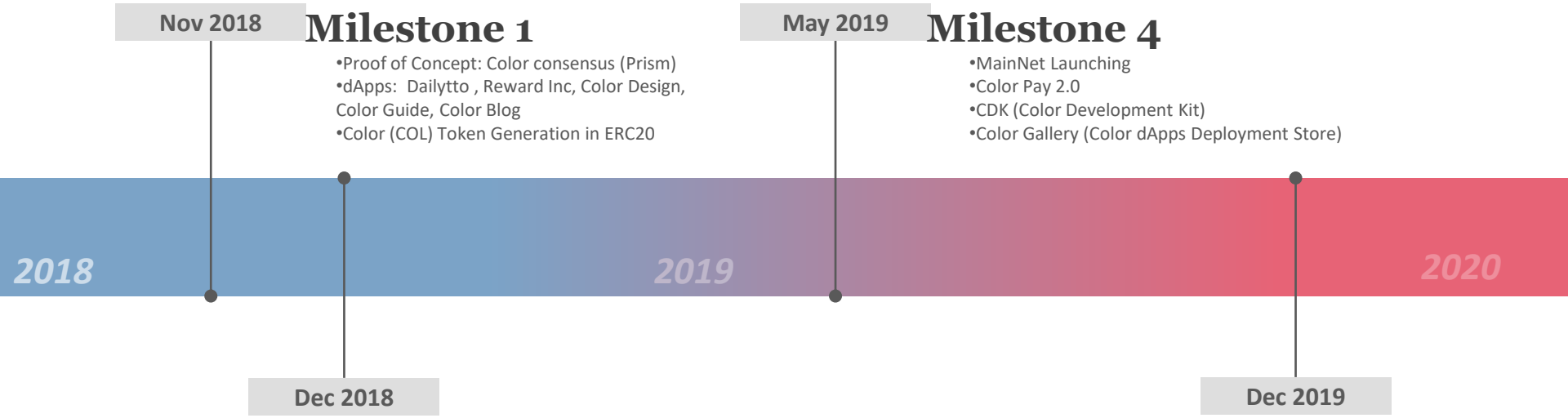


- No 3rd Party Consensus Needed
- Low Fees
- Infinite Scaling



Phases of Development

Follow the Innovative path of Color's Revolution



Conclusion

- Blockchain is slow and expensive as legers

- Blockchain is the most advanced social technology
- Blockchain establishes trust!
  - This is why crypto currency

Thank You!