

LECTURE 2

BLOCKCHAIN TECHNOLOGY EVOLUTION

THE PAST:

THE VENDING MACHINE DAYS

NEW USE CASES

Namecoin	2011	Decentralized domain name service
Bytecoin	2012	Privacy, first to use the CryptoNote algorithm
Dogecoin	2013	So Coin Much meme 
Aurora	2014	Digital currency for Iceland
Monero	2014	Privacy, CryptoNote, ring signatures

DIFFICULTIES IN IMPLEMENTATION


- ▶ Required copying, modifying and redeploying the bitcoin codebase every time.
- ▶ Required highly specialized developers, well versed in cryptography, security and decentralized system
- ▶ Required significant modifications of the core bitcoin system

SECURITY IN NUMBERS

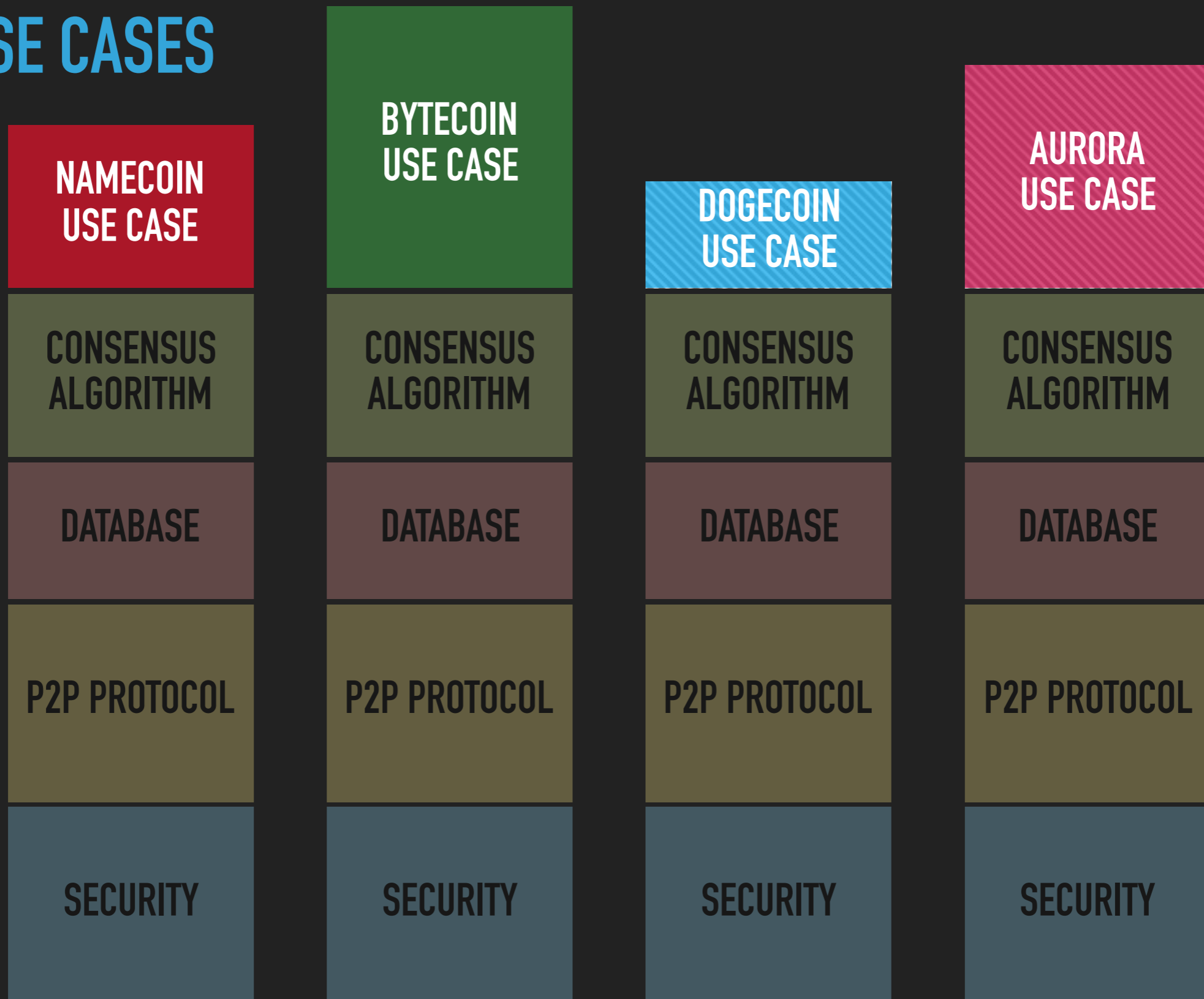
- ▶ Network security requires large number of nodes
- ▶ 51% attack
- ▶ Significant amount of miners has to secure the network

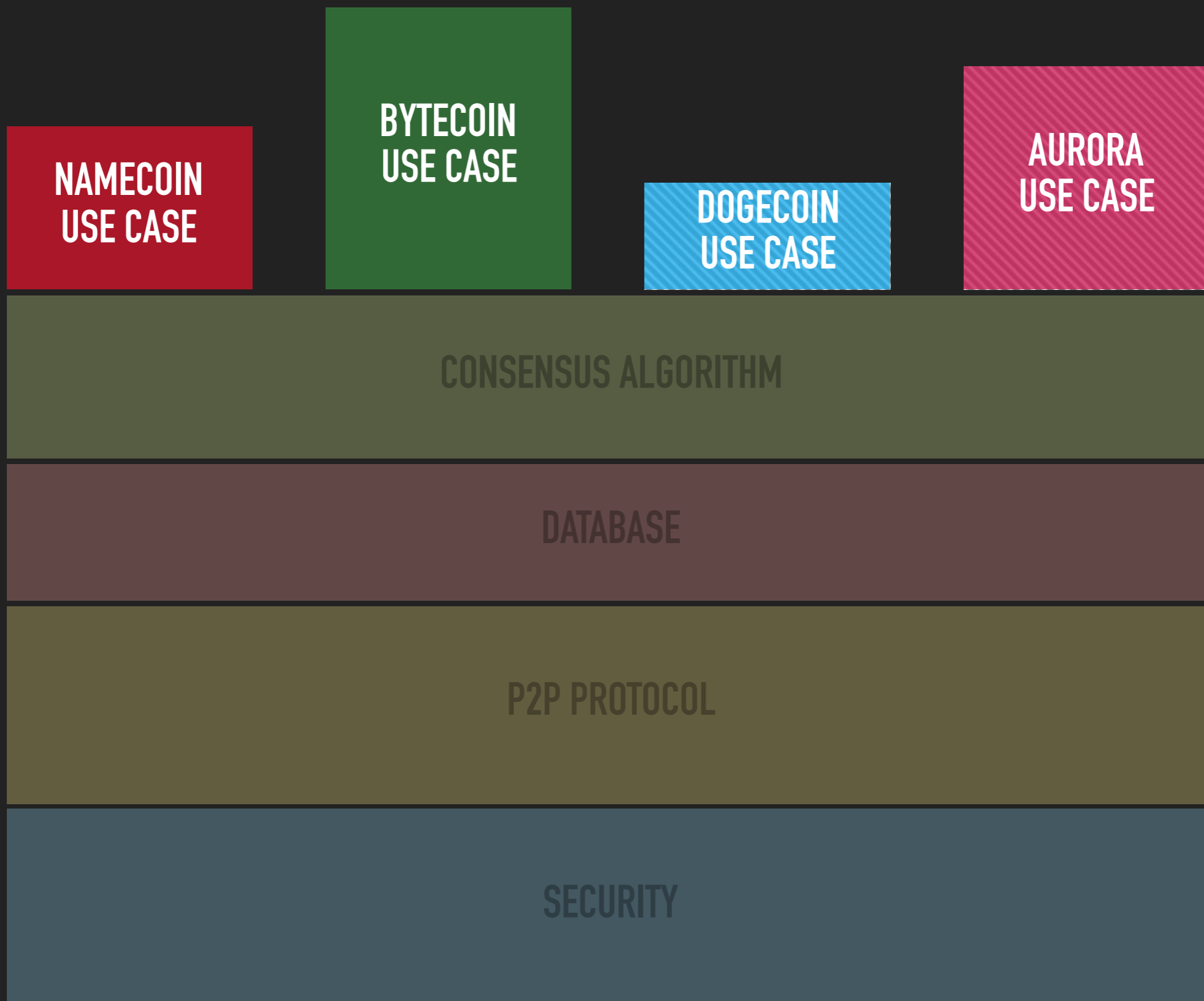


NEW USE CASES

	Use case	Blocks?	Needs Miners?	Decentralized?
Namecoin	Domain	✓	✓	✓
Bytecoin	Privacy	✓	✓	✓
Dogecoin		✓	✓	✓
Aurora	Iceland	✓	✓	✓
Monero	Privacy	✓	✓	✓

NEW USE CASES





**NAMECOIN
USE CASE**

**BYTECOIN
USE CASE**

**DOGECOIN
USE CASE**

**AURORA
USE CASE**



ethereum

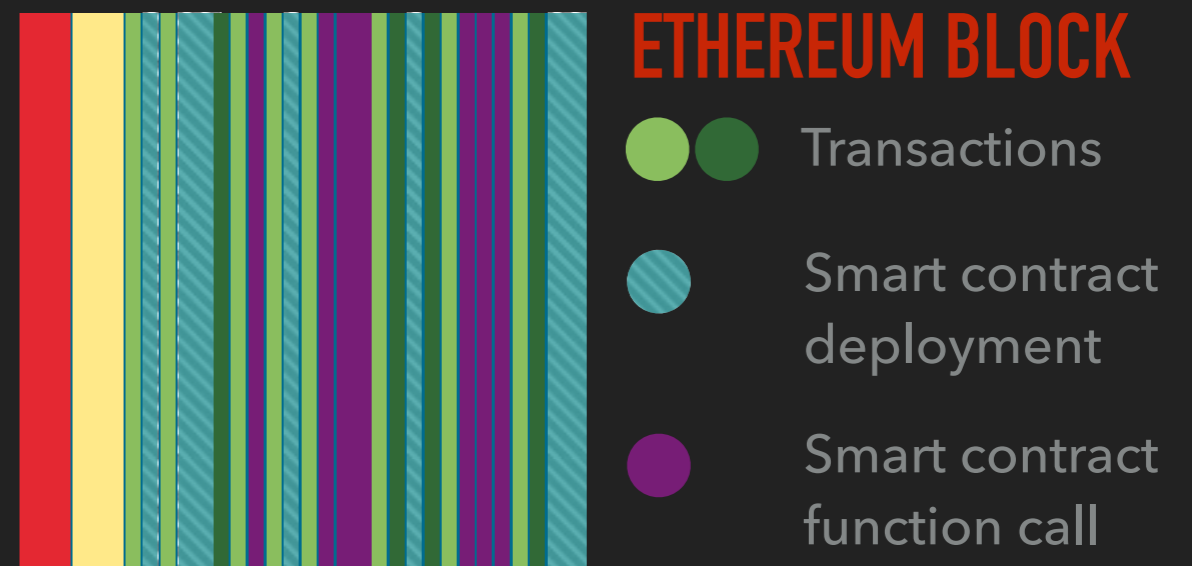
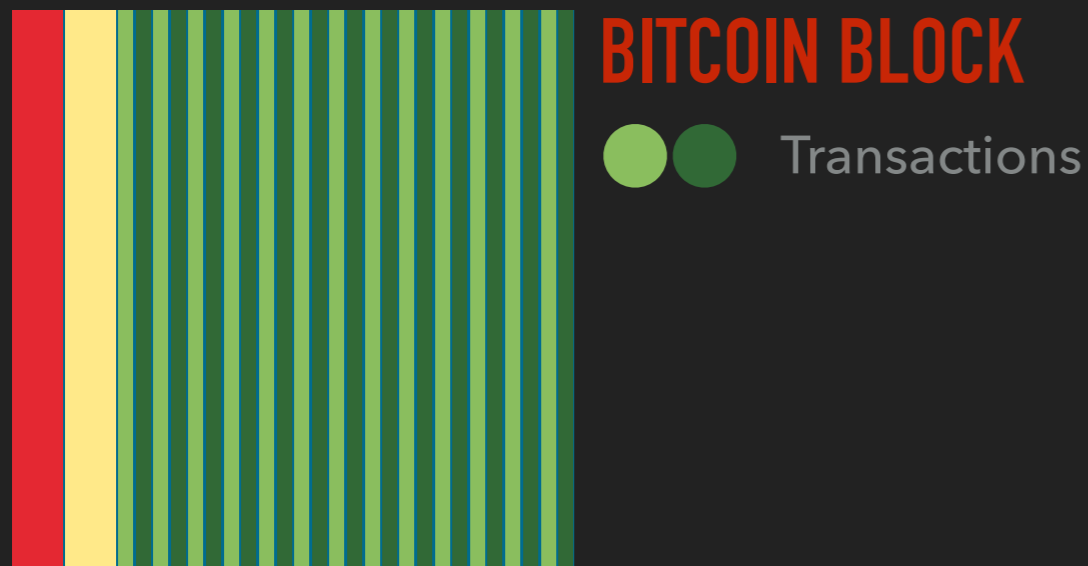
THE PRESENT:

MULTI PURPOSE BLOCKCHAINS

EVM — ETHEREUM VIRTUAL MACHINE

The EVM executes program code stored on the blockchain.

Ethereum processes different kinds of transactions:



DEMO












- ▶ Deploying a smart contract on a test net and interacting with it.
- ▶ Observing Blockchain transactions



APPLICATIONS ON THE BLOCKCHAIN

- ▶ Coins (Tokens)
- ▶ Multi signature wallets
- ▶ Exchanges
- ▶ ENS – Ethereum Name Server
- ▶ Kittens
- ▶ Autonomous Organizations
- ▶ ICOs

COINS

	Token	Price	%Change	MarketCap
1	 EOS (EOS) Infrastructure for Decentralized Applications	\$14.0958 <small>0.00106675 Btc</small> <small>0.011007 Eth</small>	▼ -16.03%	\$9,041,374,248
2	 Tron (TRX) TRON is a blockchain-based decentralized protocol that aims to construct a worldwide free content entertainment system with the blockchain and distributed storage technology.	\$0.0945 <small>0.00000672 Btc</small> <small>0.000070 Eth</small>	▼ -16.27%	\$5,212,020,721
3	 Qtum (QTM) Build Decentralized Applications that Simply Work. Executable on mobile devices, compatible with major existing blockchain ecosystem.	\$52.5112 <small>0.00072540 Btc</small> <small>0.006825 Eth</small>	▼ -2.51%	\$3,875,655,280
4	 OmiseGO (OMG) OmiseGO (OMG) is a public Ethereum-based financial technology for use in mainstream digital wallets.	\$21.1002 <small>0.00171440 Btc</small> <small>0.017819 Eth</small>	▼ -1.34%	\$2,458,245,805
5	 Binance (BNB) Binance will build a world class crypto exchange, powering the future of crypto finance.	\$21.4399 <small>0.00152521 Btc</small> <small>0.010122 Eth</small>	▼ -2.35%	\$2,122,850,259
6	 Status Network (SNT) Status is an open source messaging platform and mobile browser to interact with decentralized applications that run on the Ethereum Network.	\$0.4430 <small>0.00003151 Btc</small> <small>0.000028 Eth</small>	▼ -10.10%	\$1,537,445,141
7	 OxProject (ZRX) The Protocol for Trading Tokens	\$2.2674 <small>0.00016050 Btc</small> <small>0.001669 Eth</small>	▼ -0.32%	\$1,112,386,620
8	 Augur (REP) Augur combines the magic of prediction markets with the power of a decentralized network to create a stunningly accurate forecasting tool.	\$100.9150 <small>0.0017806 Btc</small> <small>0.071614 Eth</small>	▼ -6.27%	\$1,110,065,000
9	 Qash (QASH) We envision QASH to be the preferred payment token for financial services, like the Bitcoin for financial services. As more financial institutions, fintech startups and partners adopt QASH as a method of payment, the utility of QASH will scale, fueling the fintech revolution.	\$2.2504 <small>0.00010005 Btc</small> <small>0.001664 Eth</small>	▲ 10.92%	\$787,643,500
10	 GOLEM (GNT) Golem is going to create the first decentralized global market for computing power.	\$0.9228 <small>0.00000500 Btc</small> <small>0.000682 Eth</small>	▼ -3.96%	\$769,850,974
11	 Basic Attention Token (BAT) The Basic Attention Token is the new token for the digital advertising industry.	\$0.7020 <small>0.00000921 Btc</small> <small>0.000019 Eth</small>	▼ -6.38%	\$702,009,000

COINS

- ▶ Coins are Smart Contracts
- ▶ Current standard: ERC20
- ▶ Same or better than a bitcoin fork
- ▶ Contract code is visible and readable by anyone ([example: HelloGold token code](#))
- ▶ The visible and auditable code creates **accountability**.

MULTISIG WALLETS

- ▶ Every smart contract on ethereum can hold ether
- ▶ A multisig wallet is a smart contract that requires the signature of multiple parties before making a transfer
- ▶ Another system wide functionality implemented on the application layer
- ▶ **Autonomous behavior!**

EXCHANGES

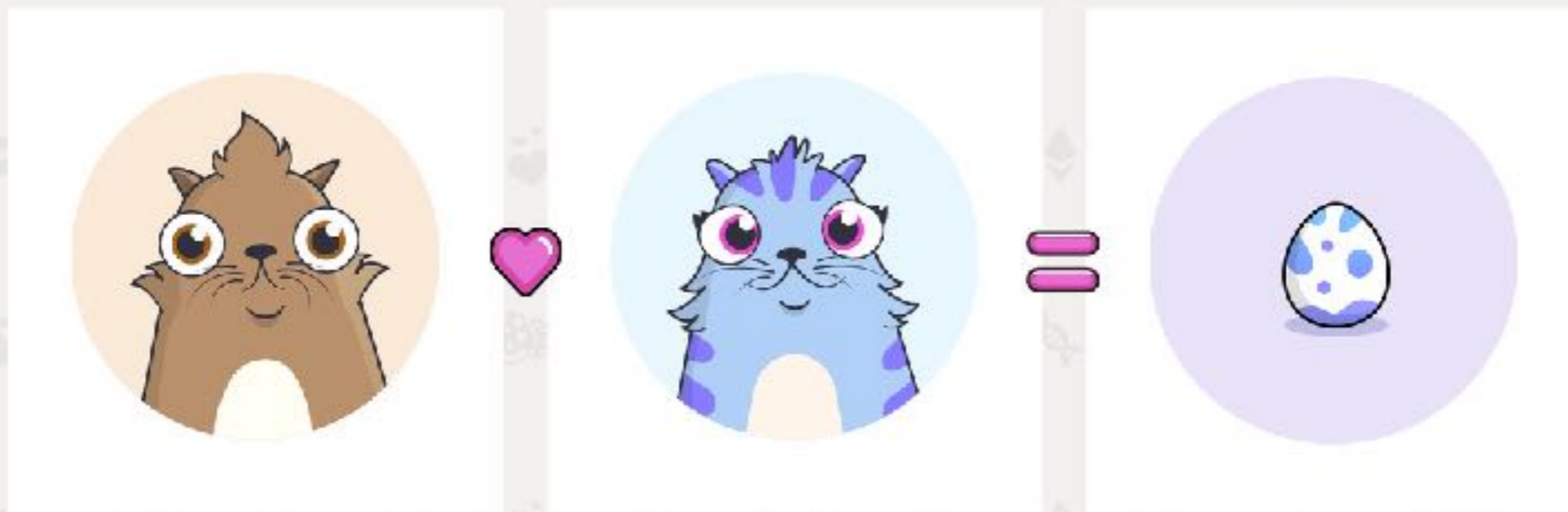
- ▶ Exchanges are the major source of centralization
- ▶ Therefore a major source of trouble
- ▶ Decentralized exchanges already exist
- ▶ Scalability is a problem
- ▶ Functionality will be implemented at the protocol level

ENS - THE ETHEREUM NAME SERVER

- ▶ Another critical piece of infrastructure implemented on the application level, as a smart contract
- ▶ Equivalent in functionality to Namecoin or DNS servers
- ▶ Completely decentralized
- ▶ DEMO

KITTENS AND OTHER GAMES

- ▶ Gambling and trading games
- ▶ More use cases once the scalability issues are solved.



THE FUTURE: AUTONOMOUS ORGANIZATIONS

- ▶ The DAO
- ▶ Real Collaborative Economies

ICOS (FINALLY!)

- ▶ Originated from crowd sourcing campaigns
- ▶ The first “killer application” on blockchain. (But not the last)
- ▶ Builds on all previous discussed use cases:
 - ▶ accountability
 - ▶ removes the 3rd parties
 - ▶ Needs coins
 - ▶ Needs wallets

CONCLUSION

- ▶ Past: Single purpose blockchains
- ▶ Present: Multi purpose blockchains
- ▶ Future: Autonomous Organizations
- ▶ Abstracting out the framework enables faster and simpler implementation of use cases
- ▶ Use cases naturally build upon each other

CONCLUSION 2: KEY FEATURES

- ▶ Accountability
- ▶ Removal of 3rd parties
- ▶ Autonomy

THANK YOU

© 2018 ANDRAS KRISTOF

TWITTER, MEDIUM: @AKOMBA, EMAIL: A@AKOMBA.COM