

Blockchain & Web 3

BlockchainHub ■ Dr. Shermin Voshmgir

Web 1
Communication

Read

Web 2
Interactions

Read
Write

Web 3
Contracts

Read
Write
Execute

Web3

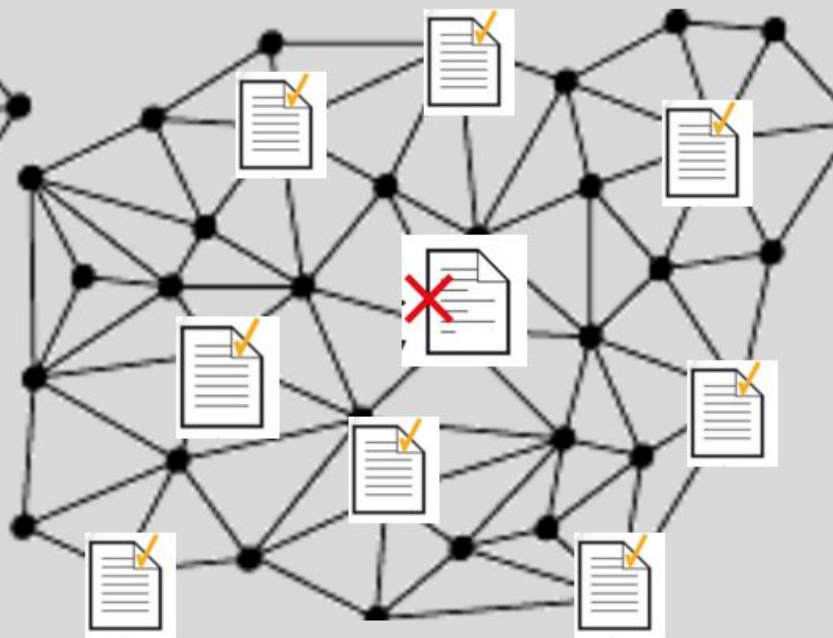
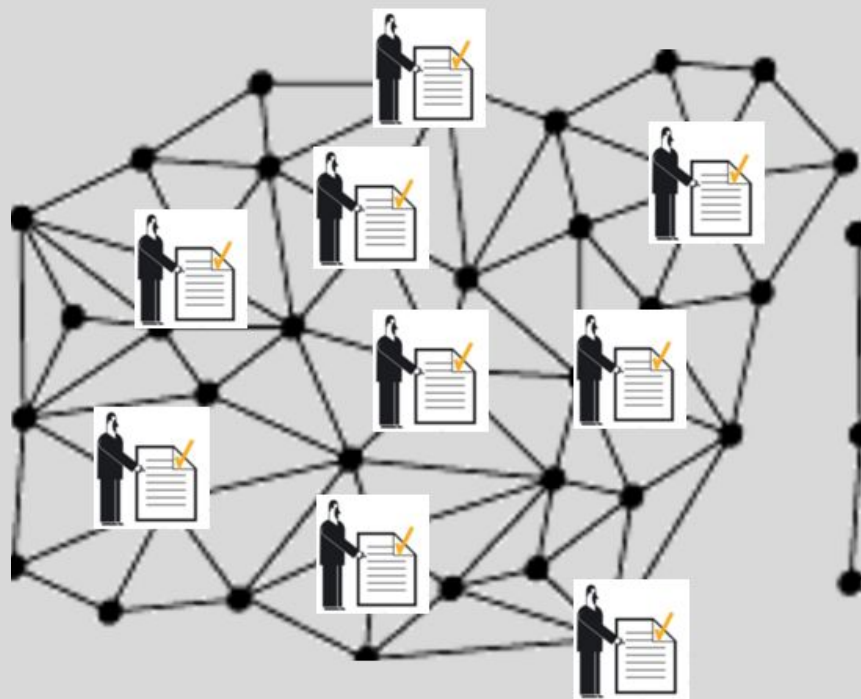
- **New Data Structures**
- **Governance Machine**
- **Tokens as Killer App**



**Data
Monarchy**
Server



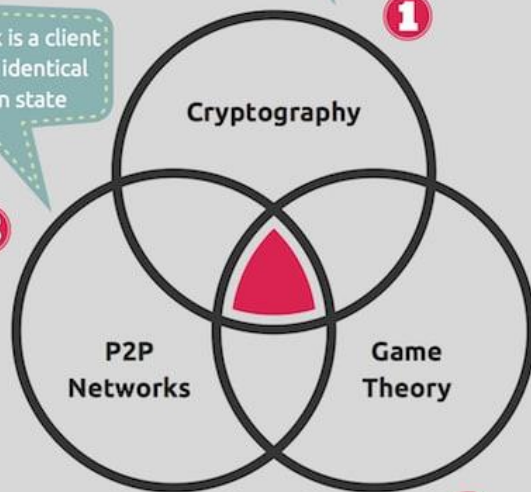
**Data
Democracy**
P2P Networks



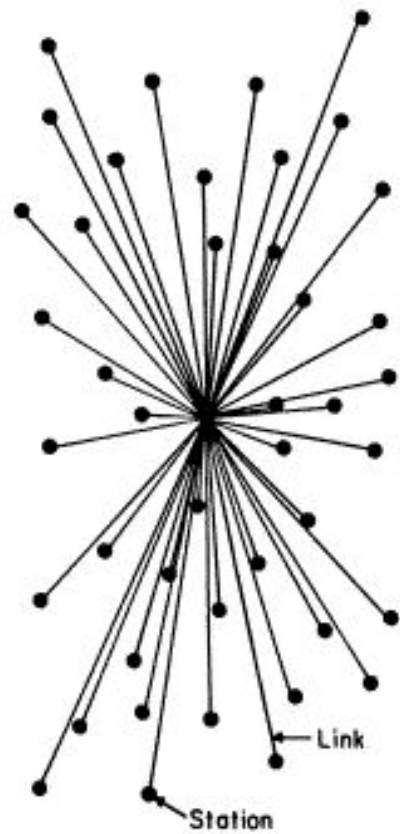
Use of public key cryptography and cryptographic hash functions: essential for transparency & privacy

Every node of the network is a client as well as server, holding identical copies of the application state

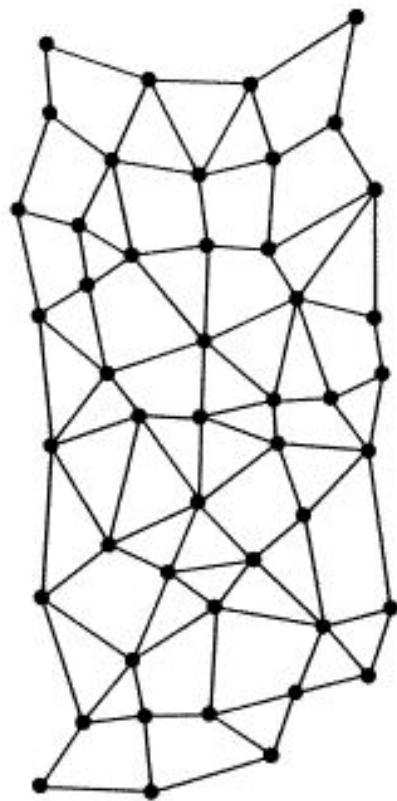
3



Nodes of P2P Network validate transactions by consensus, following economic incentive mechanisms (Proof of Work, Proof of Stake, etc.)



CENTRALIZED
(A)



DISTRIBUTED
(C)

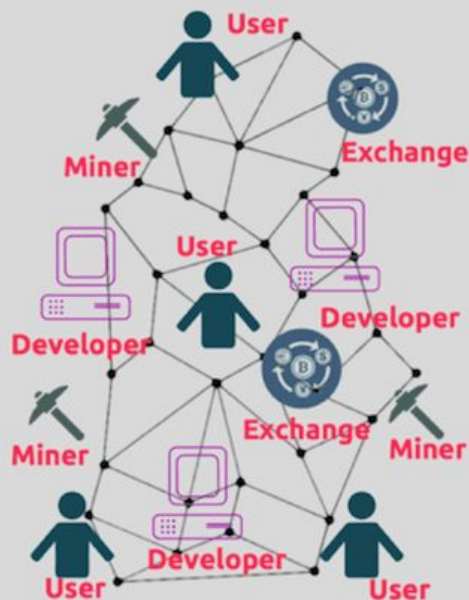
Traditional Top Down Organizations



Top Down Management

One legal entity
Employment contracts

Decentralized Autonomous Organizations



Distributed Network of Autonomous Stakeholders

No centralized legal entity!
No employment contracts!

RECORD OF TRANSACTIONS

Assets



File containing all information since block 1 - tracking all asset movements.

CONSENSUS RULES

Governance



Defining game theoretical behavioural rulesets of all actors in the network

P2P NETWORK OF COMPUTERS

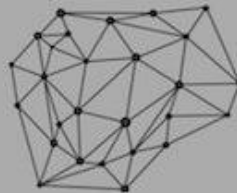
Physical Network



A network of all devices running the blockchain protocol, and keeping records of transactions

BLOCKCHAIN LAYER

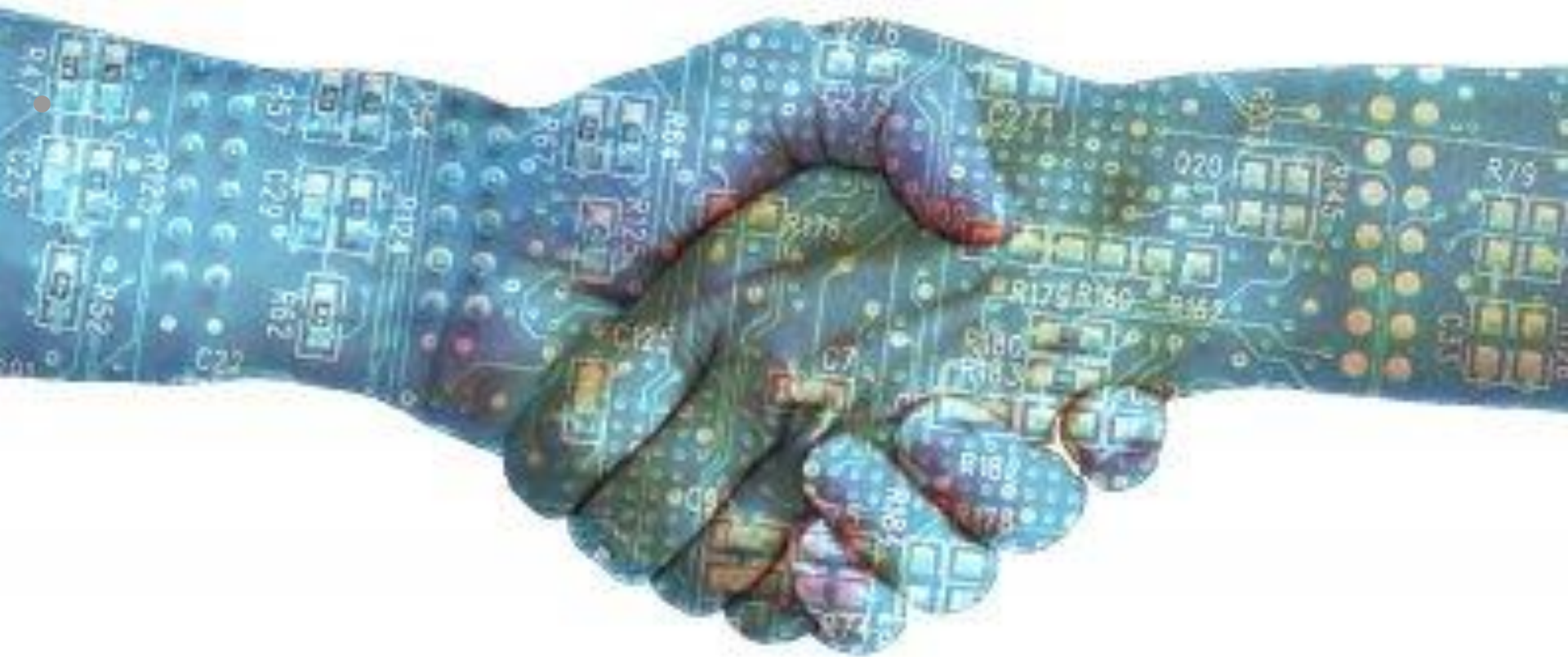
TCP/IP
Infrastructure



INTERNET LAYER

Smart Contracts

Rule of Code







[Blurred text from the top of the page]

Assignment. The Contractor shall not assign, subcontract, or otherwise transfer its obligations under this Agreement, or delegate the performance of any of the obligations hereunder, without the prior written consent of the Commission.

SIGNATURE



```
address public minter,  
mapping (address => uint) public balances;  
  
// Events allow light clients to react on  
// changes efficiently.  
event Sent(address from, address to, uint amount);  
  
// This is the constructor whose code is  
// run only when the contract is created.  
function Coin() {  
    minter = msg.sender;  
}  
function mint(address receiver, uint amount) {  
    if (msg.sender != minter) return;  
    balances[receiver] += amount;  
}  
function send(address receiver, uint amount) {  
    if (balances[msg.sender] < amount) return;  
    balances[msg.sender] -= amount;  
    balances[receiver] += amount;  
    Sent(msg.sender, receiver, amount);  
}
```



-----BEGIN PRIVATE KEY-----

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBANLslcT4md+HTRdJ5Q7tbIGoERSG
uYe3E4LWmL+8efrCsG69y3N5R2e8UB0PoCRJNpQif/cVcnLQG0f4+IkeVTQpFmTsJPJTWmQsTsAW
AMWAo0IrskyI0To+Xnd9rUMdlhXACdjend4v9fhtj7Thtnr6yemiBHcSzaFX86y0B12bAgMBAaec
gYBqta8gy7TtRYJW+eeMuclffyvE+rP6WUDhvLfiqPP9TWn9XMAFV6IsdTUCvtkCApg+MYYT9yHD
vE1RCECU/meT5MeeaCUZXvilePue+FLgU83Wfy8W/Qo7r0luIFHdu25Z9I9zcbAHcwS8K0WabIKc
v80Rcblc3W/AL3a0BntEoQJBA0/c8xMDbJgnjcdRCEnr4ajlEscov1YvDzJncUu2tfGVcPDxD+ZE
xrLnP5vmDYg51BjaLvjyxwlZwXnyz05Vt/OCQQdhHYAuKMS8FFX9vDpoR7h10BzAAYZp11W0V7h
I5CfNAhDzDkKW43AeflKGQpRQ8GWPI9ZvIziXQHwS+7eqGN3AkBjsoq2FG5Gr+oTgs7XKtwYxgSQ
Ewx6HgVLBgPpXIAzcdIH06qwI1YTdlrSCcUGIiiUS9vKTd6+hdgNQAc6oBZhAkBfGX1bArIJ2nVx
WaE7CIfuk9pxar0DzADSzGjPB51DBFIxggbez0qU83QDZ4yqQ/t2ImNUv4is4Cm/f/SLb4uFAkEA
xzh2beww/lGGY+CyFw2NooKSreJSp8Blal1BcNo2507BRTmdk+BTJLOAcM4h2HvwYGrSBk/VPAsZ
T48dmV94Tw==

-----END PRIVATE KEY-----

Close



Software Oracle

Big Data
AI

Smart Contracts

Software Oracle

Big Data
AI

Internet of
Things

Hardware Oracle

Internet of
Things

Hardware Oracle

Energy
Commerce
Banking
Insurance
eGovernment
Education
Telecom
Healthcare

Gambling & Gaming

Ethereum Technology Stack

Application Layer

Ethereum Blockchain Layer

Internet Layer



App
Tokens
Smart contract
based



Ether
Native
BC Token
























CryptoCurrency Market Capitalizations



Join ICO now!
First ever tokenized closed-end fund

Market Cap - Trade Volume - Trending - Tools - 

All - Currencies - Assets - **USD** Next 100 → View All

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$18,220,705,965	\$1120.95	16,254,700 BTC	\$516,351,000	-1.04%	
2	 Ethereum	\$4,088,579,992	\$45.23	90,401,309 ETH	\$175,215,000	-2.49%	
3	 Ripple	\$1,245,259,154	\$0.033194	37,514,472,563 XRP *	\$115,785,000	-27.13%	
4	 Dash	\$512,483,943	\$71.12	7,205,540 DASH	\$34,356,100	10.00%	
5	 Litecoin	\$407,660,571	\$8.07	50,487,282 LTC	\$129,736,000	-4.99%	
6	 Monero	\$289,261,240	\$20.32	14,234,947 XMR	\$6,584,760	0.98%	
7	 Ethereum Classic	\$240,283,625	\$2.66	90,360,725 ETC	\$6,695,530	-1.49%	
8	 NEM	\$159,263,100	\$0.017696	8,999,999,999 XEM *	\$1,473,850	-11.56%	
9	 Augur	\$115,602,300	\$10.51	11,000,000 REP *	\$1,608,290	-8.32%	



scalable smart contracts interfacing with real world data

Get AE Token

Phase 1 of Contribution Campaign Starts 3rd of April (lasting 72 hours)




ONLY TODAY
10 RLTY
GET

- **Transparency**
all actors have access to same information
- **Reduction of transaction costs**
auditing, compliance, enforcement
- **Automated coordination**
Decentralized Autonomous Organizations

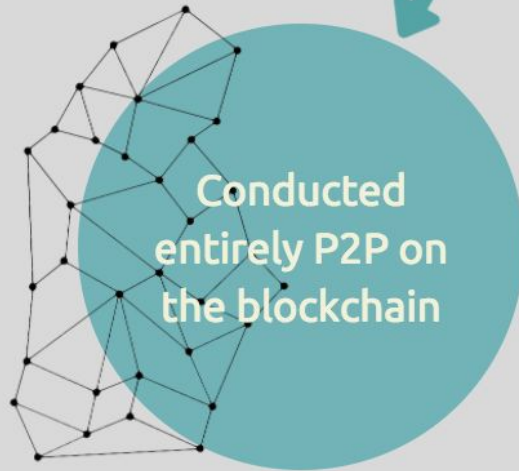
Permissioned vs Permissionless

Faster
Managed upkeep
Private membership
Trusted
Legal



Slower
Public ownership
Open & transparent
Trust-free
Illegal

ICOs



Web2

Web3

Business plan



Whitepaper

Elevator pitch
& Personal intro



Twitter
Website Telegram
Slack Github

Institutions



Everyone

VC



ICO



History of ICOs



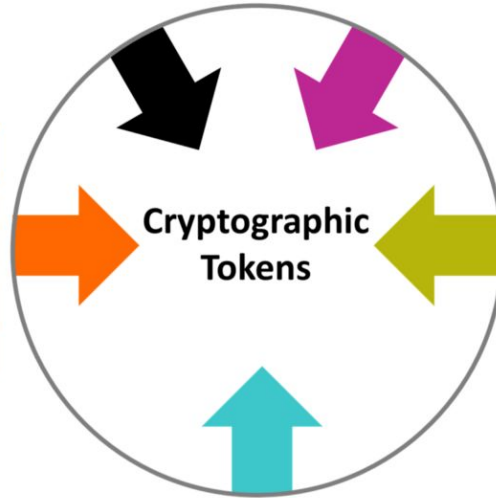
Total market cap: **\$312 Million** (Total coin supply: 10 Million)

- **Native Blockchain Tokens**
- **Application Tokens (Usage Tokens)**
- **Asset Backed Tokens**

Purpose	
What is the token's main purpose?	
Cryptocurrencies	
Network Tokens	
Investment Tokens	 

Utility	
What utility does the token provide?	
Usage Tokens	 
Work Tokens	
Hybrid Tokens	

Technical Layer	
On which system layer is the token implemented?	
Blockchain-Native Tokens	
Non-native Protocol Tokens	 
(d)App Tokens	



Legal Status	
What is the token's legal status?	
Utility Tokens	
Security Tokens	 
Cryptocurrencies	

Underlying Value	
Where does the token derive its value from?	
Asset-backed Tokens	
Network Value Tokens	 
Share-like Tokens	

New Asset Class
Fluctuates between currency,
commodity, utility, security

Banking

blockchains as
record of who owns what
instead a series of internal ledgers

- **Bitcoin Blockchain**
 - transactions (few cent vs. 5-10%)
 - faster (m/seconds vs. days)
 - censorship resistant (Russia...)
 - more secure: hard to quantify
- **Fintech Use Case**

Santander Bank reckons that it could save banks up to \$20 billion by 2022



eGovernment

- Self Sovereign Identity
- Public Registries: Land registries,, Marriage Cerificates,...
- Transparency
- Participation
- eVoting



Online Notaries

Registers of the ownership

- Documents
- Luxury goods
- Works of art



Energy

Energiewende in Deutschland

- P2P Energy Trading
- Smart Grids
- Mobile Charging



IoT

User Access Control
for machine to machine
smart contracts



Accounting

Revolution

Auditing & Compliance

On the fly, no after the fact

Cooking the Books?

Less human errors

Faster taxation cycles

Business Process & Supply Chain

#Disintermediation

#Transparency

#Provenance

Insurance

P2P Insurance

- Automated **claims handling**
 - **Reliable & transparent payout mechanism** for the customer
 - **Contract-specific rules** can be used to enforced
 - **Self Sovereign Identity:** Improve customer engagement
 - More effectiveness **fraud detection & pricing**
 - **Emerging markets:** Cost-efficient product offerings
 - **IoT:** New insurance products
-

Telekom

Carrier study Blockchain Group
Consortium of
Sprint, SoftBank, and FarEasTone

- **Cost savings:** billing, provisioning
 - **Fraud Prevention:** identity management & KYC
 - **Smart Cities & IoT**
 - **Connectivity provisioning:** instantaneous micro contracts for WIFI Access
 - **Mobile Payment:** Bitpesa, phone-to-phone payments, Bitcoin converted into local currency
 - **Identity Provider:** IaaS
 - **Payment Provider:** smart wallets
 - **Loyalty Programs**
-

E-commerce

- **Logistics**
- **Transparency**
- **Authenticity & anti-counterfeiting**
- **Proof of ownership and resale**
- **Loyalty**
- **Payments**
- **Insurance**



It's like 1990 for the Internet

we don't know how this will pan out
but the future is likely to be much more #decentral

WU

VIENNA

**INTERDISCIPLINARY
RESEARCH INSTITUTE
FOR CRYPTOECONOMICS**

Website: <http://wu.ac.at/cryptoeconomics>

Twitter: @crypto3conomics

Likedin: @crypto3conomics

Facebook: @crypto3conomics

Our Team

3 researchers in management team
16 professors from 8 WU departments
30 researchers from WU in total



Learing Resources

blockchainhub.net

 blockchainhub

 @blockchainhub

Shermin Voshmgir

 @sherminvo

 @sherminvoshmgir