

Blockchain for Innovative Peer to Peer Business Models

Zonyin Shae

Department of Computer Science and Information Engineering
Asia University
Taichung, Taiwan

zshae1@gmail.com

About Speaker

- Name: 薛榮銀 (*Zonyin Shae*)
- Chiao-Tung University (BS and MS)
- University of Pennsylvania (PhD)
- 24 years at IBM Watson Research Center, NY
- 4 years at ILL (R&D Director and Director of Cloud Business Center)
- From 2016 at Asia University (Chair Professor)

Outline

- **Introduction to Blockchain**
- **Bitcoin - Crypto Currency**
- **Blockchain Core Components**
- **Distributed Application Flow**
- **Applications**
- **Challenges**
- **Summary**

Introduction to Blockchain

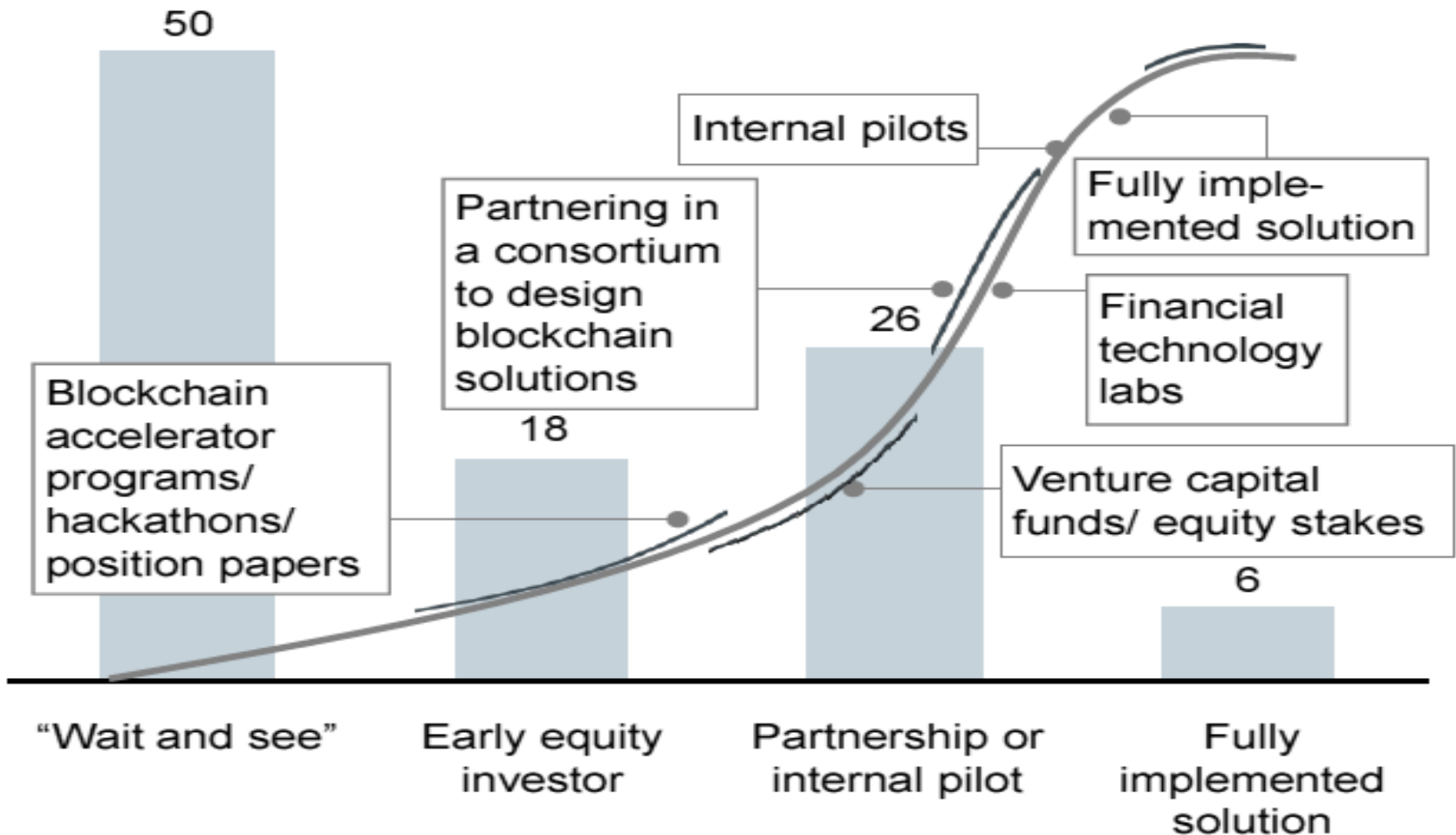
Trend

- 10% of global world GDP will come from blockchain based business activities before 2027 (WEF)
- Centralized platforms and applications via current Internet (via UDP/TCP/IP and HTTP) has created various business models, economy, and job opportunity. (e.g., Amazon, Uber, Airbnb, banks, Yahoo, Facebook, Google, etc.)
- Blockchain de-centralized technology will replace applications that currently need 3rd party, and provide new innovative business model based on distributed trust platform.
- Transcending the current internet into even higher level of de-centralized business value of next generation of Internet.

McKinsey Survey of Finance Execs Early 2016

One half of Institutions are in 'Wait & See' mode

% of respondents¹



Startup Market Map 2-2017

BITCOIN & BLOCKCHAIN STARTUPS MARKET MAP

WALLETS & MONEY SERVICES



EXCHANGES & CRYPTOCURRENCY TRADING



P2P MARKETPLACES & P2P LENDING



MERCHANT SERVICES



ENTERPRISE SERVICES & CURRENCIES



SOCIAL & BROWSERS



CRYPTOCURRENCY MINING



IoT, IDENTITY & CONTENT MANAGEMENT



STORAGE, SECURITY & REGULATORY



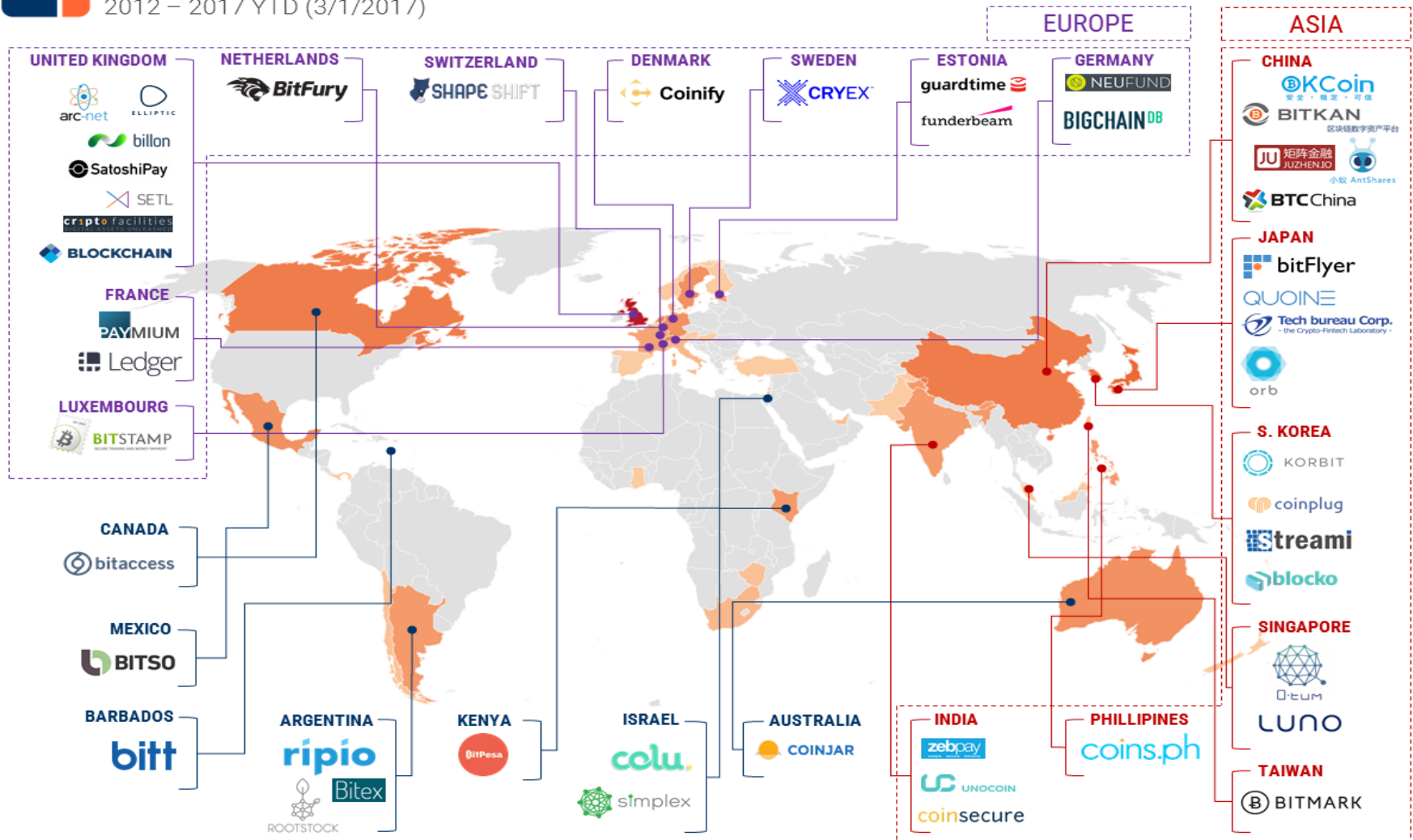
CAPITAL MARKETS & FINANCIAL SERVICES



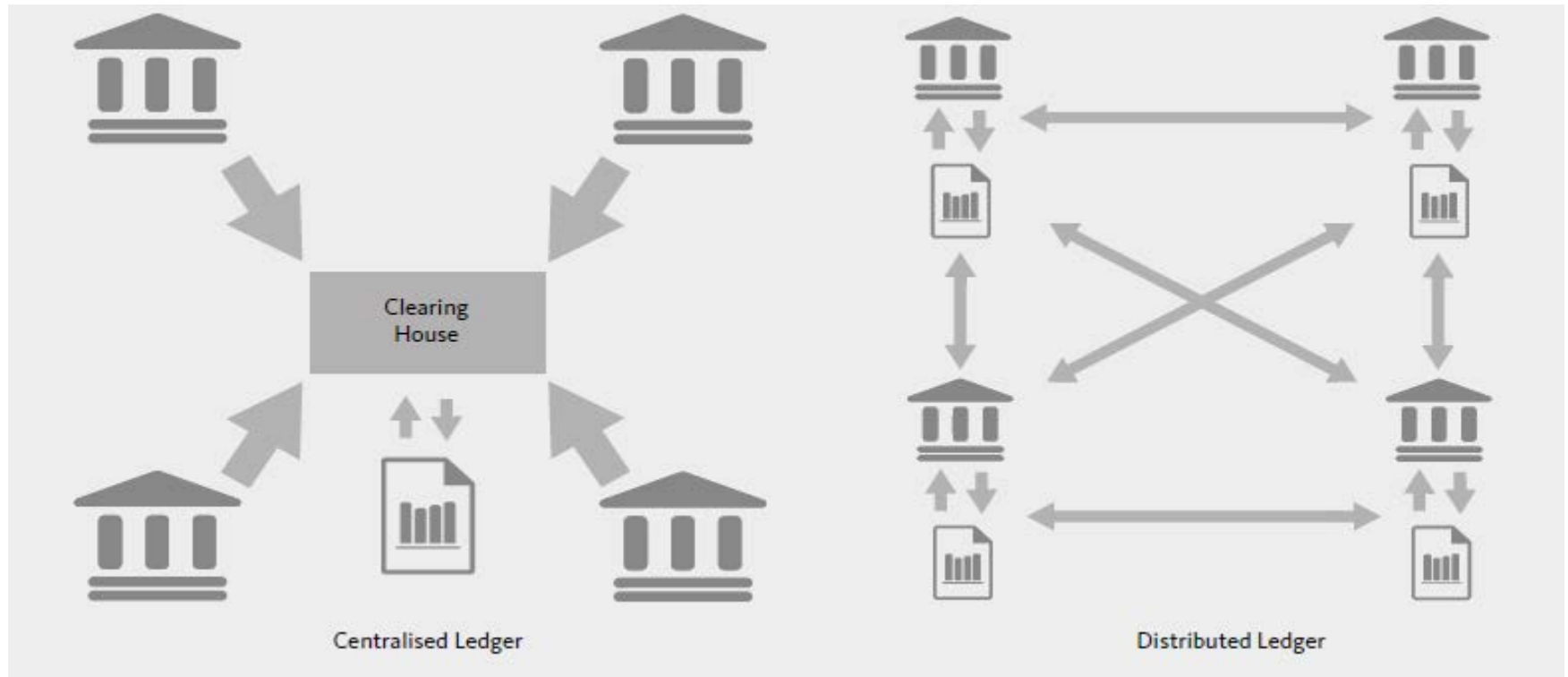
CBINSIGHTS

Global Bitcoin/Blockchain Companies 3/2017

GLOBAL BITCOIN & BLOCKCHAIN COMPANIES 2012 – 2017 YTD (3/1/2017)



Basic Change to Business Process



- Core technology behind Bitcoin, but its value is far beyond
- Distributed ledger, Distributed trust
- Smart contract
- **Records can not be modified, and can not be denied**

Centralized Trust

- With the Internet of information we have to rely on powerful intermediaries to establish trust.
 - Banks, governments and even social media companies like Facebook work to establish our identity and ownership of assets. They help us transfer value and settle transactions.
 - Limitations.
 - Centralized servers, which can be hacked.
 - Take high fee for their services—say 10% to send money
 - Capture our data, not just preventing us from monetizing it, but often undermining our privacy.
 - Sometimes unreliable and often slow.
 - Exclude two billion people who don't have enough money to justify a bank account.
 - In sum, they capture a lopsided share of the benefits of the digital economy.

Peer-to-Peer Exchange of Value

- What if there were a second generation of the Internet that enabled the true, peer-to-peer exchange of value?
- Currently,
 - If I'm going to send some money to somebody else, I have to go through an intermediary—a powerful bank, a credit-card company
 - I need a government to authenticate who I am and who you are.
- What if we could do that peer to peer?
 - Distributed trust protocol
 - Enabling transactions, commerce, exchange money, without a powerful third party

Distributed Trust - Blockchain

- Blockchain, the first native digital medium for peer-to-peer value exchange.
- Ensure the integrity of the data traded without going through a trusted third party.
- Trust is hard-coded into the platform.
 - Trust Protocol.
 - in the form of globally distributed computations and heavy duty encryption.
- It acts as a ledger of accounts, a database, a notary, a sentry and clearing house, all by consensus.

Bitcoin - Crypto Currency

Notable Electronic Payment Systems and Proposals

ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Satoshi Nakamoto

- Satoshi started coding Bitcoin around May 2007.
- He registered the domain bitcoin.org in August 2008.
- At that time, he started sending private emails to a few people who he thought might be interested in the proposal.
- In October 2008, he publicly released a white paper that described the protocol, and then soon after, he released the initial code for Bitcoin
- October 2008 – December 2010
 - He posted lots of messages on forums, emailed with lots of people, and responded to people's concerns. On the programming side, he submitted patches to the code.
 - He maintained the source code in conjunction with other developers, fixing issues as they arose.
- By December 2010, others had slowly taken over the maintenance of the project, and he stopped communicating with them.

Bitcoin Properties – Pseudo Anonymous

- Bitcoin is not anonymous to the same level as cash is.
- Don't need to use real identity to pay in Bitcoin,
- Transactions can be tied together based on the public ledger of transactions with clever algorithms
- Linked to your identity if not careful.
- ZeroCoin/ZeroCash make the transactions unlinkable (but need a different blockchain network)

Bitcoin Properties – Decentralized

- Bitcoin allows directly user-to-user/merchant transactions.
- The support for user-to-user transactions probably contributed to Bitcoin's success.
 - send it to other users, while the community tried to drum up support for Bitcoin and get merchants to accept it.
- Bitcoin transaction is an online transaction
 - It doesn't require a central server
 - Rely on a peer-to-peer network which is resilient in the way that the Internet itself is.

Market Price of Bitcoin (8/28)

Bitcoin (USD) Price

Closing Price ☐ OHLC

1h

12h

1d

1w

1m

3m

1y

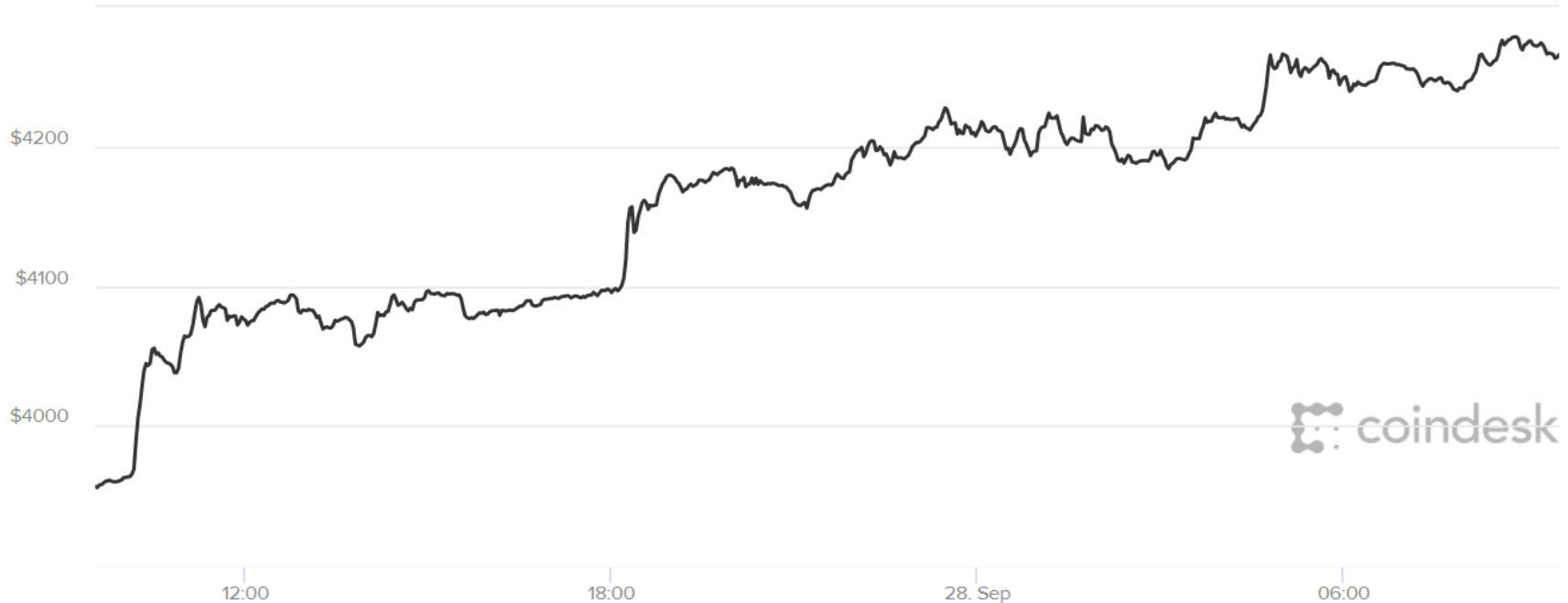
All

Sep 27, 2017

to

Sep 28, 2017

Export



coindesk

\$4,265.61 ▲ 1.36%

Today's Open

\$4,208.56

Today's High

\$4,278.78

Today's Low

\$4,183.40

Change

▲ \$57.05

Market Cap

\$70.77B

Supply

16,591,550

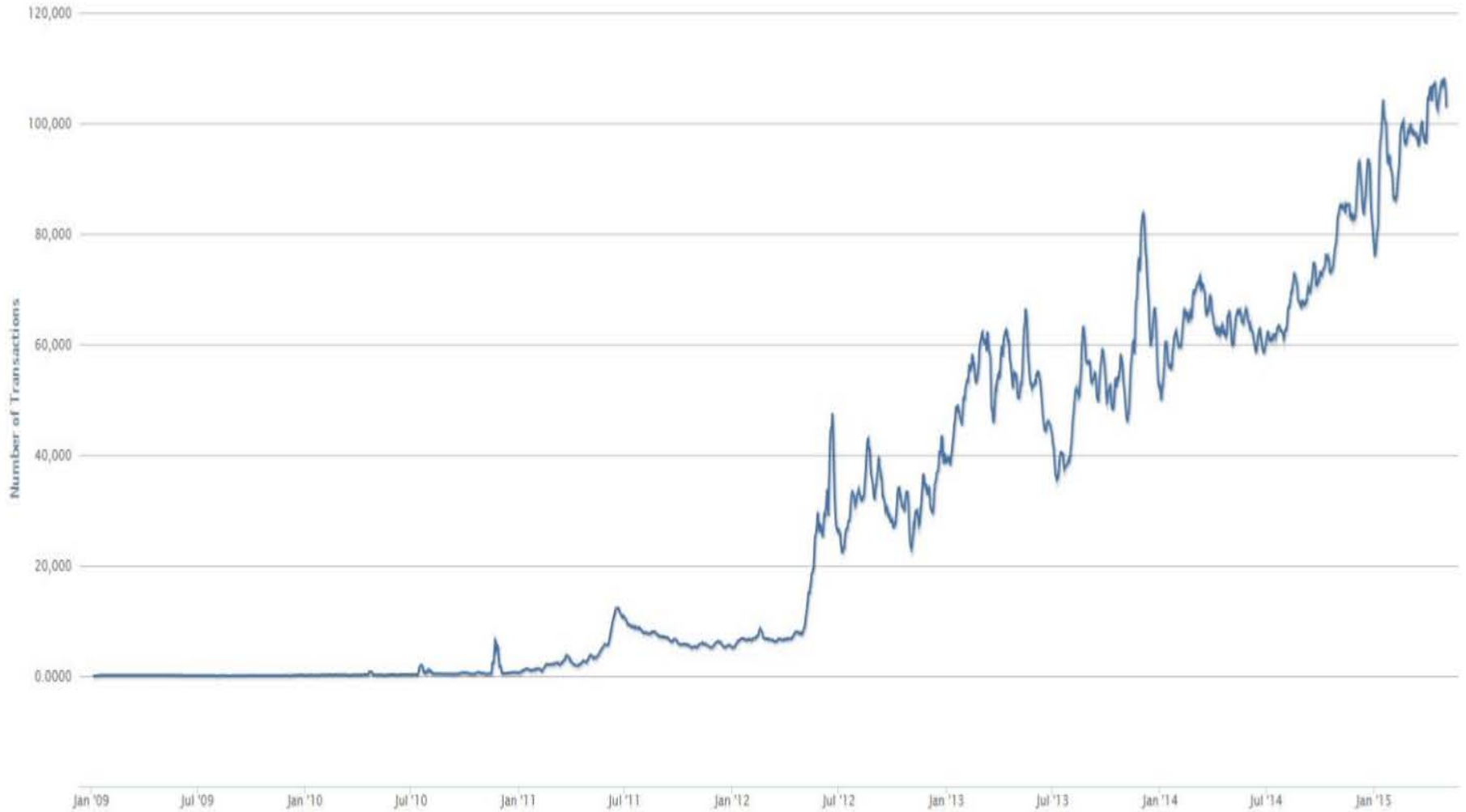
Market Price of Bitcoin (all)



Market Price of ETH (all)



Daily Transaction Volume



Daily transaction volume (7-day average). Source: bitcoincharts.com.

Virtual Currency

≠

Blockchain

Blockchain Core Components

Blockchain Core Components

- Minting Money out of Thin Air
- Recording Everything in a Ledger
- Distributed Consensus
- Smart Contract

Smart Contract

User → Merchant → Miners → [Block] → [Runners]

reserve a room with Expedia
User sent payment, in bitcoins, to Expedia
The transaction is broadcasted to all Miners
Miners package this transaction, along with others, in a bid to build a block (in every 10 minutes)
Miners race to solve the difficult mathematical puzzle

Distributed Consensus

[Block] → [Miner] → [Blockchain]

The winning miner seals off a completed block of transactions and broadcasts their proof of work to the network
The other miners check the proof of work and confirm the authenticity of the work
Blocks are hashed together in one long, unbreakable, record of activities, this is blockchain

Minting Money out of Thin Air **Recording Everything in a Ledger**

Block 51	Block 52	Block 53	Block 54
Proof of work: 000000857vvv	Proof of work: 00000000xvz5	Proof of work: 00000000xvz5	Proof of work: 00000000xvz5
Previous block: 000000432gza1	Previous block: 000000857vvv	Previous block: 00000000xvz5	Previous block: 00000000xvz5
Transaction 1a5d1xx	Transaction 9d5j11m	Transaction 94cv14	Transaction 550b412
Transaction 0945e1d	Transaction 22pxd87	Transaction a6b73eeq	Transaction bc94ee0201
Transaction v4232v32	Transaction 0019K009	Transaction 34cv088x	Alice → Bob

Minting Money out of Thin Air

Recording Everything in a Ledger

Smart Contract

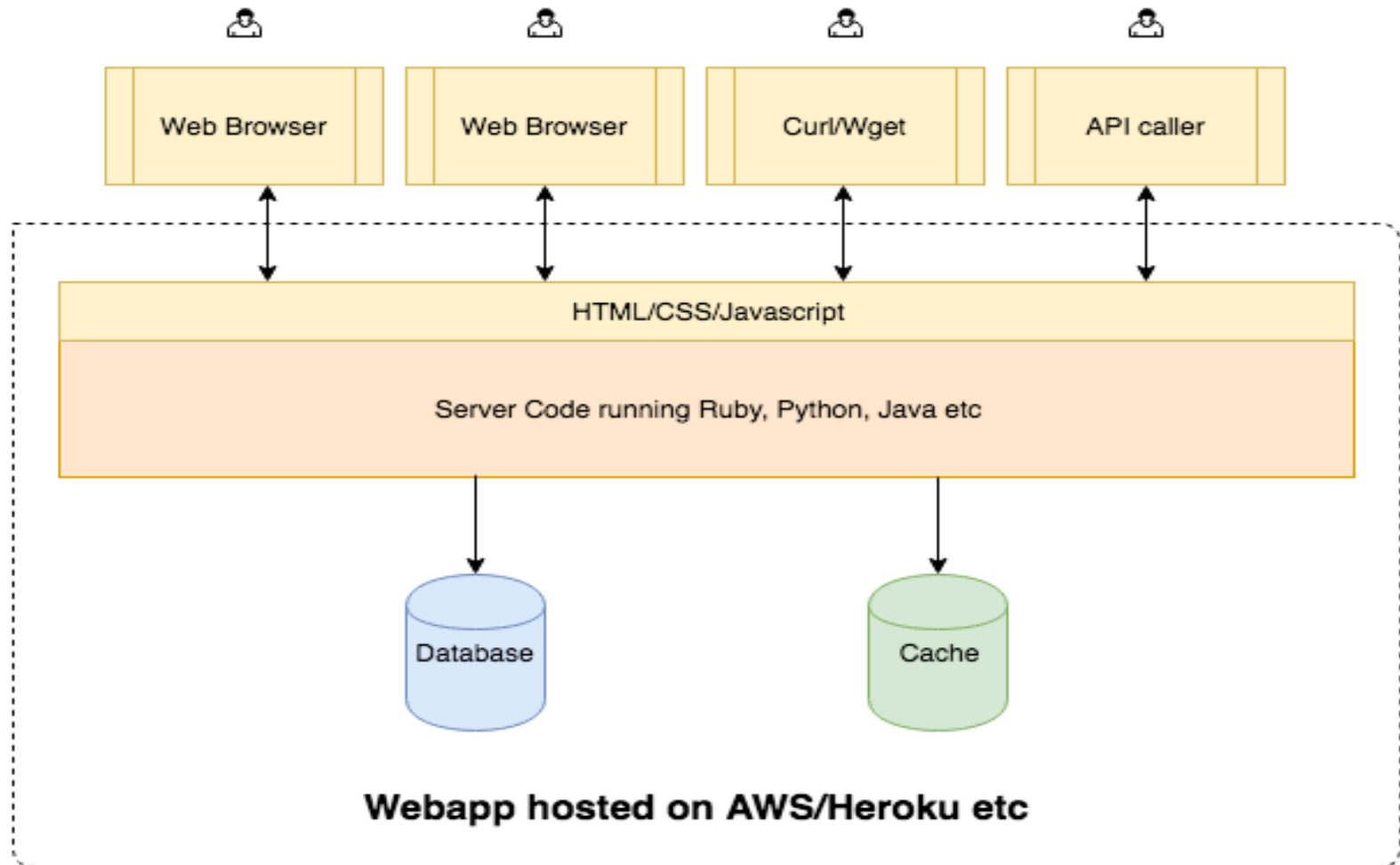
- Smart contract was originally mentioned by Nick Szabo 1994.
- Smart contract defines “promises” that can be executed without the 3rd party arbitrator.
- This enables transactions with strangers via Internet --- transaction settlement based on distributed trust Internet

Smart Contract Recap

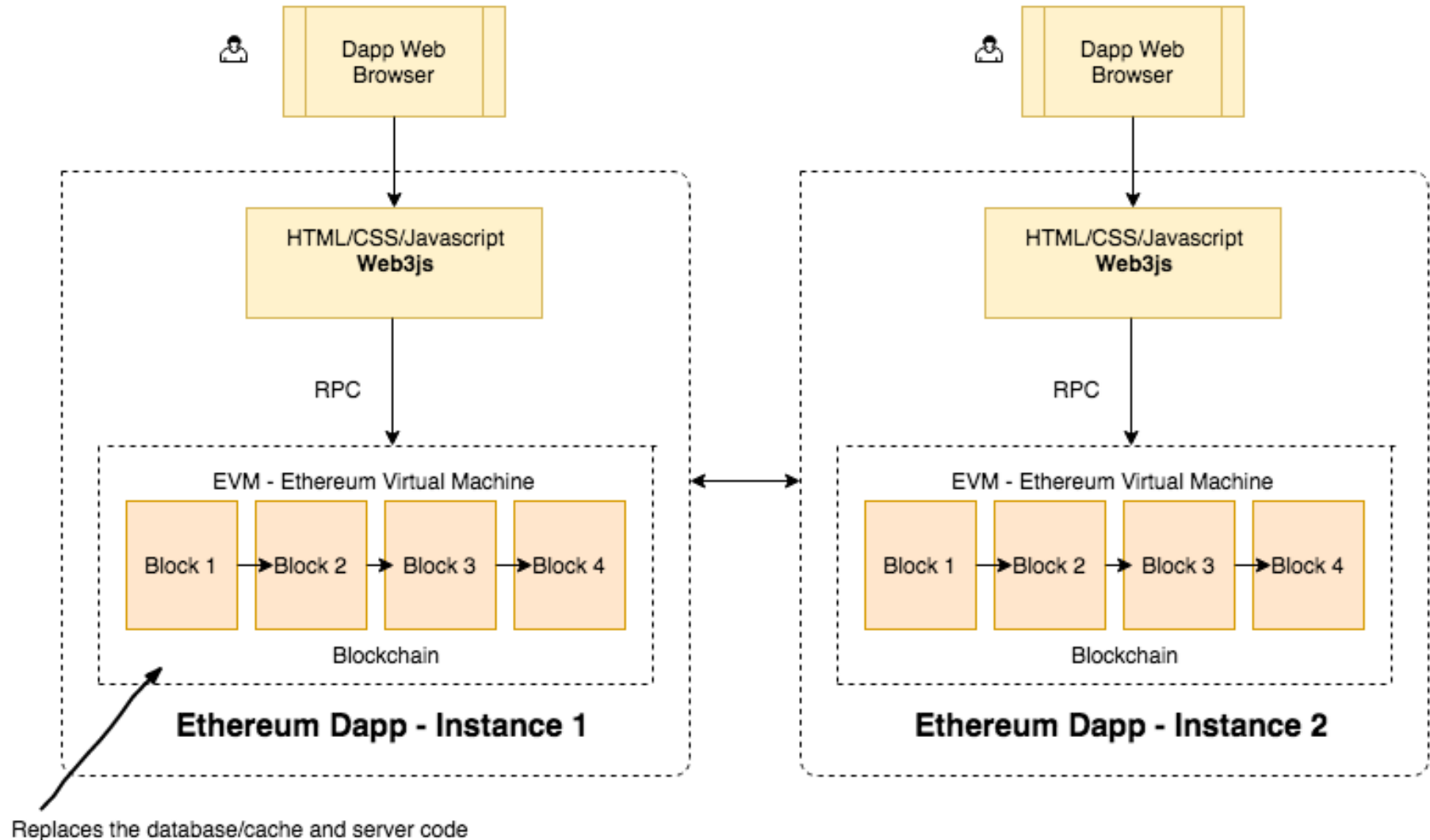
- Smart contract is a state machine
- Smart contracts are pieces of code that live on the blockchain
- Execute commands exactly how they were told to.
- Each smart contract has its own blockchain address after deployed (similar to the user account)
- Either own by the contract creator or nobody by default
- They can read other contracts, make decisions, send ether and execute other contracts.
- Contracts will exist and run as long as the whole network exists,
- Only stop if they run out of gas or if they were programmed to self destruct.

Distributed Application Flow

Centralized Web App Client Server Architecture

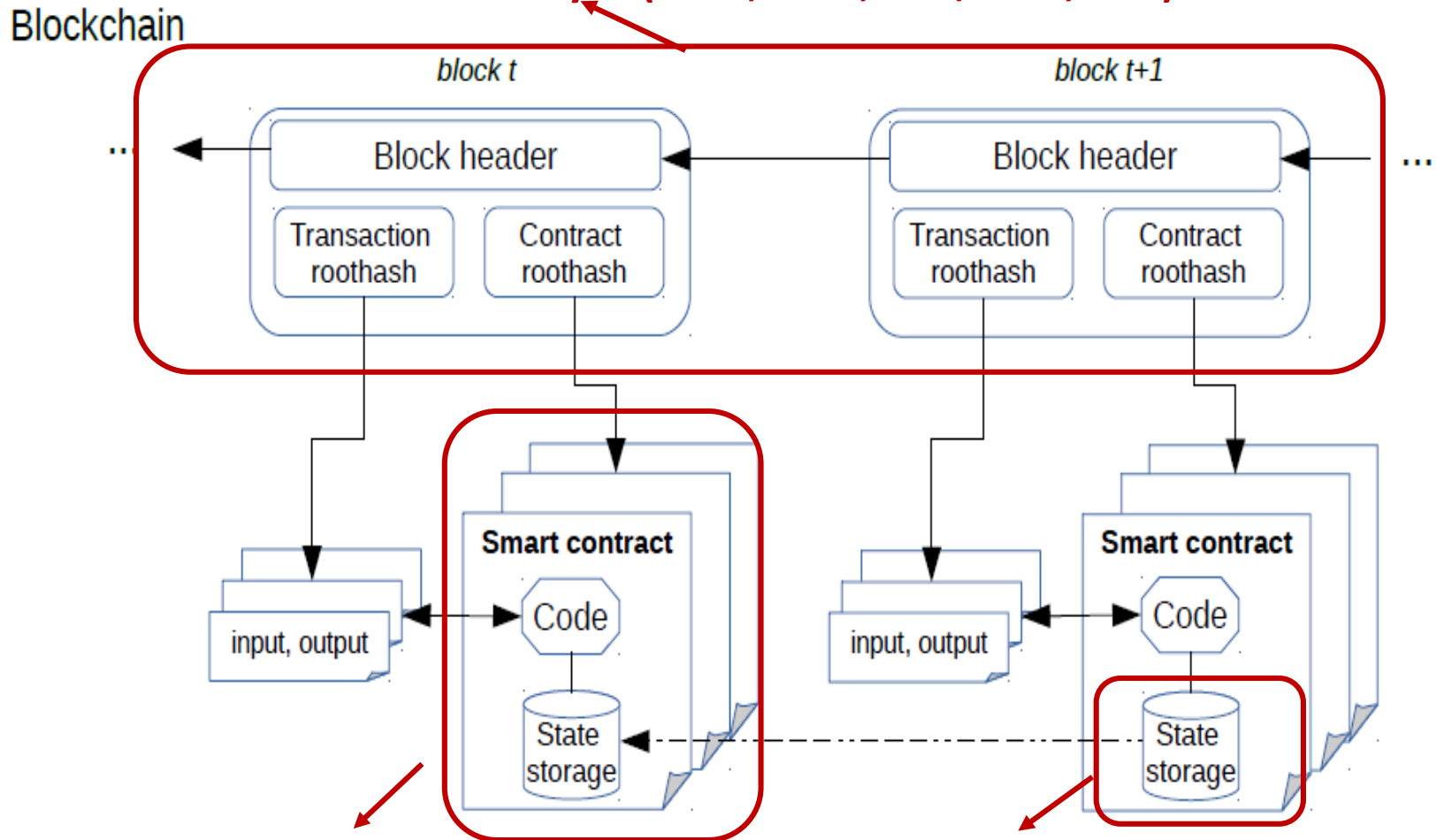


High Level View of Dapp Architecture



Blockchain Software Stack

Consensus Layer (PBFT, PoW, PoS, POA, etc.)

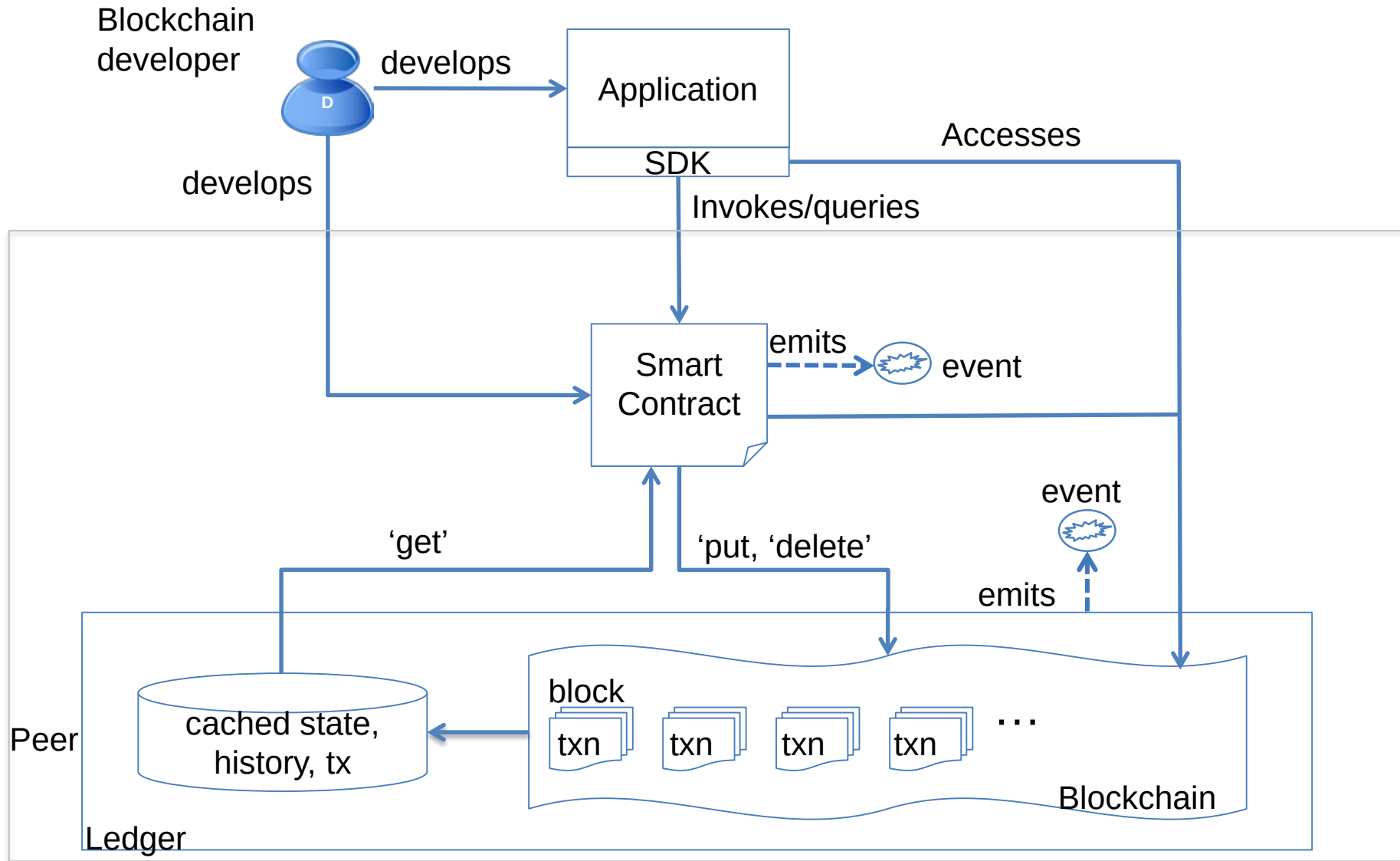


**Smart Contract Execution Engine
(Virtual Machine, Docker, etc.)**

**Data Model Layer
(LevelDB, RocksDB, etc.)**

Source: Anh Dinh, et al., 2017

Overview of Application Flow



Blockchain Companies/Consortia & Banks

	No. of partners
Utility Settlement Coin	5
Global Payments Steering Group	6
Chain	9
Digital Asset Holdings	15
Enterprise Ethereum Alliance	30
R3	81
Ripple	90+
Hyperledger	122

Source: Staff research

Source: American Banker 2-2017

Enterprise Ethereum Alliance

- *Enterprise Ethereum Alliance (EEA)*
 - JPMorgan Chase, Microsoft, Intel, Accenture, Banco Santander, BNY Mellon, ConsenSys, Credit Suisse, ING, Thomson Reuters, UBS, Wipro
 - EEA will add data privacy (Quorum), scalability in performance, and pluggable consensus
 - It is a private network for Enterprise use cases
 - <https://bobsummerwill.files.wordpress.com/2017/02/enterprise-ethereum-technical-roadmap-slides-final.pdf>
- Based on Quorum from JPMorgan
 - Presentation https://github.com/jpmorganchase/quorum-docs/raw/master/Blockchain_QuorumHyperledger_20160922.pdf
 - Whitepaper <https://github.com/jpmorganchase/quorum-docs/raw/master/Quorum%20Whitepaper%20v0.1.pdf>

Linux Foundation Hyperledger Project

- Initiated by IBM
<http://hyperledger-fabric.readthedocs.io/en/latest/>
- Significant change in architecture from V0.6 to V1
- Used PBFT for consensus before V1, use Kafka for consensus ordering in V1
- Customers doing trials: Bank of Tokyo, London Stock Exchange, Maersk, Northern Trust, Walmart

Bigchain DB

- Designed to merge best of DB & blockchain worlds
 - Scale, permissioning and NoSQL querying from DB side
 - Decentralization, immutability, and assets from blockchain side
 - All data as JSON documents in RethinkDB/MongoDB
 - Intended to play well alongside decentralized file systems (e.g., IPFS) and processing (e.g., Ethereum)
 - Modelled around *assets*, *inputs* and *outputs* are the mechanism by which control of an asset is transferred
- Release 1.0 to ship 6/2017

Applications

Screenshot of Silk Road Website (April 2012)

Welcome! | Silk Road | State of the Road Address

silkroadvb5piz3r.onion

Welcome [redacted]
messages(0) | orders(0) | account(\$0.00) | settings | log out

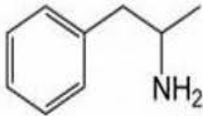
 **Silk Road**
anonymous marketplace

search | (0)

Shop by category:

- Drugs(1582)
 - Cannabis(271)
 - Dissociatives(33)
 - Ecstasy(217)
 - Opioids(106)
 - Other(65)
 - Prescription(274)
 - Psychedelics(306)
 - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)


10 Grams high grade
MDMA 80+%
\$61.17


Amphetamines sulfate /
Speed freebase...
\$28.59


2g Jack Frost (weed) *420
SALE****
\$8.54


Dr Amsterdam


Michael
Jackson

News:

- The gift that keeps on **giving**
- Who's your **favorite?**
- Acknowledging **Heroes**
- A new anonymous market **The Armory!**
- **State of the Road Address**

the eBay for illegal drugs

operated as a Tor hidden service

operated from February 2011 until October 2013

Blockchain Applications

- Food Safety (Wal-Mart, Nestle, Unilever), Logistics
- Trade/Channel Finance – resolve finance dispute (IGF)
- Trade Information Warehouse - post-trade processing (DTCC)
- Private Equity Fund Management (Unigestion)
- Diamond/Valuables Tracking and Protection – Provenance Management (Everledger)
- Insurance + P2P insurance
- Airbnb acquired ChangeCoin, a startup that runs a bitcoin-based micropayments service (2016)
- Toyota pushes into blockchain tech to enable the next generation of cars (May, 2017)
- IBM Watson, FDA to explore blockchain for secure patient data exchange (July, 2017)
- Healthcare and precision medicine
-

Client/Application Examples

CLS



FX Netting



*Diamond
provenance*

Crédit
Mutuel
Arkéa



*Identity
management*

DTCC

Credit Default Swaps

BAML
HSBC



Trade Finance

IBM
Global
Financing



*Channel
Financing*

Japanese
Stock
Exchange



*Low liquidity
securities trading &
settlement*

Walmart



Food Safety



*Health Data
Exchange*

Toyota Next Generation of Blockchain Cars

- Toyota + MIT's Media Lab
- Blockchain technology to create an open platform where users can control their driving data
- Develop safe and reliable autonomous vehicles by monitoring and distributing information about the safety of individual vehicles, the way owners use the cars, and cut down on fraud.
- Initially the research is focusing on sharing data on every trip that an autonomous vehicle takes
- Developing tools to make ride-sharing easier
- Create new insurance products that are usage-based for customers who may prefer that coverage.

Cars Blockchain Ecosystem

- Toyota + MIT's Media Lab + industrial partners
- Berlin-based BigchainDB
 - develop a flexible, scalable blockchain-based ledger
- Oaken Innovations, based in Dallas and Toronto
 - application for P2P car sharing, vehicle access and payments with a newly created mobility token
- Commuterz, a startup from Israel
 - P2P carpooling solution
- Gem, from Los Angeles
 - Toyota Insurance Management Solutions (TIMS)
 - Provides a ledger for distributed inputs from a number of different sources that can then be used to automate much of the insurance claim process.
- Aioi Nissay Dowa Insurance Services
 - usage-based insurance platform

IBM Watson, FDA to Explore Blockchain for Secure Patient Data Exchange

- Announced July, 2017, IBM Watson Health and the FDA will explore the exchange of patient-level data from several sources, including
 - electronic medical records (EMRs)
 - clinical trials
 - genomic data
 - health data from mobile devices, wearables and the "Internet of Things."
- The initial focus will be on oncology-related information.

Blockchain Examples for Medical Domain

- Blockchain is gradually edging into healthcare.
 - HealthNautica + Factom to securely store medical records and provide efficient audit trails.
 - Gem + Capital One to reduce long process time in healthcare insurance claim process.
 - DNA.Bits is planning to store genetic and medical data into blockchain as a personal “DNA wallet”.
 - BlockVerify uses blockchain to fight counterfeit drugs.
- These are all silo vertical applications

Nasdaq (Linq)

- Nasdaq enabled the issuer to digitally represent a record of ownership using Nasdaq Linq blockchain, while significantly reducing settlement time.
- Expediting trade clearing and settlement from the current equity market standards of three days to as little as ten minutes.
- As a result, settlement risk exposure can be reduced by over 99 percent, dramatically lowering capital costs and systemic risk.
- Linq goes live now.

Banks and Financial Services

- R3
 - The 45 banks in the R3 CEV LTD consortium pilot a private blockchain
 - **Corda blockchain**, Plan to go live next year
- Chain Inc.
 - Citi Ventures, Visa Inc. , Capital One, Fiserv and French telecom Orange, and others put \$30 million into Chain Inc.,
 - Building blockchain infrastructure for the financial industry.
- Digital Asset Holdings LLC
 - led by banker Blythe Masters, raised \$50 million from 13 investors including [J.P. Morgan Chase](#) & Co., [Citigroup](#) Inc. and [BNP Paribas](#) SA.
 - Platforms for deals involving stocks, derivatives, loans and other assets
- Hyperledger
 - Lead by IBM to pilot hyperledger with many banks

Diamonds, Art, Airplane Parts

- A definitive registry to trace ownership and certify provenance of big-ticket items would root out illegal goods and decrease fraud worldwide.
- **Everledger** to develop a blockchain to track diamonds from mine to retail sale.
 - Late last year, the Gemological Institute of America said that grading reports for 1,042 registered diamonds were [altered in a cybersecurity breach](#).
- Ownership histories could also help police and insurance investigators track stolen gems.
- Reputable buyers could check the blockchain for information about the diamond on offer.
- Everledger has registered more than 858,000 diamonds with an additional 906,000 in queue.

Music, Movies, News

- Blockchain could shift the dynamics in the media business through smart contracts.
 - a news website would unlock an article when a reader transfers payment.
- Smart contracts could prevent piracy and give artists their due
- Musicians have started to push back against major streaming services over royalties.
- **Ujo, a peer-to-peer music blockchain built on software from open-source consortium Ethereum.**

Food Safety

- Food safety chain
 - In agriculture, farmers could put sensors in fields to monitor crops through growth, harvest and transport, recording data on a blockchain via wireless network.
 - In a recall, farmers could quickly match tainted product to supply chain records. They could more accurately trace where their food went and assess the size and expense of the recall.
- Filament, offers wireless Internet of Things technology, is exploring such ideas with agriculture companies.
- Coca-Cola Co. is in discussions with Filament, which could lead to the use of blockchain and IoT to monitor vending machines,

Insurance Opportunity

- Startup Tierion Inc. recently built a blockchain to [process insurance claims](#), working with business and technology experts from Citigroup Inc.
- Blockchain can provide an efficient, and trusted at each hand-off in claims processing.
- Companies could offer “instant” policies good for a few hours.
 - A whitewater rafter, for example, could request extra accident coverage during his Sunday afternoon venture.
- Blockchain can also ease peer-to-peer insurance, circumventing established companies.
 - For example, Uber or Lyft drivers, who currently rely mainly on their personal auto policies, could pool their money on a blockchain and create a smart contract to insure each other.

Challenges

Challenges

- Scalability
- Privacy/Identity
- Transparency/confidentiality
- Last mile issues

Scalability Challenges

- All blockchain nodes are processing the same block at the same time.
- Increase the number of the nodes would not scale the performance (the performance is worse if the number of nodes increase)
- Performance
 - Bitcoin: 7 transactions per second (TPS)
 - Visa network: on average 1000-2000 TPS, peak at 10000 TPS
 - Taobao (淘寶) peak at 86,000 TPS
 - IoT (Huge) TPS
- Blockchain size
 - bitcoin blockchain size is now about 65 GB (for 7 transaction per second)
 - To support Visa 100000 TPS, the blockchain size will reach Terabyte quickly

Privacy/Identity

- Pseudonymous Identification
- Anonymity is favorable for SaaS applications, because data providers may not want to expose their identity.
- Some applications, especially banking applications, user identity is absolutely needed.

Transparency/Confidentiality

- The transparency of a distributed ledger of is the core feature to make blockchain trustable
- But the bank A in the blockchain will require confidentiality and will not want its business transactions be snooped by other banks (in the same chain).

IoT Blockchain Challenges

- Sensors and its owners have to be uniquely identified and authenticated
- The values delivered by the sensors should be traceable and have to be secured against manipulation
- A low cost micropayment system has to enable the seller side to receive monetary gratification from the buyer side.

Summary

- Blockchain: a disruptive innovation in computer science
- Next generation of Internet (creates excitement similar to the onset of the first generation of Internet at 1993)
- New innovative business models and large number of (big and small) startups emerging
 - Huge investment (too big to fail or become hype?)
- A lot of technology challenges, and huge return.

Q&A