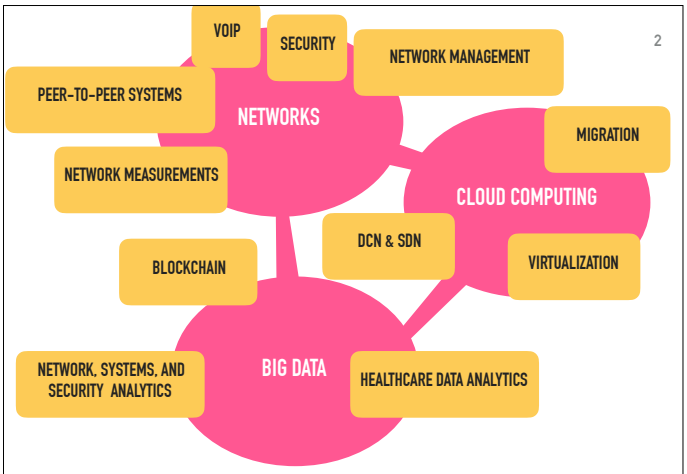
BLOCKCHAIN FOR FUN AND PROFIT?

Kunwadee Sripanidkulchai, Ph.D.

Computer Engineering, Chulalongkorn University



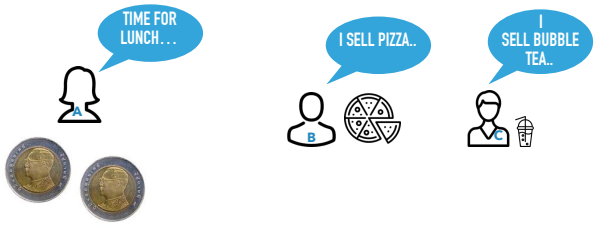
WHAT IS BLOCKCHAIN?

WHAT IS BITCOIN?

OUTLINE

- BitCoin
- Blockchain
- Smart Contracts
- Applications
- Research

PHYSICAL CURRENCY IS ANONYMOUS AND SECURE



Physical currency is

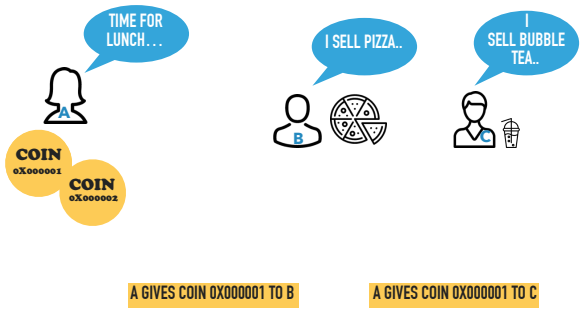
- anonymous (cannot identify parties involved) and
- secure (difficult to fake).

DIGITAL CURRENCY

A GIVES COIN 0X000001 TO B

A GIVES COIN 0X000002 TO C

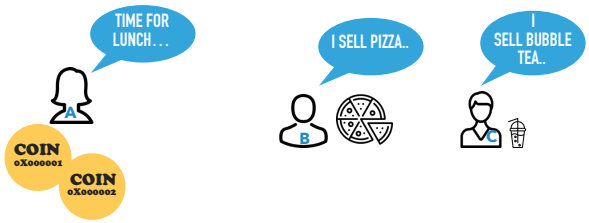
THE DOUBLE-SPENDING PROBLEM



A GIVES COIN 0X000001 TO B

A GIVES COIN 0X000001 TO C

THE DOUBLE-SPENDING PROBLEM SOLVED USING TRUSTED 3RD-PARTY



Ledger Managed by Trusted 3rd Party

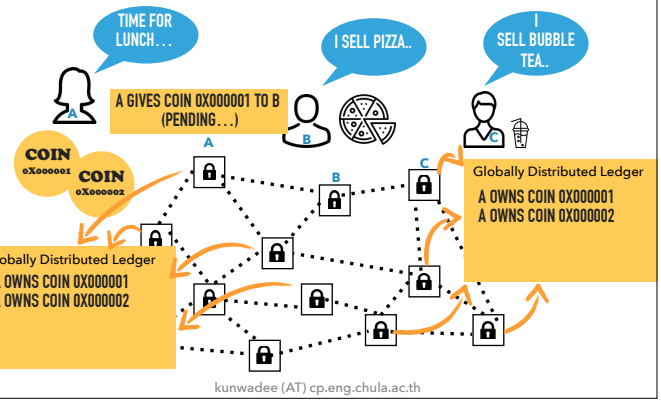
A GIVES COIN 0X000001 TO B APPROVED!

~~A GIVES COIN 0X000001 TO C~~ DENIED!

This is centralized!! This is traceable!! :(And this is difficult to scale!!

WE WANT DIGITAL CURRENCY TO BE ANONYMOUS AND SECURE JUST LIKE PHYSICAL CASH

BITCOIN [SATOSHI NAKAMOTO 2008]



GLOBAL DISTRIBUTED DECENTRALIZED LEDGER

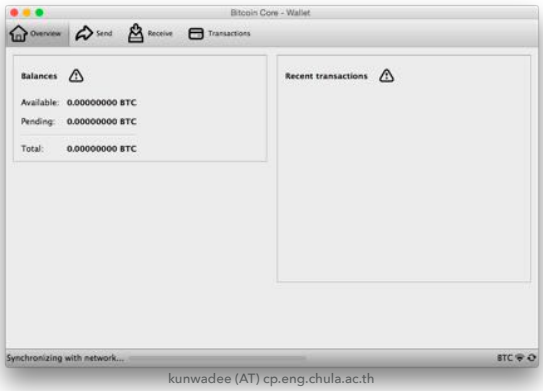
Globally Distributed Ledger
A OWNS COIN 0X000001
A OWNS COIN 0X000002
A GIVES COIN 0X000001 TO B
~~A GIVES COIN 0X000001 TO C~~
…

- Secure
  - All peers see all transactions
  - Ledger is append-only, so everyone can validate that there is no double-spending
  - Immutable: cannot go back and change past entries in the ledger
- Anonymous
  - Bitcoins are sent to 'addresses' such as 0x00000A and 0x00000B so you cannot tell who is who
  - Use new keys to avoid establishing "patterns of use"

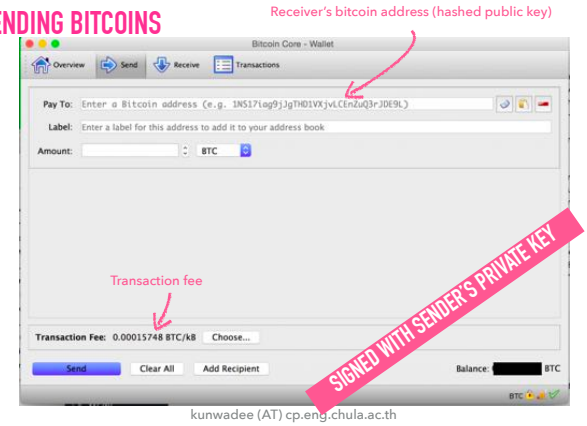
JOINING THE BITCOIN SYSTEM

- Download a "wallet" software
- Wallet software will generate your identifiers (private and public key pairs)
  - Private key is used to sign your transactions
  - 160-bit hash of your public key is used as your bitcoin address
- Wallet will join and run the Bitcoin protocol on your behalf using your keys
- You can send and receive coins using your bitcoin address

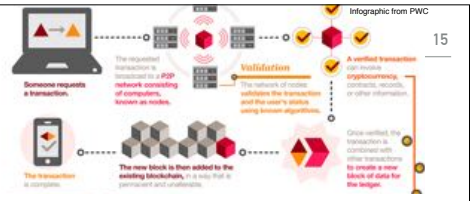
BITCOIN CORE WALLET



SENDING BITCOINS



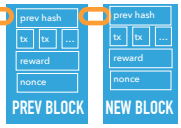
BITCOIN MINING



- Transactions (~500) are grouped together into a "block" that needs to be "mined" or "created" before appended to the global ledger.
- Peers in the network verify transactions in the block and compete to mine the new block. Every 10 minutes there is one winner and a new block gets created. The winner gets a reward worth 12.5 BTC (was 50 BTC in 2009) and the transaction fees.
- Currently (8/2017) 16 million coins mined from the maximum possible 21 million coins.

HOW ARE NEW BLOCKS CREATED (MINED)

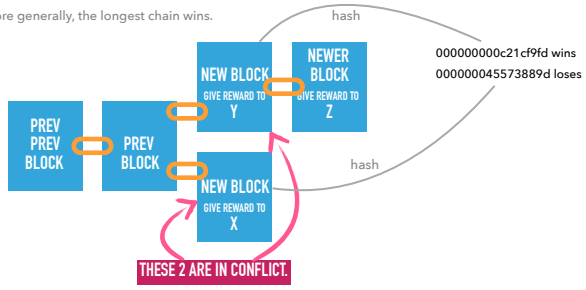
- Peers gather a set of pending transactions to put into this new block (< 1 MB size)
- Verify transactions
- Solve a hashing problem "proof of work" based on
  1. Hash of previous block
  2. Transactions in this new block
  3. Creation of the rewards (12.5 BTC)
  4. Nonce



- The miner has to hash 1-4 and keep changing the nonce until it finds a nonce that produces a hash with enough zero's
  - **0000000000000000000**45573ef92236dbf4ec21cf9fdd42271f12be9e78272c1b
- Transactions are confirmed after 6 blocks have been appended
- Bitcoins are confirmed after 100 blocks have been appended

BREAKING TIES

- Two miners may happen to publish new blocks at the same time. This is called a fork.
- To break ties, the branch with more 0's in the hash wins.
- More generally, the longest chain wins.



WORTH IT?

Select miner	Antminer R4	AntMiner S9	Avalon 7
Released	August 2016	June 2016	November 2016
Power consumption	845Ws±9%	1375W ±7%	850W-1000W
Power efficiency	0.1 J/GH +9%	0.098 J/GH	0.29 J/GH
Hash rate	8.6TH/s±5%	12.93 TH/s	6 TH/s
Dimensions	20 x 3.9 x 8.7 inches	13.7 x 5.3 x 6.2 inches	13.4 x 5.3x 5.9
Weight	unknown	10 lbs	9.5 lbs
Revenue in vacuum*	0.29 BTC/month	0.5 BTC/month	0.14 BTC/month
Price	Estiamted $1000	~$2000	$880
Overall rating	88%	95%	81%
	Read review	Read review	Read review

https://99bitcoins.com/best-bitcoin-miners-2016-hardware-reviews/

THIS IS FOR REAL…

The BM1387 ASIC Chip

The world's first bitcoin mining ASIC based on the 16nm process node

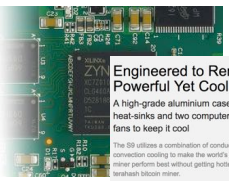
Bitmain's BM1387 chip is built using TSMC's 16nm FinFET technology and, delivering a record-breaking 0.098 J/GH/s, is the world's most efficient bitcoin mining chip in the consumer market.

Each Antminer S9 employs 189 such chips to deliver more hashrate and efficiency than any bitcoin miner ever made.

Controlled by a Dual ARM® Cortex®-A9 Microprocessor

S9's control board uses a Xilinx® Zynq®-7000 series FPGA with a Dual ARM® Cortex®-A9 microprocessor

Bitmain's engineering team understood the importance of every detail while working to make the world's most power-efficient yet powerful Bitcoin miner. The Antminer S9's control board employs the fast Dual ARM® Cortex®-A9 microprocessor with CoreSight™ and supports Gigabit Ethernet to ensure that mined blocks are submitted instantly.



Engineered to Remain Powerful Yet Cool

A high-grade aluminium case, customized heat-sinks and two computer-controlled fans to keep it cool

The S9 utilizes a combination of conduction and convection cooling to make the world's most powerful miner perform best without getting hotter than any other terahash bitcoin miner.

Every chip of the S9 is fitted with custom-made heat sinks that are made of a high-grade Aluminium alloy. The case of the S9 is made of the same material. Two computer-controlled high speed fans on both ends of the "tube" ensure that the hot air is rapidly replaced by cooler air at the required pace.

A Compact Time-tested Design

World's most powerful bitcoin miner, yet smaller than many portable boom-boxes

The Antminer S9 follows the same form factor as that of the hugely popular Antminer S7 and is nearly the same size. Yet it has more than thrice the power and twice the efficiency of the S7.

Each Antminer S9 employs 189 such chips to deliver more hashrate and efficiency than any bitcoin miner ever made.

http://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm

WHO IS IN THE BITCOIN P2P NETWORK?

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Aug 10 2017 23:56:20 GMT+0700 (+07).

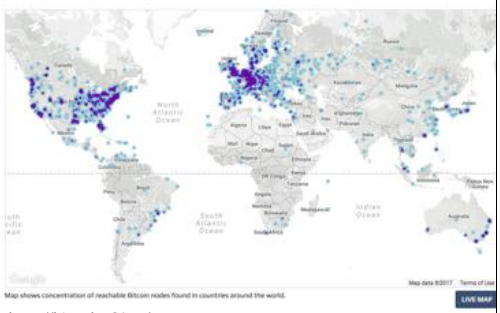
8838 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2461 (27.85%)
2	Germany	1598 (18.08%)
3	France	506 (5.86%)
4	Netherlands	438 (4.95%)
5	China	382 (4.32%)
6	Canada	337 (3.81%)
7	n/a	329 (3.72%)
8	Russian Federation	325 (3.68%)
9	United Kingdom	311 (3.52%)
10	Singapore	168 (1.90%)

More (95) »



https://bitnodes.21.co/

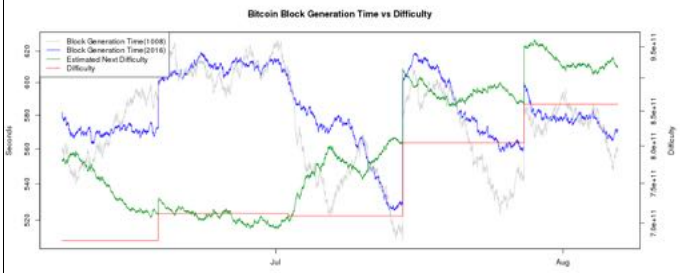
HTTP://BLOCKCHAIN.INFO/UNCONFIRMED-TRANSACTIONS

1731 Unconfirmed Transactions Live updating list of new bitcoin transactions

17062 Unconfirmed Transactions Live updating list of new bitcoin transactions

- A transaction is verified by the miner who **A GIVES COIN 0X000001 TO B**
  - checks that A really made the transaction (check A's signature)
  - checks the public ledger to verify that A hasn't already sent these Bitcoins to someone else (prevent double-spending)

ADJUST THE DIFFICULTY TO MAINTAIN BLOCK GENERATION TIME



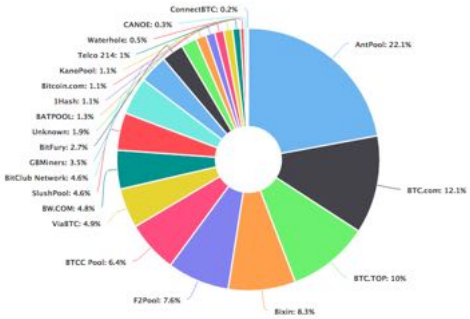
https://bitcoinwisdom.com/bitcoin/difficulty

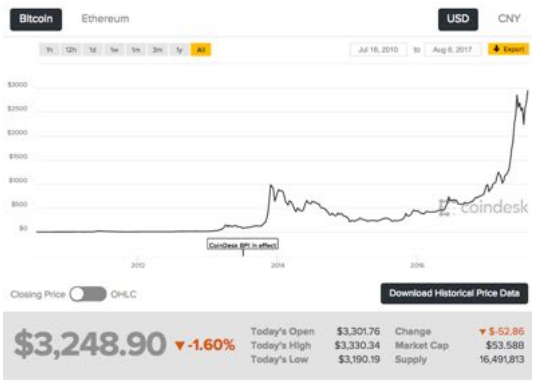
ADJUST THE REWARD OVER TIME

http://www.bitcoinblockhalf.com/

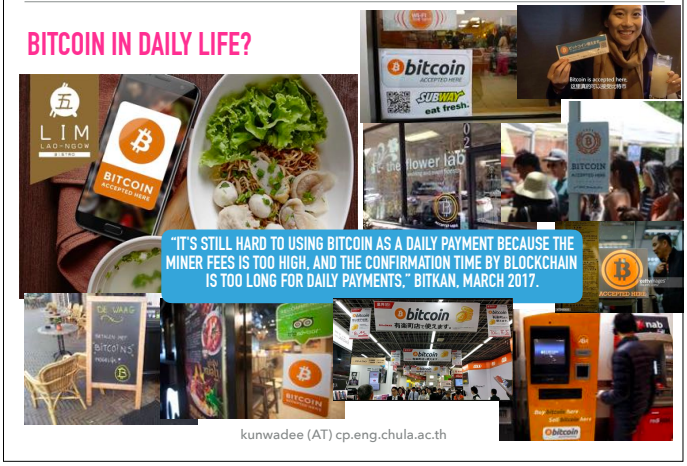
NEED DIVERSE POOL TO PREVENT AGAINST COLLUSION / CONTROLLING THE NETWORK

51% attack: do not want anyone to have > 50%





BITCOIN IN DAILY LIFE?



BITCOIN VS. BLOCKCHAIN

- Bitcoin is a digital currency based on Blockchain technology
- Blockchain is the peer-to-peer network that provides an open, public, anonymous and immutable distributed ledger
  - Mining to create blocks
  - Can be used for any "transaction", not just digital currency
  - Supports smart contracts

APPLICATIONS BEYOND DIGITAL CURRENCY

Infographic from PWC

SLASHDOT POLL

Your favorite alternative Blockchain use?

Displaying poll results.

Proof of identity
503 votes / 6%

Notary service
453 votes / 5%

Non-repudiable proof of voting
910 votes / 11%

DNS replacement
674 votes / 8%

Micro-lending
195 votes / 2%

Something not on this list
475 votes / 6%

How can a chain be made of blocks?
4523 votes / 58%

7733 total votes.

SMART CONTRACTS

Agreements between parties that are published to blockchain and are automatically executed when conditions are met. Written in a programming language. Can be very complex.

```
// pay rent for apartment every month
// up to LAST RENTAL DATE
if ((last day of the month) &&
(date < LAST_RENTAL_DATE)) then
   (pay 1 BTC) to (apartment manager)
```

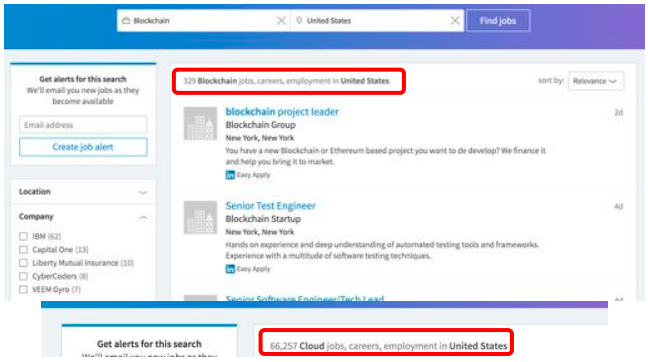
```
// buy 10 coffees, get 11th cup free
purchase ++;
if (purchase <= 10) then
   (pay 0.1 BTC) to (starbux)
else
   purchase = 0;
```

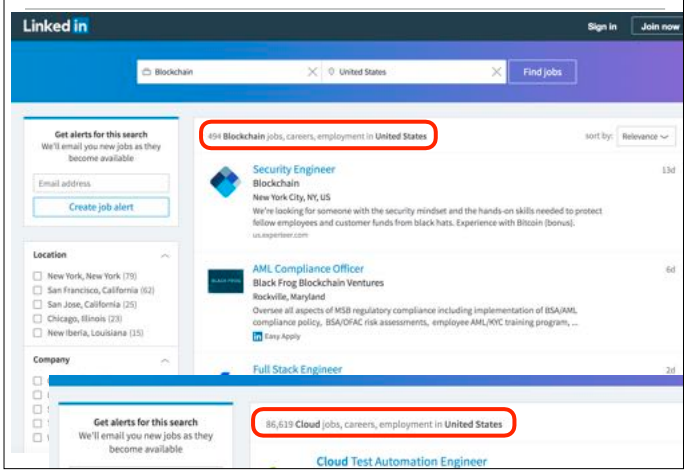

KEY PLAYERS

- Traditional players
  - Blockchain as a Service
  - IBM Hyperledger
  - Microsoft Azure BaaS
  - Banks and Financial Services
- Start ups
  - Lots in the FinTech space
- Open-Source Software/Platforms
  - Ethereum
  - Hyperledger
  - Eris
  - Ripple
  - Multichain

	Blockchains with no smart contracts	Blockchains with smart contracts	Blockchains with Turing-complete smart contracts
What?	Distributed storage	Distributed compute: an compute some pre-templated logic	Distributed compute: can compute any logic
Examples	Bitcoin (public) Litecoin (public) Multichain (private)	NXT (public)	Ethereum (public) Eris (private) Clearmatics (private)

Table from http://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/

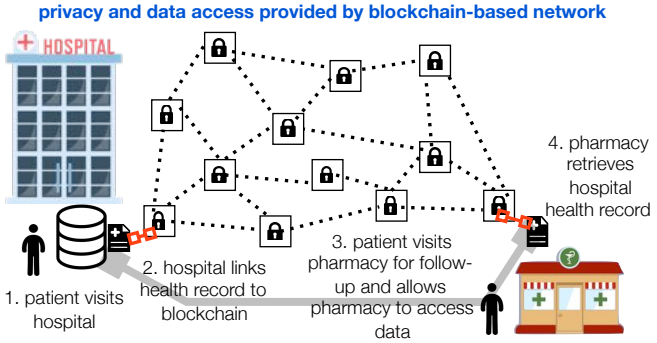




การแลกเปลี่ยนข้อมูลคนไข้ระหว่างร้านยาและโรงพยาบาลเพื่อการดูแลอย่างต่อเนื่อง (Secure Health Record Exchange between Pharmacies and Hospitals for Continuity of Care)

ผศ.ภก.ดร.อนุชัย ธีระเรืองไชยศรี อ.ดร.กุลวดี ศรีพานิชกุลชัย และคณะ

privacy and data access provided by blockchain-based network



RESEARCH ISSUES

- Scaling without compromising security

The War Between Segwit vs. BIP148 vs. Bitcoin Unlimited, Explained

By Investopedia | June 14, 2017 — 12:23 PM EDT

RESEARCH ISSUES

- Smart contract security