

Blockchain Networks and People

PHIL TECH58100–PHIL 58000A

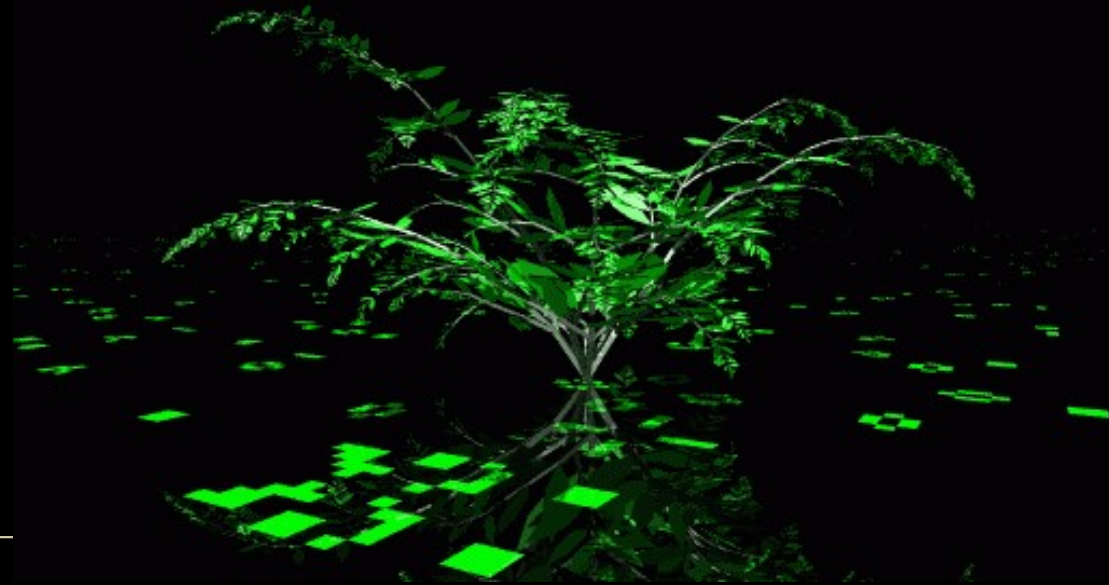
Blockchain Network Theory

Purdue University, Aug 30, 2018

Slides: <http://slideshare.net/LaBlogga>

Agenda

- Introduction to...
 - Blockchain
 - Theorizing
 - Networks



What is blockchain? Conceptual overview

1. Digital money (better version of PayPal/Venmo)
2. Enterprise software (digital asset inventories)
3. Inclusion technology (unbanked, credit, literacy)
4. Emerging legal jurisdiction (game theory not police)
5. Web 3.0: larger-scale collaboration technology
 - (Web 3.0 = smart network, “Internet's new pipes”)
6. Truth verification method (rich information attributes)



basics.

information.

email.

voice.

video.

money.

internet content.

What is Blockchain/Distributed Ledger Tech?

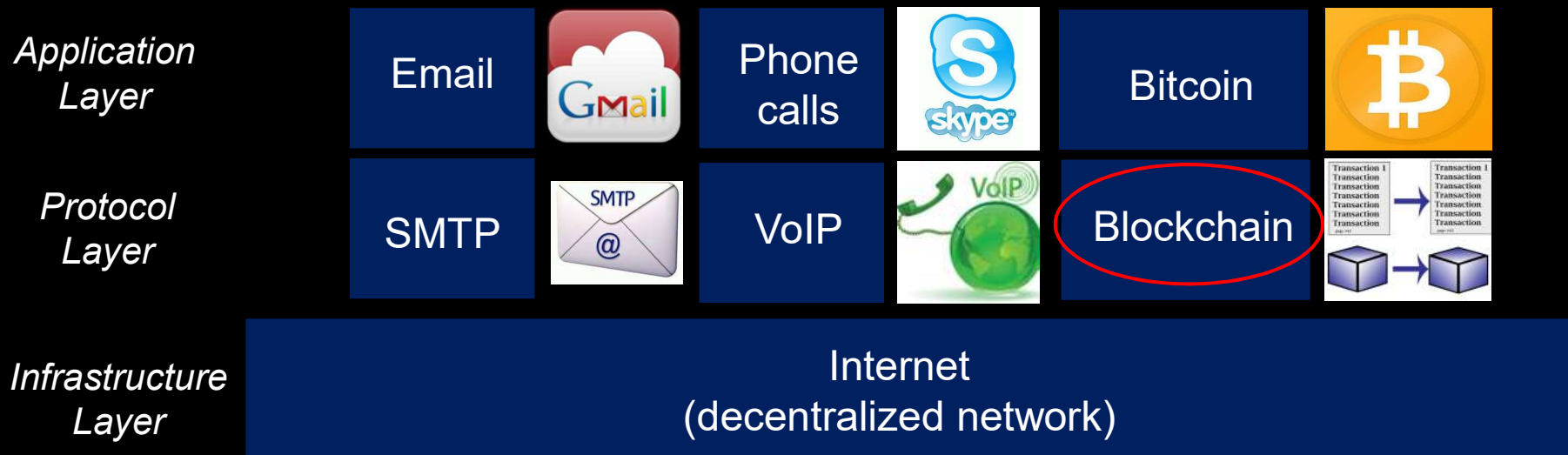
Conceptual Definition:

*Blockchain is a software protocol;
just as SMTP is a protocol for
sending email, blockchain is a
protocol for sending money*

Blockchain Technology: What is it?

- Blockchain technology is the secure distributed ledger **software** that underlies cryptocurrencies like Bitcoin
 - “Internet of Money” leapfrog technology; Skype is an app allowing phone calls via Internet without POTS; Bitcoin is an app allowing money transfer via Internet without banks; ‘decentralized Paypal’

OSI Protocol Stack:



software.
secure cryptographic transfer.
internet.

blockchain.

secure transfer of value, of...

52315231

23 3 35 212

23 12 35

23 5 12 2

52315231





money & securities.

property.

contracts.

identity credentials.

killer apps.

 <p>Finance Trade and settle securities at a fraction of the time and cost.</p>	 <p>Property Permanently record and access real-time property rights.</p>
 <p>Contracts Self-enforcing contracts based on predefined conditions.</p>	 <p>Identity Eliminate invasive identity practices via digital identities.</p>

public chains.

*trustless. mined.
p2p software.*



private chains.

*trusted. not-mined.
enterprise software.*



How does Bitcoin work?

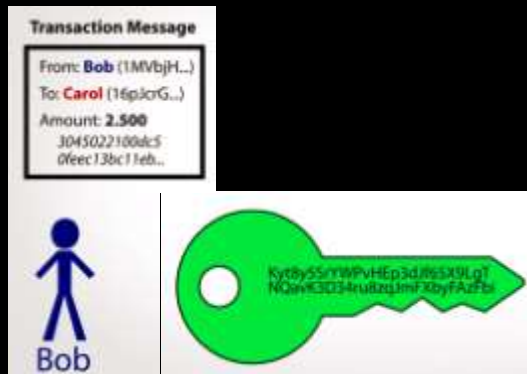
Use eWallet app to submit transaction



Scan recipient's address and submit transaction



\$ appears in recipient's eWallet

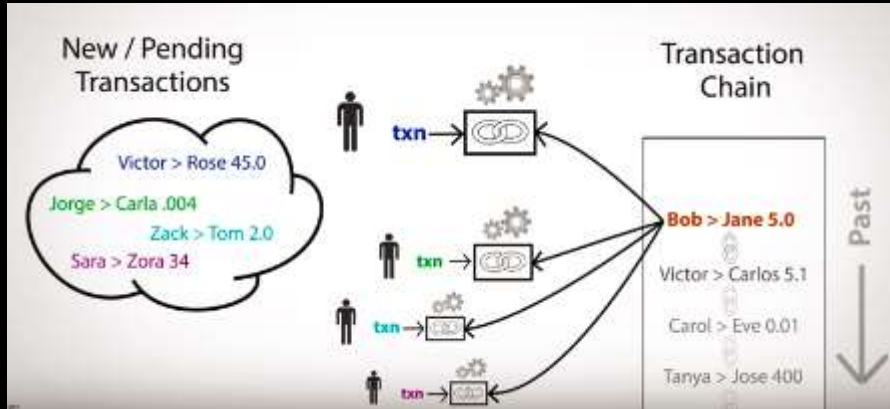


Wallet has keys not money
Creates PKI Signature address pairs



A new PKI signature for each transaction

P2P network confirms & records transaction



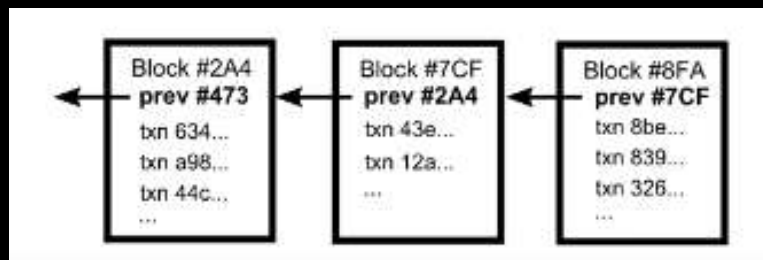
Transactions submitted to a pool and miners assemble new batch (block) of transactions each 10 min

Ledger

account number	balance
1G8bnej6etY...	12.5
1K7A6wsyxj6...	323
Carol 16pJcrGl51nr...	6.0 +5.0
Bob 1MVbjHicuJr...	10.2 -5.0
1G4HyHp1oa...	100
17UP3moev2...	.00000001
1Eeq4FM2Ts...	45

Bob and Carol are shown with their respective ledger updates.

Transaction computationally confirmed Ledger account balances updated



Each block includes a cryptographic hash of the last block, chaining the blocks, hence "Blockchain"



Peer nodes maintain distributed ledger



mining and consensus algorithms.

Run the software yourself:



bitcoin / bitcoin

What is Bitcoin mining?

- Mining is the accounting function to record transactions, fee-based (\$103,000/block)
- Mining clients (ASICs) “find new blocks”
 - Mining software constantly makes nonce guesses per specified cryptographic parameters
 - At the rate of 2^{32} (4 billion) hashes (guesses)/second
 - One machine at random guesses a solution
- Winning machine confirms and records the transactions, and collects the rewards
 - All nodes confirm the transactions and append the new block to their copy of the distributed ledger
- “Wasteful” effort deters malicious players



Fast because ASICs represent the hashing algorithm as hardware

```
Sample code: while (hash_256(hash_256(block_header, nonce) >= target_string) do  
              nonce = nonce + 1  
            end while
```



52315231

23 3 35 212

23 12 35

23 5 12 2

52315231

bitcoin mining.

Proof of Work: secure but expensive.

How will we work in the class...

Course structure, matrix, ...

Seminar style: Use matrix to structure discussion

Practical Problem	XXX	XXX
Theoretical motivation	XXX	XXX
Research Question	XXX	XXX
Theory Logic	XXX	XXX
Causal Model	XXX	XXX
Research Design	XXX	XXX
Findings	XXX	XXX
Plausible Alternative Interpretations	XXX	XXX
Theoretical Contribution	XXX	XXX
Research Design Learning	XXX	XXX
Theoretical Learning	XXX	XXX
Key References	XXX	XXX
Generative Hypotheses	XXX	XXX

Who wants to lead the first discussion?

Semester Week	Date	Agenda	LEADER?
2	Th 8/30	Introduction	
4	Th 9/13	Research matrix discussion	
6	Th 9/27	Research matrix discussion	
8	Th 10/11	Research matrix discussion	
10	Th 10/25	Action-oriented research experience	
12	Th 11/8	Research matrix discussion	
14	Th 11/22	No Class: Thanksgiving Break	
16	Th 12/6	Research Presentations (no finals)	

Contacts and Office Hours

Instructor TECH: Professor Sabine Brunswicker

Email: sbrunswi@purdue.edu

Office: Wang Hall, 316 Northwestern Ave, 47906 West-Lafayette

Office Hours: Monday 1:30 – 3:00 pm

Instructor PHIL: Melanie Swan

Email: swan3@purdue.edu

Office: Beering Hall, Room 7154

Office Hours: Monday 1:00 – 2:30 pm

Schedule: Class meets second Thursdays 4:30 to 6:20 pm

KNOY BO31

Credits: 1, Website: www.purdue.edu/opendigital/courses

There is no final exam; just a final presentation

	Deliverable	Percentage
1	Matrix Deliverable (template and examples provided)	40%
	One matrix for each session, due anytime, graded Pass/Fail	
2	Research Project Proposal Presentation (examples provided)	40%
3	Class attendance and participation	20%

No Final Exam: final presentation only

And here is the schedule and content

	Date	Readings	Topics
1	Th 8/30	Welcome, Introductions, Blockchain and Network Science Course Overview	
2	Th 9/13	<ul style="list-style-type: none"> Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Brandes, U., Robins, G., McCranie, A., and Wasserman, S. (2013). What is network science? <i>Network Science</i>. (1):1–15. 	Blockchain Overview
			Network Science Overview
3	Th 9/27	<ul style="list-style-type: none"> Morabito, V. (2017). <i>Business Innovation Through Blockchain: The B3 Perspective</i>. Springer. Ch 1: The Blockchain Paradigm: 3-20. Jackson, M.O. (2008). <i>Social and Economic Networks</i>. Princeton University Press. Ch 1: Introduction to Social and Economic Networks: 17-38. 	Blockchain Business Applications
			Social and Economic Networks
4	Th 10/11	<ul style="list-style-type: none"> Allen, D.W.E., Berg, C., Davidson, S., Novak, M., Potts, J. (2018). <i>Blockchain TradeTech</i>. APEC Study Centres Consortium, May 2018, Papua New Guinea. Sohn, I. (2017). Small-World and Scale-Free Network Models for IoT Systems. <i>Mobile Information Systems</i>. Pp. 1-9. 	Blockchain Supply Chain
			Small-world and Scale-free Properties
5	Th 10/25	<ul style="list-style-type: none"> Moreno-Sanchez, P., Modi, N., Songhela, R., Kate, A., & Fahmy, S. (2018). Mind Your Credit: Assessing the Health of the Ripple Credit Network. Sherchan, W., Nepal, S., and Paris, C. (2013). A Survey of Trust in Social Networks. <i>ACM Computing Surveys (CSUR)</i>. 45(4): 1-47. 	Blockchain credit network: Ripple
			Social Network Trust Theories
6	Th 11/8	<ul style="list-style-type: none"> Miller, A., Möser, M., Lee, K., & Narayanan, A. (2017). An Empirical Analysis of Linkability in the Monero Blockchain. Orlikowski, W.J. and Scott, S.V. (2015). The algorithm and the crowd: considering the materiality of service innovation. <i>MISQ</i>. 39(1): 201-216. 	Blockchain: Monero
			Network Theory Development
7	Th 11/22	No Class: Thanksgiving Break	
8	Th 12/6	Research Presentations	