FINE 434: FinTech

Lecture 12

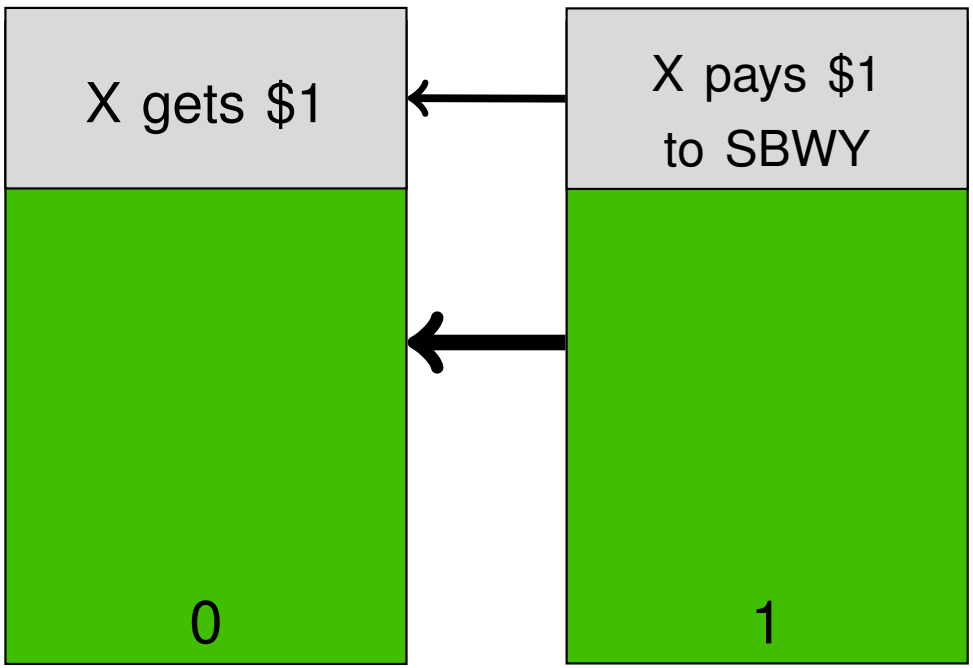
Professor Fahad Saleh

McGill University - Desautels

Blockchain: A Distributed Ledger System

- Electronic Ledger
  - Entries are recorded in discrete chunks called blocks
  - Blocks are chained together in a near-chronological order
- Distributed System
  - Network of agents
  - Each agent holds a copy of the ledger

Electronic Ledger



Typology

- Private (Permissioned) Blockchain
  Selective and Verifiable Information Sharing
- (Public) Permissioned Blockchain
- **Public Permissionless Blockchain**
  “Trustless” and “Immutable”

Permissionless Blockchains

- Payment System (e.g. Bitcoin)
- Smart Contracts Platform (e.g. Ethereum)

Significant distinction from an economic perspective

(see Hinzen, John and Saleh, and Cong, Li and Wang)

Permissionless Blockchains

- Payment System (e.g. Bitcoin)
- Smart Contracts Platform (e.g. Ethereum)

Significant distinction from an economic perspective

(see Hinzen, John and Saleh, and Cong, Li and Wang)

We focus on Permissionless Payment Systems initially for exposition...

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1909 levels

Business, page 47

H2 2008

Bitcoin is Born!

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

A New Paradigm?

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model."

A New Paradigm?

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model."

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. "

Conceit

“In this paper, we propose... a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”

Conceit

"In this paper, we propose... a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."

Note: Nakamoto proposed a public permissionless payment system blockchain but neither invented the blockchain data structure nor even used the term "blockchain"

Desired Properties (Bonneau et. al. 2015)

- **Correctness**
  "All blocks in the longest chain will only include valid transactions."
- **Liveness**
  "New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"
- **Eventual Consensus**
  "At any time, all compliant nodes will agree upon a prefix of what will become the eventual valid blockchain."

Desired Properties (Bonneau et. al. 2015)

- **Correctness**
  "All blocks in the longest chain will only include valid transactions."
- **Liveness**
  "New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"
- **Eventual Consensus**
  "At any time, all compliant nodes will agree upon a prefix of what will become the eventual valid blockchain."

What about economic usefulness??

Correctness

"Digital signatures provide part of the solution"
- Nakamoto (2008)

Bitcoin, for example, uses the Elliptic Curve Digital Signature Algorithm (ECDSA). This use of cryptography makes fraud transparent up to a difficult math problem (akin to RSA with prime factoring large numbers).

Practically speaking, correctness is not a concern.

Liveness

"New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"

i.e., We need somebody to update the ledger!

Liveness

"New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"

i.e., We need somebody to update the ledger!

... how do we induce agents/ nodes to update the ledger?

Liveness

"New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"

i.e., We need somebody to update the ledger!

... how do we induce agents/ nodes to update the ledger?

monetary compensation?? (... we will come back to this)

Eventual Consensus

"At any time, all compliant nodes will agree upon a prefix of what will become the eventual valid blockchain."

i.e., The network must agree on the ledger

Eventual Consensus

"At any time, all compliant nodes will agree upon a prefix of what will become the eventual valid blockchain."

i.e., The network must agree on the ledger

How do we ensure this outcome??

Eventual Consensus

"At any time, all compliant nodes will agree upon a prefix of what will become the eventual valid blockchain."

i.e., The network must agree on the ledger

How do we ensure this outcome??

Attempt #1: Proof-of-Work