School of
Law

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Blockchains, Bitcoins and Smart Contracts

#VictoriaUniversity

Eliza Mik

School of
Law

SMU
SINGAPORE MANAGEMENT UNIVERSITY

I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
S. Adams E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.

Some very important distinctions!

Bitcoin # Blockchain

Blockchain? Blockchains!

Blockchains # Crypto-ledgers / “DLTs”

a very basic definition

Blockchain:

a decentralized, peer-validated crypto-ledger that provides a publicly visible, chronological and permanent record of all prior transactions

and another one…

A **blockchain** is a distributed database that maintains a continuously growing list of records called *blocks*. Each block contains a timestamp and a link to a previous block. By design, blockchains are inherently resistant to modification of the data — once recorded, the data in a block cannot be altered retroactively. Blockchains are "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically."[7]

[7] Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain”-*HBR*

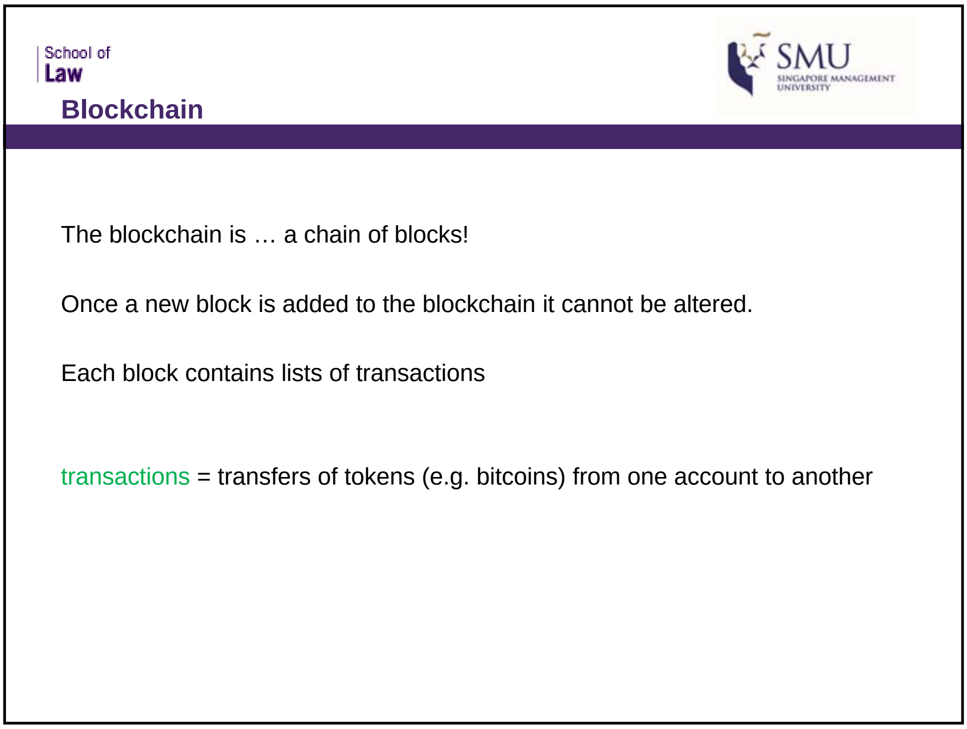
Why the big fuss?

Old components… beautifully re-arranged:

- **P2P**
- **Public Key Infrastructures (assymmetric cryptography)**
- **Decentralized consensus!**

Blockchain – main attributes

- **Decentralized** – distributed = no single point of failure but also… no single point of control
- **Secure + permanent** – cannot be modified retrospectively, *very* difficult to corrupt
- **Open** = the entire transaction history is public, visible to all



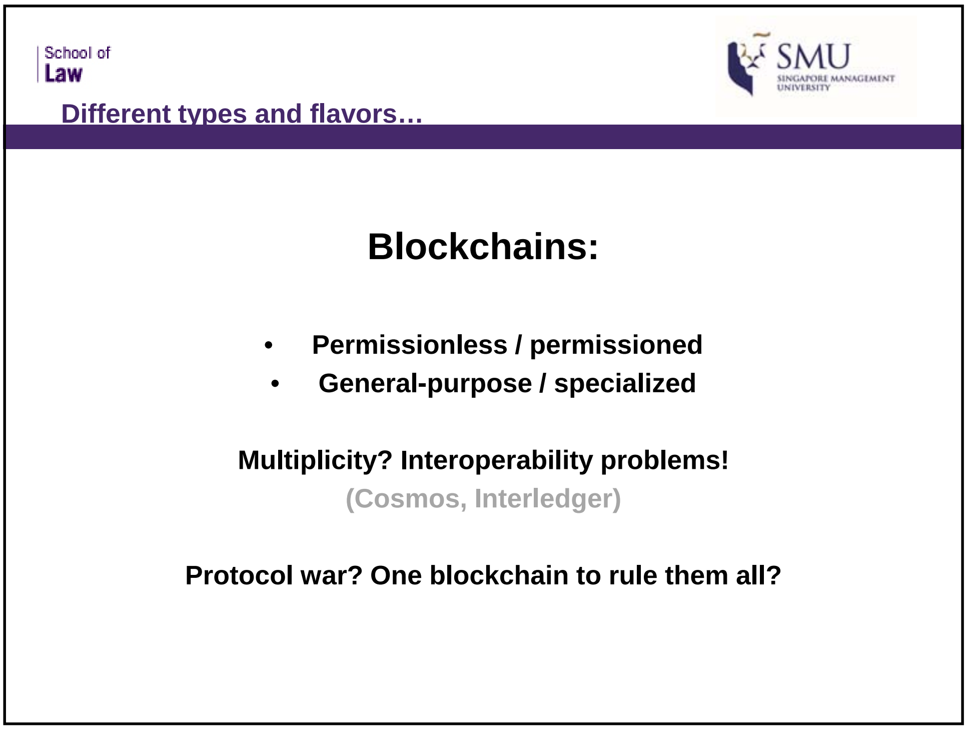
Blockchain

The blockchain is … a chain of blocks!

Once a new block is added to the blockchain it cannot be altered.

Each block contains lists of transactions

transactions = transfers of tokens (e.g. bitcoins) from one account to another



Different types and flavors…

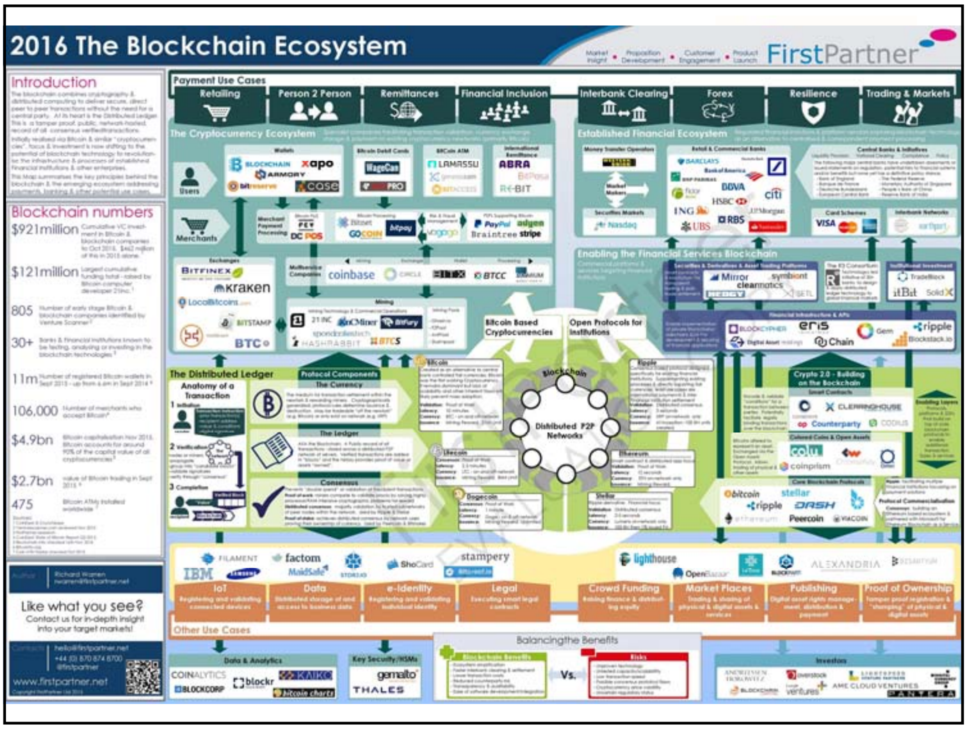
Blockchains:

- **Permissionless / permissioned**
- **General-purpose / specialized**

Multiplicity? Interoperability problems!

(Cosmos, Interledger)

Protocol war? One blockchain to rule them all?



School of
Law

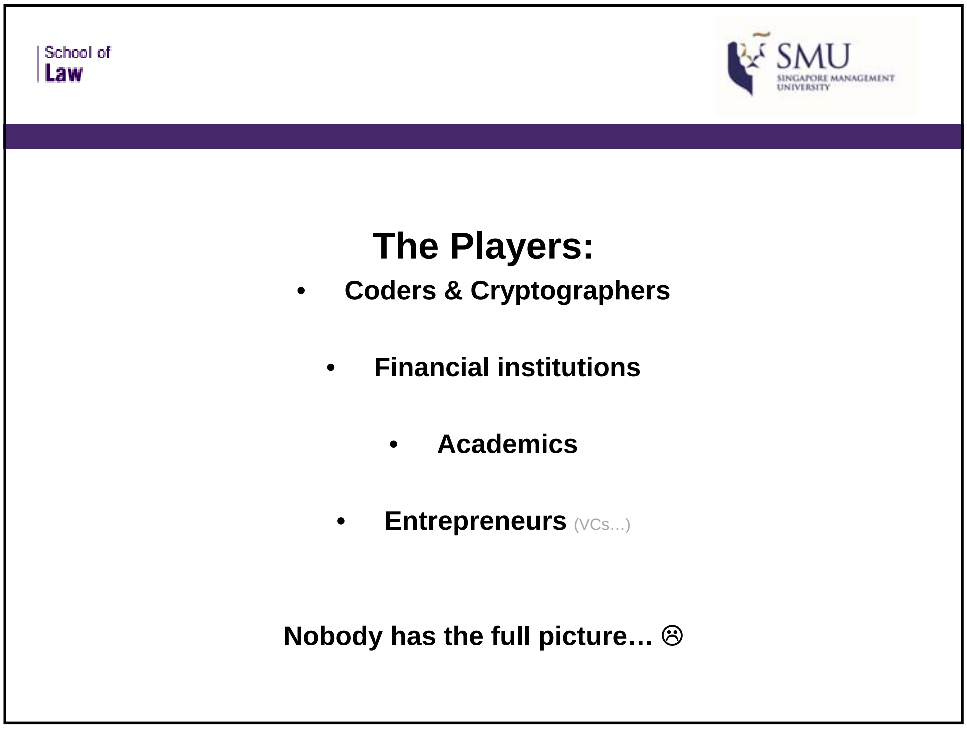
SMU
SINGAPORE MANAGEMENT UNIVERSITY

Maturity of technology?

1970? …or 1994?

Real (killer) applications?

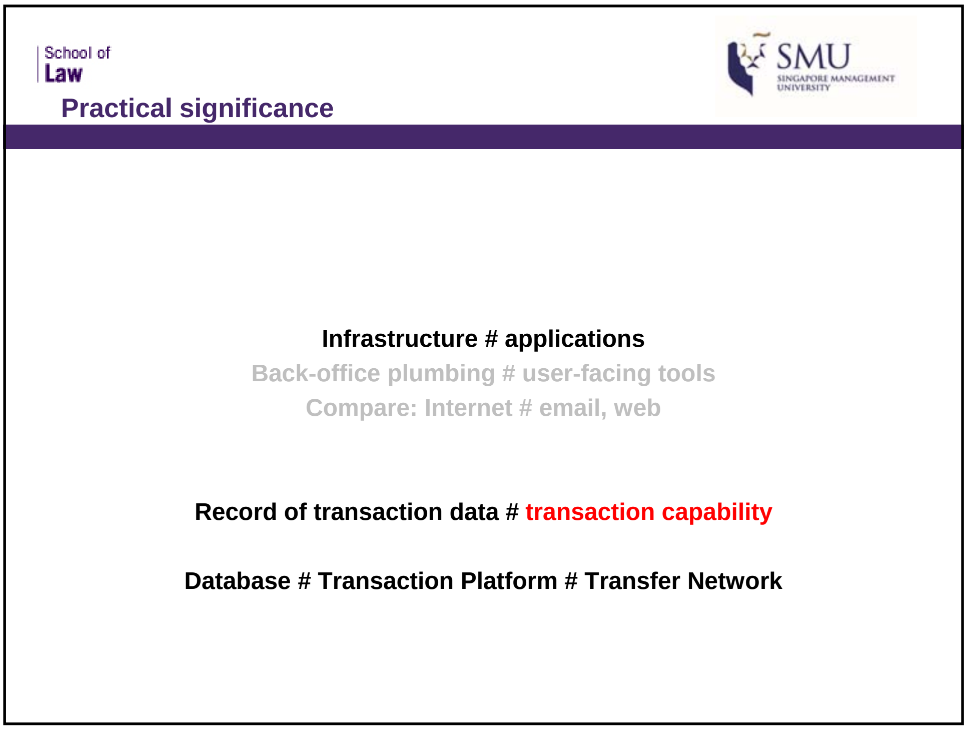
Dotcom bust soon?



The Players:

- Coders & Cryptographers
- Financial institutions
- Academics
- Entrepreneurs (VCs...)

Nobody has the full picture… ☹



Practical significance

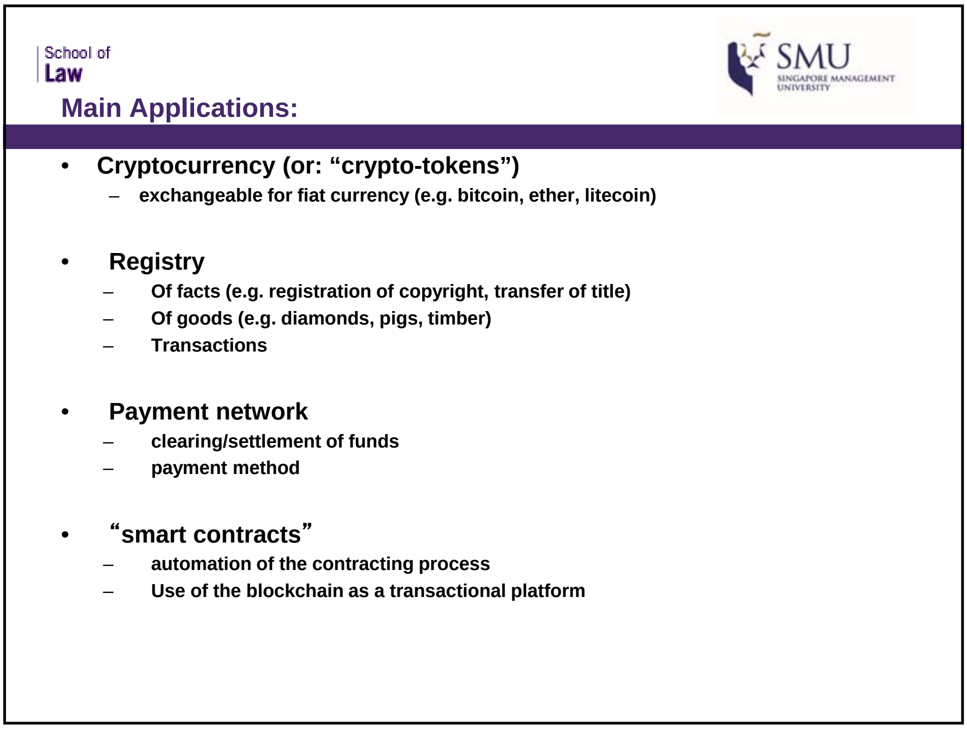
Infrastructure # applications

Back-office plumbing # user-facing tools

Compare: Internet # email, web

Record of transaction data # transaction capability

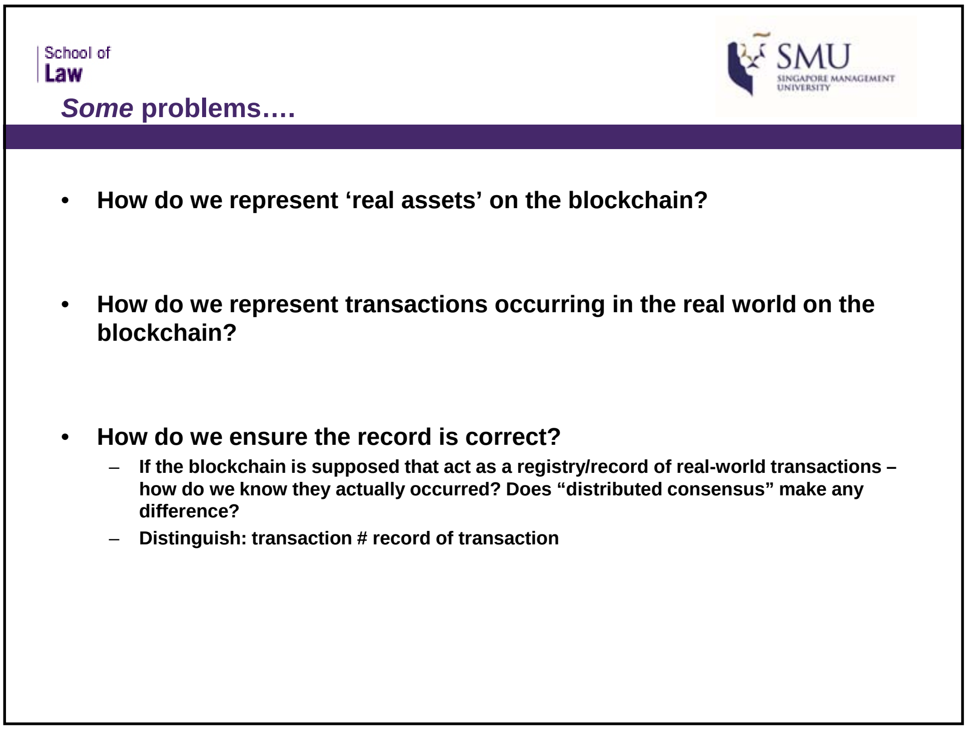
Database # Transaction Platform # Transfer Network



School of Law

Main Applications:

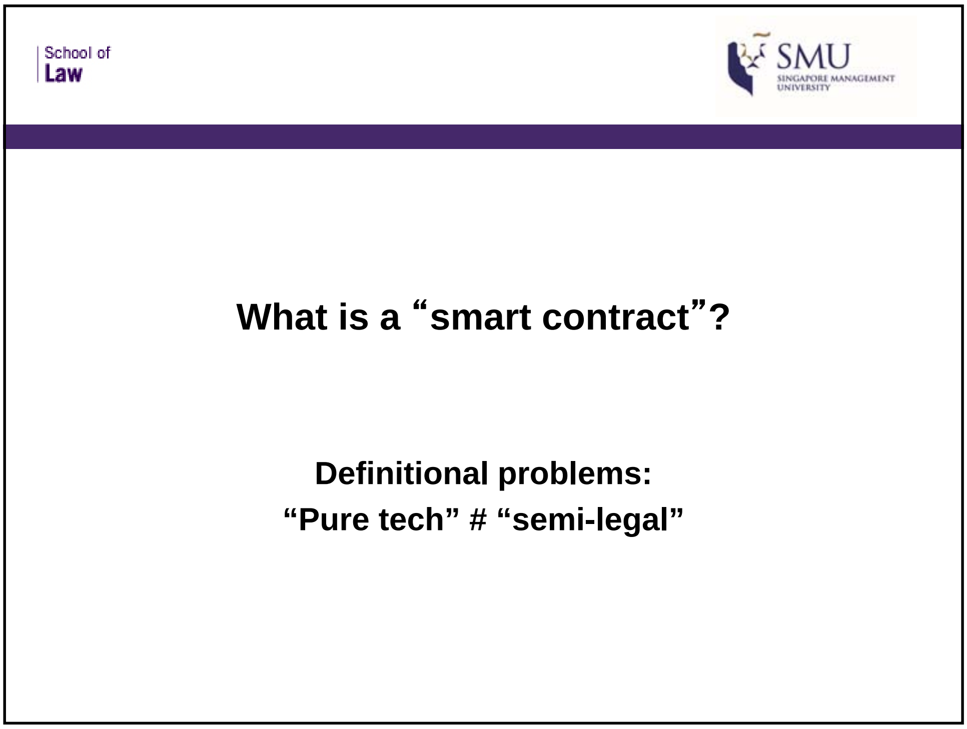
- Cryptocurrency (or: “crypto-tokens”)
  - exchangeable for fiat currency (e.g. bitcoin, ether, litecoin)
- Registry
  - Of facts (e.g. registration of copyright, transfer of title)
  - Of goods (e.g. diamonds, pigs, timber)
  - Transactions
- Payment network
  - clearing/settlement of funds
  - payment method
- “smart contracts”
  - automation of the contracting process
  - Use of the blockchain as a transactional platform



School of Law

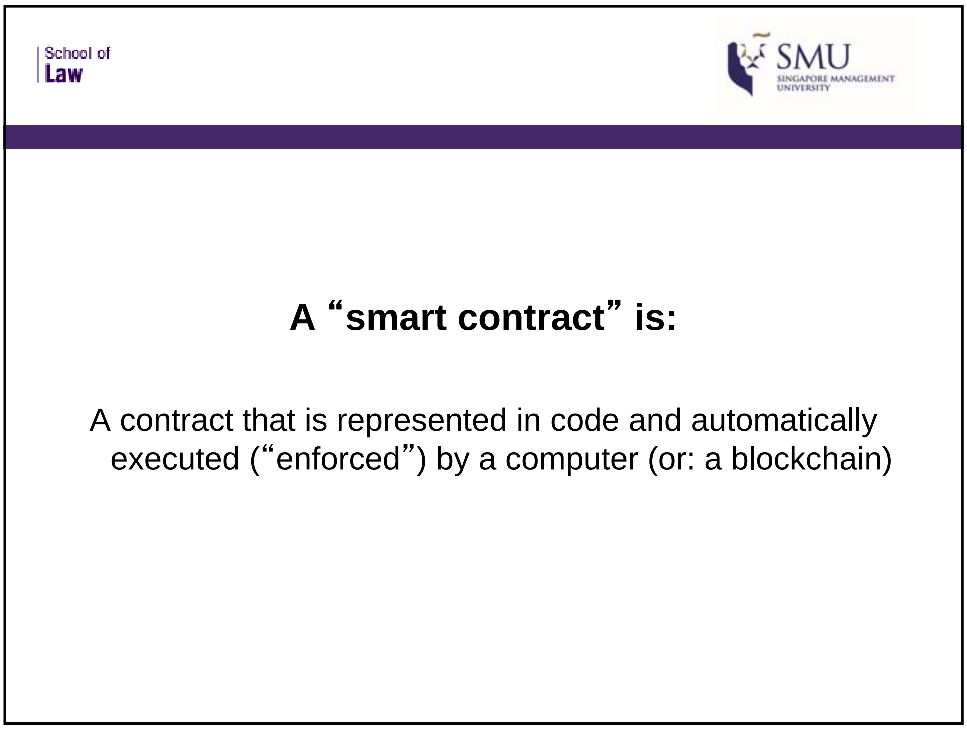
Some problems….

- How do we represent ‘real assets’ on the blockchain?
- How do we represent transactions occurring in the real world on the blockchain?
- How do we ensure the record is correct?
  - If the blockchain is supposed that act as a registry/record of real-world transactions – how do we know they actually occurred? Does “distributed consensus” make any difference?
  - Distinguish: transaction # record of transaction



What is a “smart contract”?

Definitional problems:
“Pure tech” # “semi-legal”



A “smart contract” is:

A contract that is represented in code and automatically executed (“enforced”) by a computer (or: a blockchain)

"Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols."

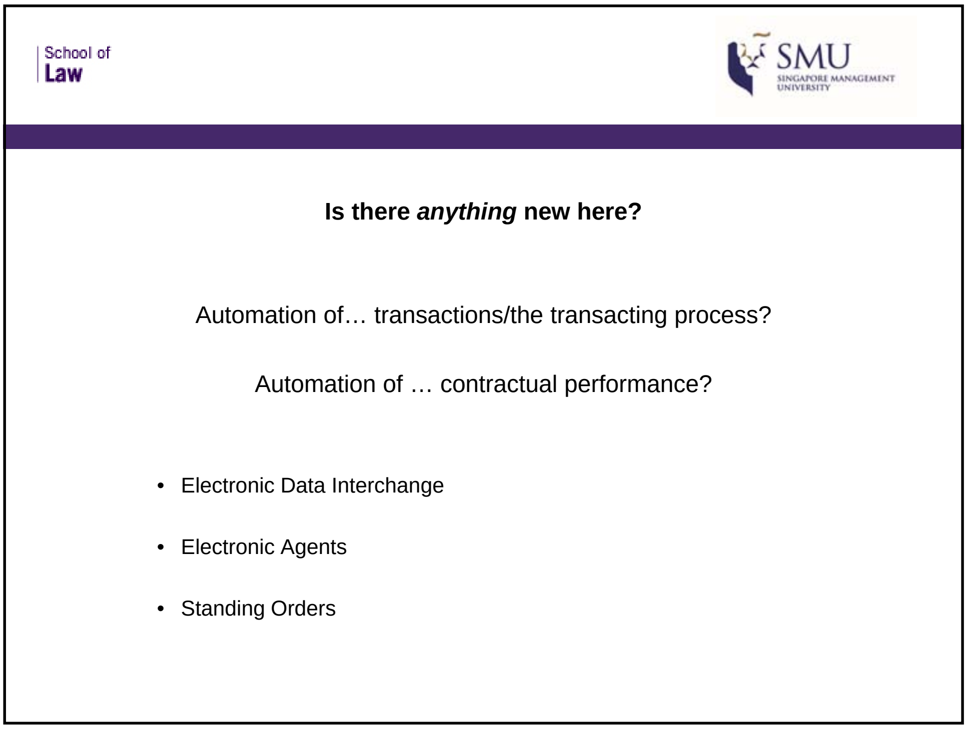
Smart contracts "*utilize protocols and user interfaces to facilitate all steps of the contracting process*," including negotiation, performance, and adjudication.

Nick Szabo, Smart Contracts: Formalizing and Securing Relationships on Public Networks, *First Monday* (1997)

+ the vending machine example

smart contracts….

- not just electronic versions of traditional contracts; not only formed online but their performance is enabled and *guaranteed* by blockchains, or other crypto-ledgers
- Originally, contemplated within a limited range of financial transactions, e.g. interest swaps.
- Progressively, the narrative has expanded, implying that all contracts can be made smart or that many different obligations can be "enforced by computers"
- Blockchains = provide secure execution environment for the smart contract or "execute" the smart contract!

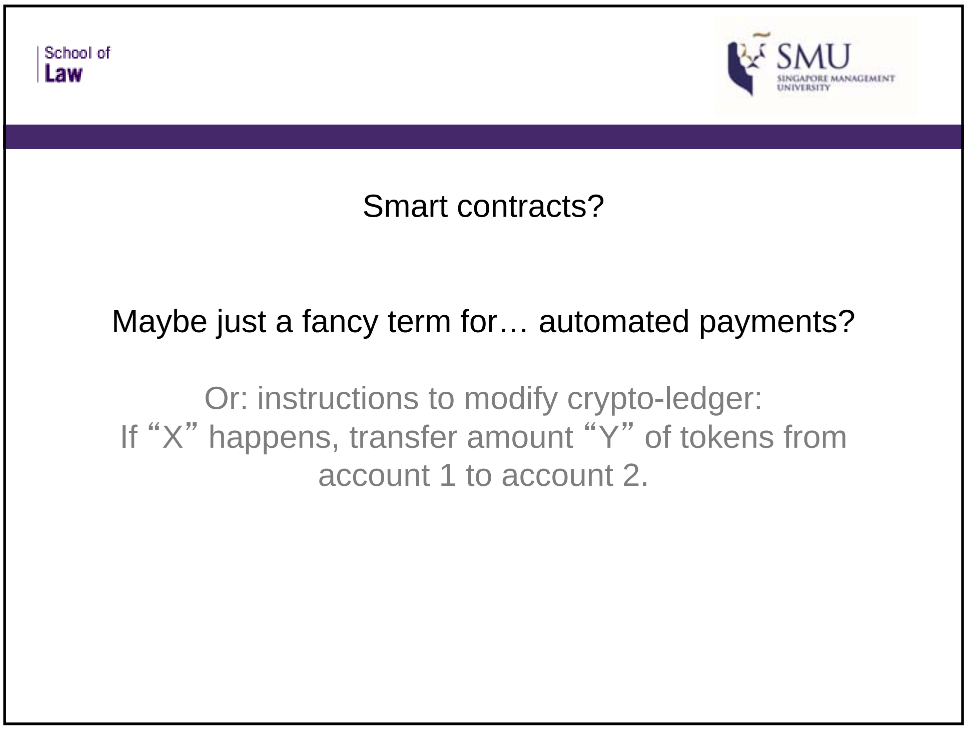


Is there *anything* new here?

Automation of… transactions/the transacting process?

Automation of … contractual performance?

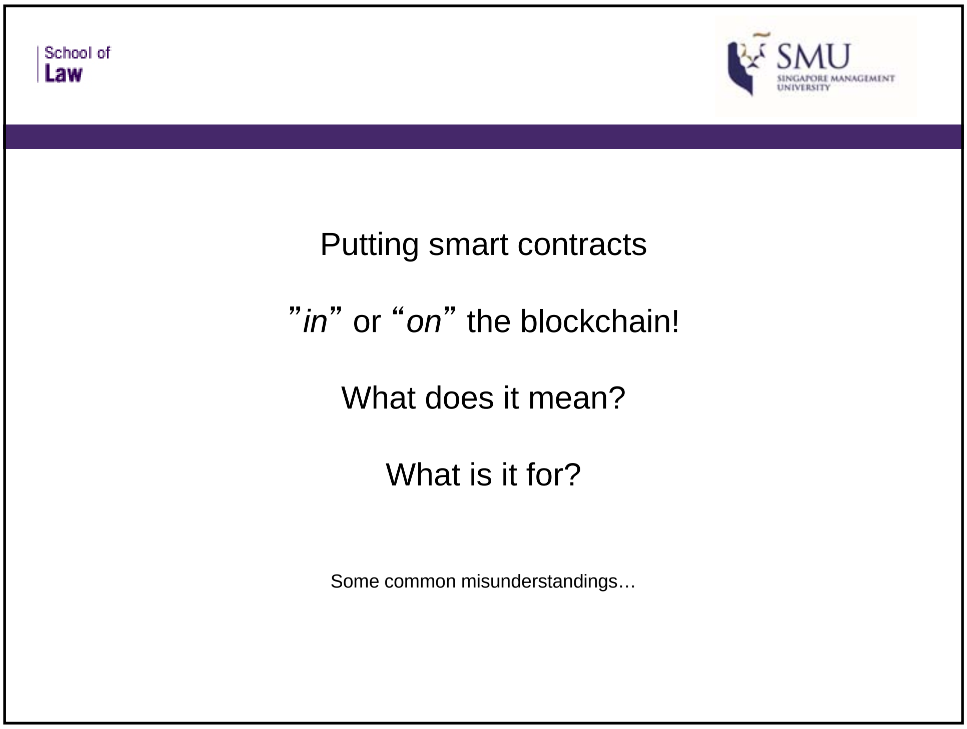
- Electronic Data Interchange
- Electronic Agents
- Standing Orders



Smart contracts?

Maybe just a fancy term for… automated payments?

Or: instructions to modify crypto-ledger:
If “X” happens, transfer amount “Y” of tokens from account 1 to account 2.



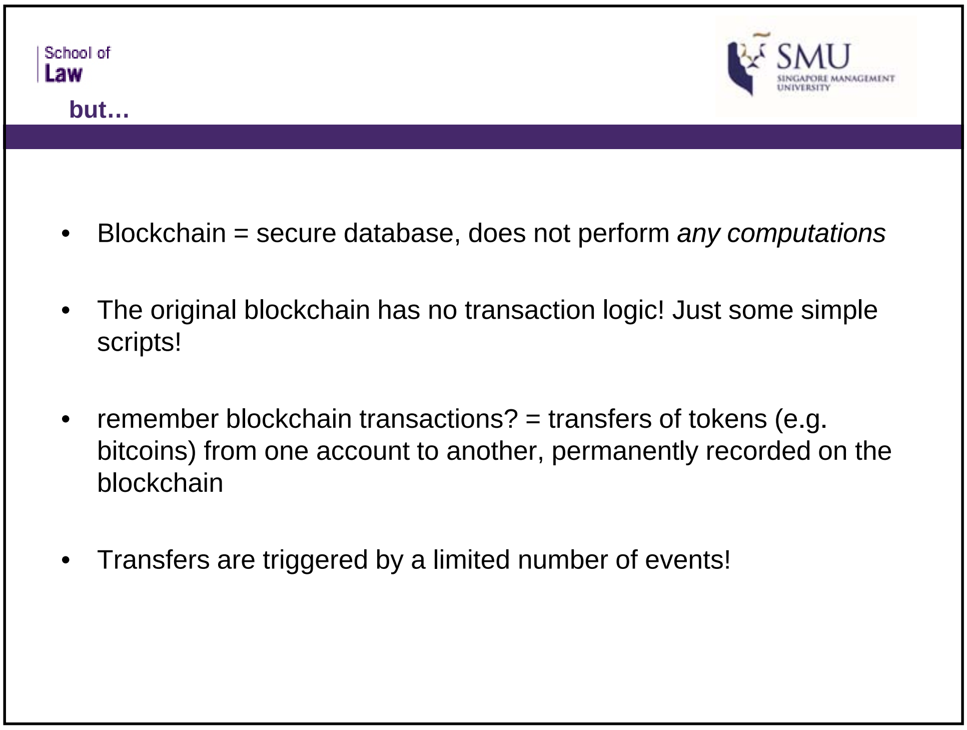
Putting smart contracts

”*in*” or “*on*” the blockchain!

What does it mean?

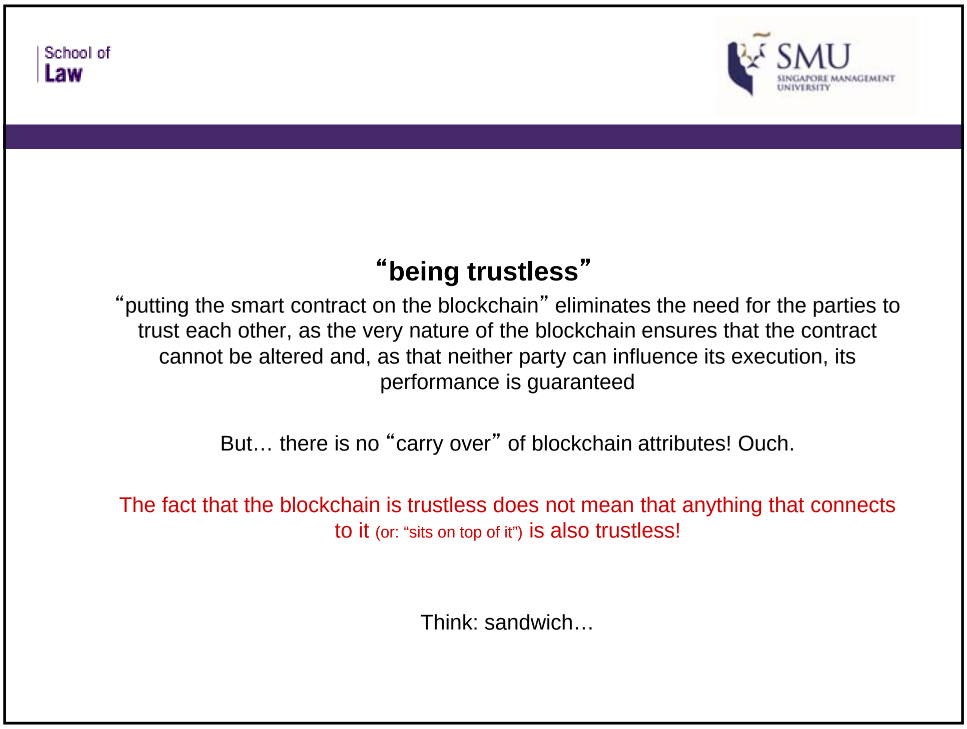
What is it for?

Some common misunderstandings…



but…

- Blockchain = secure database, does not perform *any computations*
- The original blockchain has no transaction logic! Just some simple scripts!
- remember blockchain transactions? = transfers of tokens (e.g. bitcoins) from one account to another, permanently recorded on the blockchain
- Transfers are triggered by a limited number of events!



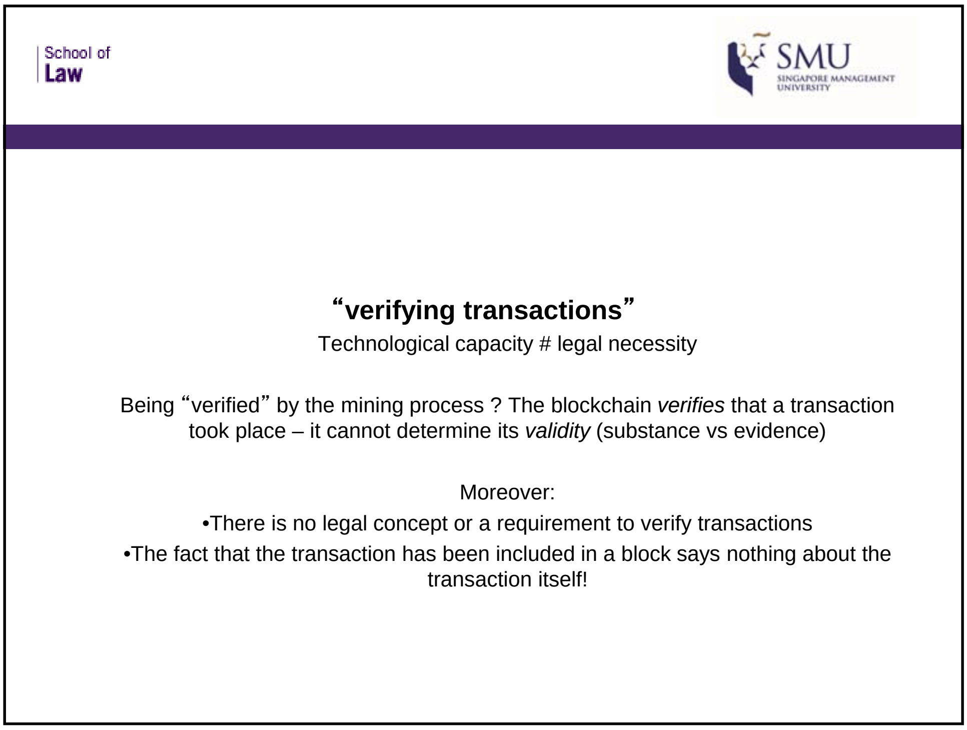
“being trustless”

“putting the smart contract on the blockchain” eliminates the need for the parties to trust each other, as the very nature of the blockchain ensures that the contract cannot be altered and, as that neither party can influence its execution, its performance is guaranteed

But… there is no “carry over” of blockchain attributes! Ouch.

The fact that the blockchain is trustless does not mean that anything that connects to it (or: “sits on top of it”) is also trustless!

Think: sandwich…



“verifying transactions”

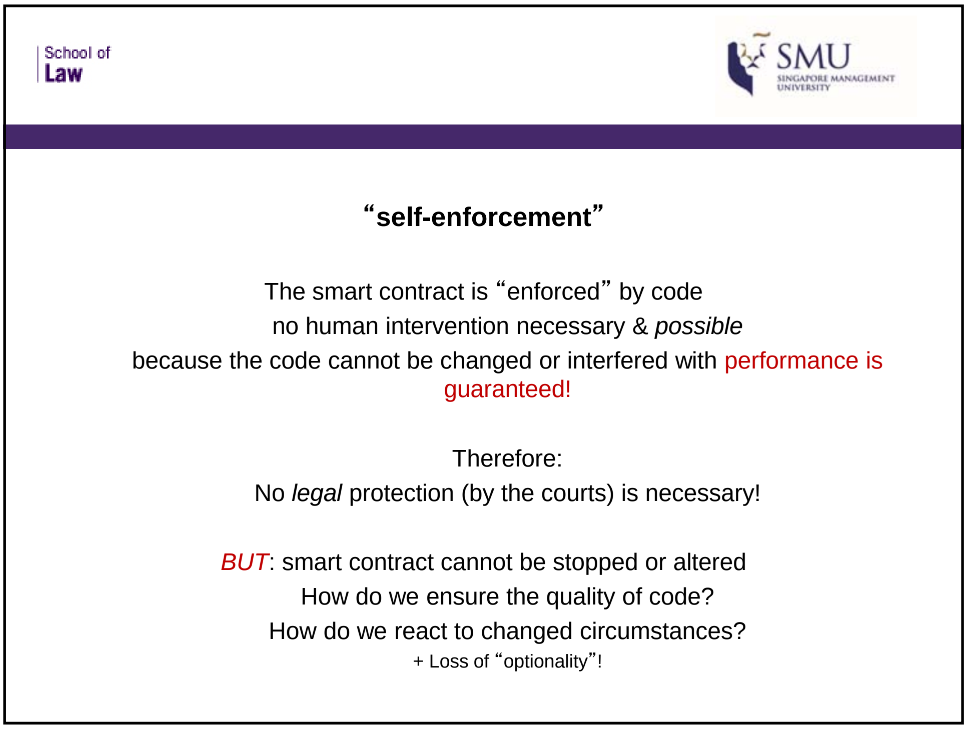
Technological capacity # legal necessity

Being “verified” by the mining process ? The blockchain *verifies* that a transaction took place – it cannot determine its *validity* (substance vs evidence)

Moreover:

•There is no legal concept or a requirement to verify transactions

•The fact that the transaction has been included in a block says nothing about the transaction itself!



“self-enforcement”

The smart contract is “enforced” by code

no human intervention necessary & *possible*

because the code cannot be changed or interfered with performance is guaranteed!

Therefore:

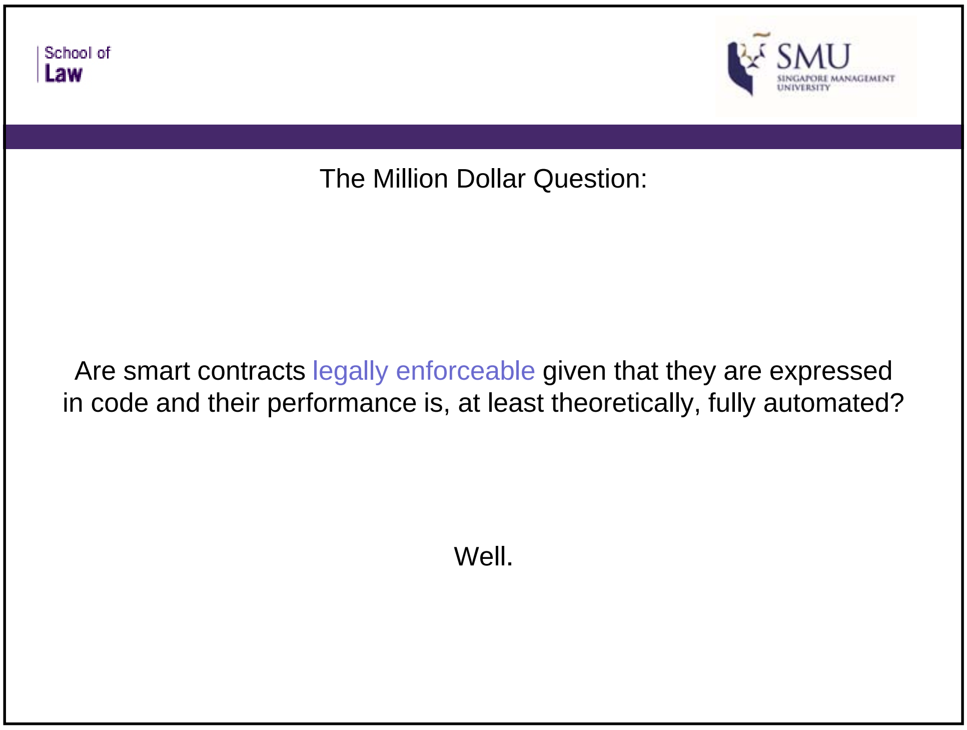
No *legal* protection (by the courts) is necessary!

BUT: smart contract cannot be stopped or altered

How do we ensure the quality of code?

How do we react to changed circumstances?

+ Loss of “optionality”!



The Million Dollar Question:

Are smart contracts legally enforceable given that they are expressed in code and their performance is, at least theoretically, fully automated?

Well.

School of
Law

Another problem:

Given that smart contracts self-enforce in response to certain events, *including contractual performance*, how is it technically possible to provide them with reliable information about real-world events?

The blockchain is blind to everything outside of it!

Need: secure data feeds about off-chain events: so-called oracles!

School of
Law

Q & A

Some good sources of info:

Anything written by Andreas Antonopoulos, one of the few super-knowledgeable people in the area

Why Many Smart Contract Use Cases Are Simply Impossible; Gideon Greenspan, April 17, 2016; http://www.coindesk.com/three-smart-contract-misconceptions/

Schumpeter, Not-so-clever contracts (2016) The Eonomist, at: www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted

J. Stark. Making sense of blockchain smart contracts (2016) www.coindesk.com/making-sense-smart-contracts

T. Swanson. Great chain of numbers: A guide to smart contracts, smart property and trustless asset management, 2014