Blockchain and ‘smart contracts’

A laboratory of IT Fails and regulatory trainwrecks or the next big thing?

David Vaile

Stream lead, privacy and surveillance,
Allens Hub for Technology Law and Innovation, Law Faculty
http://cyberlawcentre.org/comp4920/ (temp)

https://flipboard.com/@unsecurity
‘Blockchain, bitcoin & virtual currencies’

Outline for Introduction

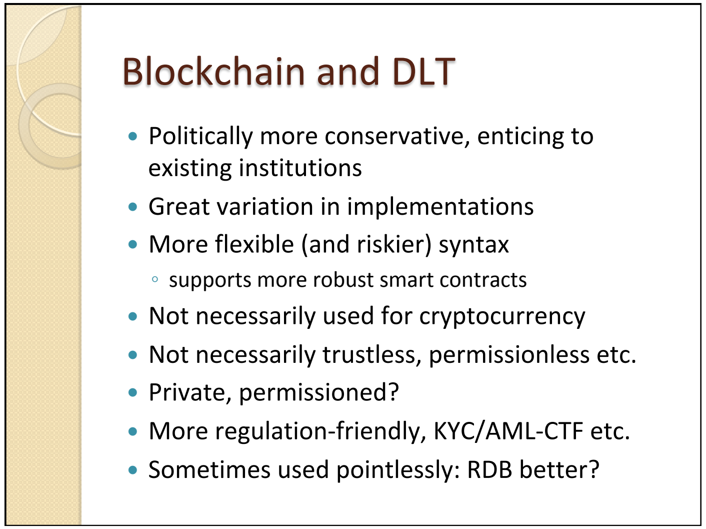
- *Bitcoin – crude but effective – the first successful blockchain cryptocurrency*
- *Blockchain and DLT*
- *Virtual currency – not our focus*
- *Smart contracts*
- *Buzzwords*
- *Consensus*
- *Resources on web page*

Why should I care?

- Blockchain continues to attract great interest, but poses great risks for the gullible
- Complex politically, technically and legally
- Great variation in assumptions, functionality, goals
- Great confusion
- Enormous hype
- Really bad, breathless writing
- Potentially very important

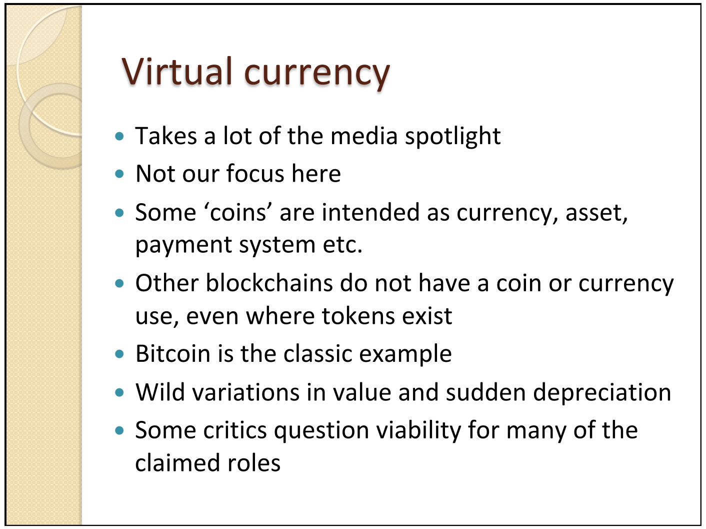
Bitcoin

- Crude but effective: 1st real blockchain cryptocurrency
- Crypto-anarchist motivation; anonymity via crypto
- Libertarian: government as threat, private actors less so
- Miners create blocks, compete for rewards, burn carbon in pointless cryptographic hashing, ever less efficient
- Radical decentralisation, duplication of the data store
- Very limited syntax, hardened to survive malefactors
- Prone to all the excesses of unregulated private schemes, including bubbles, scams and speculation
- Clever design but thwarted by large scale market manipulation, Chinese 51% miners



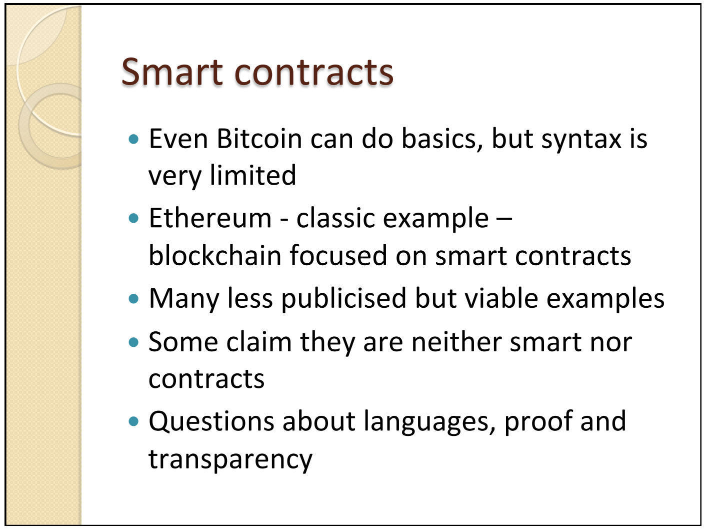
Blockchain and DLT

- Politically more conservative, enticing to existing institutions
- Great variation in implementations
- More flexible (and riskier) syntax
  - supports more robust smart contracts
- Not necessarily used for cryptocurrency
- Not necessarily trustless, permissionless etc.
- Private, permissioned?
- More regulation-friendly, KYC/AML-CTF etc.
- Sometimes used pointlessly: RDB better?



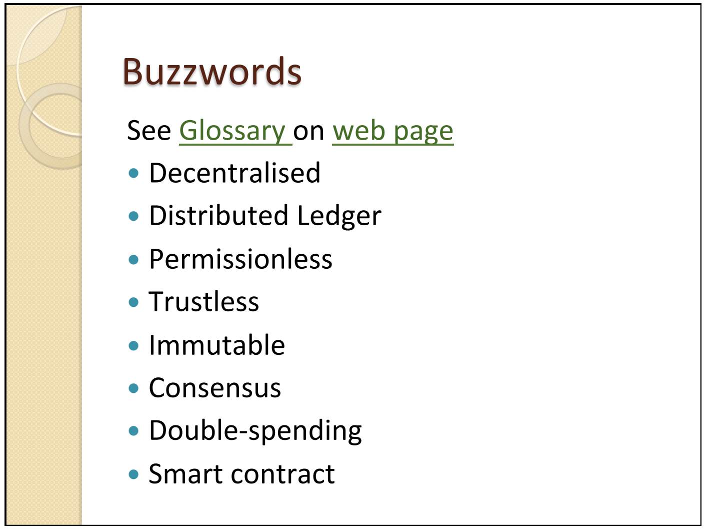
Virtual currency

- Takes a lot of the media spotlight
- Not our focus here
- Some ‘coins’ are intended as currency, asset, payment system etc.
- Other blockchains do not have a coin or currency use, even where tokens exist
- Bitcoin is the classic example
- Wild variations in value and sudden depreciation
- Some critics question viability for many of the claimed roles



Smart contracts

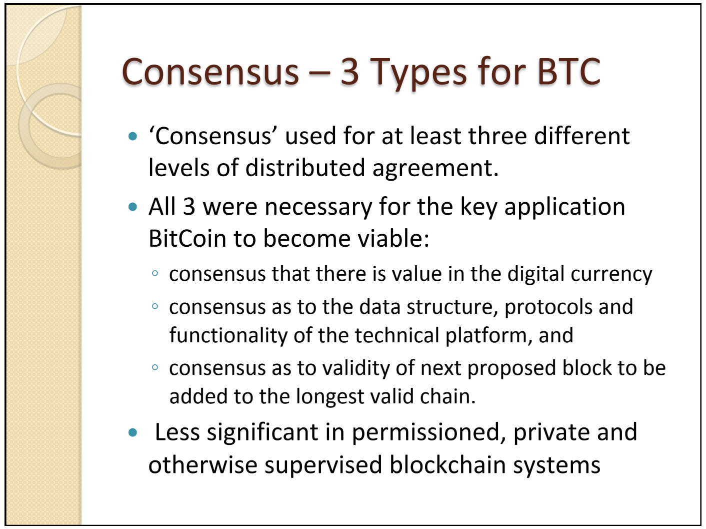
- Even Bitcoin can do basics, but syntax is very limited
- Ethereum - classic example – blockchain focused on smart contracts
- Many less publicised but viable examples
- Some claim they are neither smart nor contracts
- Questions about languages, proof and transparency



Buzzwords

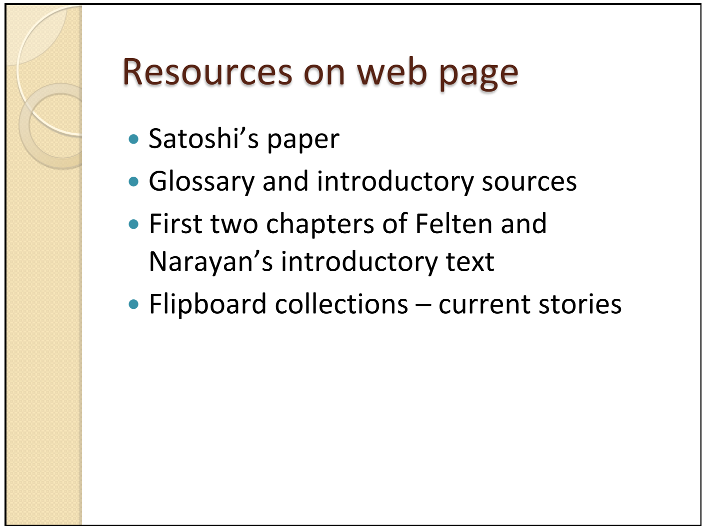
See Glossary on web page

- Decentralised
- Distributed Ledger
- Permissionless
- Trustless
- Immutable
- Consensus
- Double-spending
- Smart contract



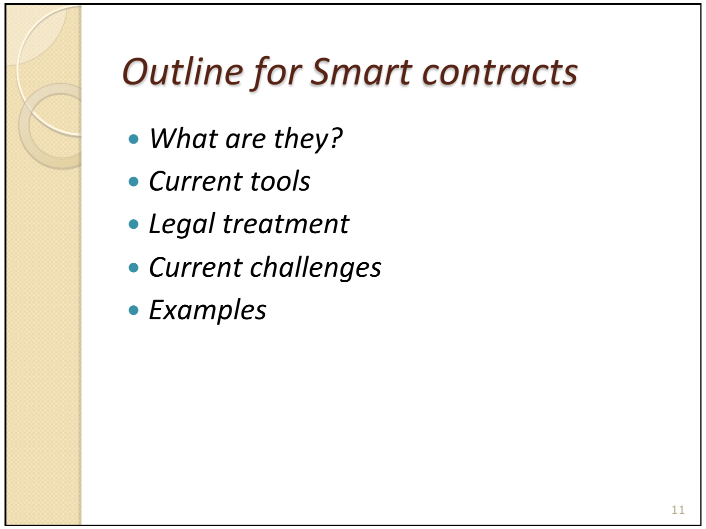
Consensus – 3 Types for BTC

- 'Consensus' used for at least three different levels of distributed agreement.
- All 3 were necessary for the key application BitCoin to become viable:
  - consensus that there is value in the digital currency
  - consensus as to the data structure, protocols and functionality of the technical platform, and
  - consensus as to validity of next proposed block to be added to the longest valid chain.
- Less significant in permissioned, private and otherwise supervised blockchain systems



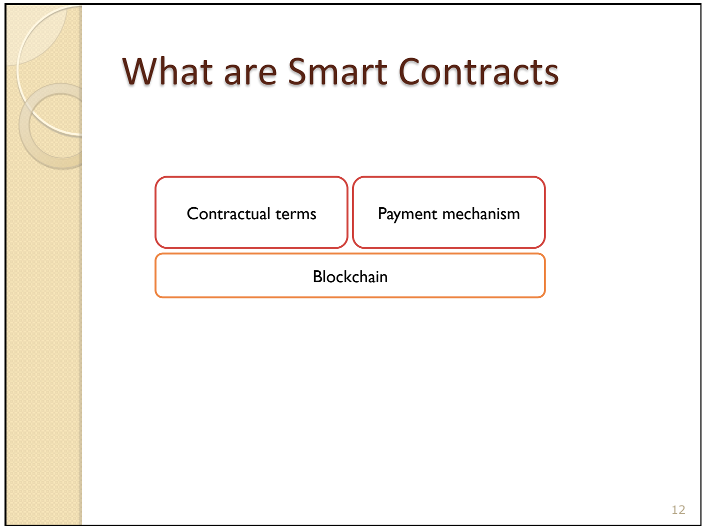
Resources on web page

- Satoshi's paper
- Glossary and introductory sources
- First two chapters of Felten and Narayan's introductory text
- Flipboard collections – current stories



Outline for Smart contracts

- *What are they?*
- *Current tools*
- *Legal treatment*
- *Current challenges*
- *Examples*



What are Smart Contracts

Contractual terms

Payment mechanism

Blockchain

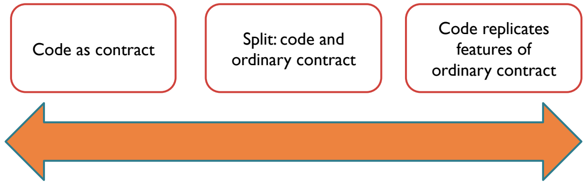
What are Smart Contracts (cont.)

- Blockchain is a data storage technology
  - Unchangeable data is stored in packages called blocks.
  - These blocks provide a record of each transaction, and are chained together in chronological order.
  - The database is distributed, meaning that it is not located just in one place or on one computer. Rather, information is disbursed across a network of interconnected computers ("nodes")
  - Every computer on the distributed network had a full and complete copy of every transaction in the chain.
- Blockchain is distributed, traceable and immutable

What are Smart Contracts (cont.)

- Blockchain
  - Core use is to store a ledger
    - Bitcoin – very basic operators but reliable store
    - Land titles
  - Can also be used to store code
- Smart contracts use block chain to:
  - store code and ensure it remains unchanged
  - execute the code (ie perform the contract)
  - effect payments

What are Smart Contracts (cont.)


Code as contract
Split: code and ordinary contract
Code replicates features of ordinary contract

- Unlikely that any real world transaction could be 100% 'code as contract'
- [Though see 'DAO'!]

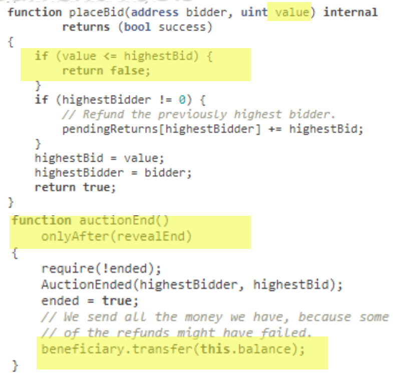
What are Smart Contracts (cont.)

- Potential benefits
  - Efficient performance of objective obligations
  - Reduce manual errors and reconciliation
  - Reduce need for intermediaries / execution risk
  - Reduce implementation / monitoring costs
- Some examples
  - payment guarantees
  - derivatives
  - recording ownership and flowing through payments

Current Tools

- Ethereum
  - Uses a simple programming language to record the contract terms
  - Payments can be made by ether, a cryptocurrency like Bitcoin
- Corda
  - Developed by R3
  - Key difference from ethereum is option for privacy

Current Tools



```
function placeBid(address bidder, uint value) internal
        returns (bool success)
{
    if (value <= highestBid) {
        return false;
    }
    if (highestBidder != 0) {
        // Refund the previously highest bidder.
        pendingReturns[highestBidder] += highestBid;
    }
    highestBid = value;
    highestBidder = bidder;
    return true;
}
function auctionEnd()
    onlyAfter(revealEnd)
{
    require(!ended);
    AuctionEnded(highestBidder, highestBid);
    ended = true;
    // We send all the money we have, because some
    // of the refunds might have failed.
    beneficiary.transfer(this.balance);
}
```

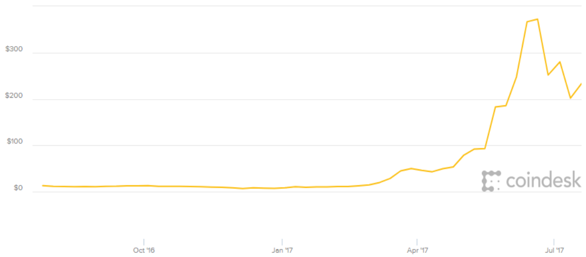
Legal treatment

- Binding and enforceable?
  - Ordinary common law principles apply
    - A promise intended to bind
    - ‘meeting of two minds’
    - Something for something
    - Sufficiently ascertainable, not void for uncertainty
  - Specific statutory requirements may need to be reviewed in some jurisdictions
- Confidentiality
  - Contract terms may be publically available

Current Challenges

- Unintended outcomes
  - eg Ethereum lottery
- “Oracles”
  - Reliability of external triggers
- Maturity of existing tools
  - Latency and execution cost
  - Templates for common obligations
  - Additional layer of abstraction
  - Interaction with ordinary contract

Current Challenges



Examples

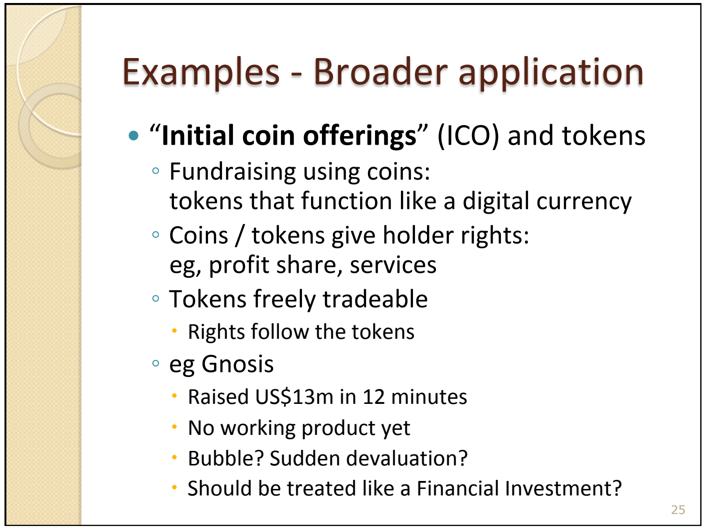
- Early experimentation
  - Distributed Autonomous Organisation, 'The DAO'
    - Venture capital firm: no management structure or board
    - Powered by a bundle of Ethereum smart contracts
    - DAO invests in projects after online voting by investors
    - May 2016, raised over $150m from 10,000+ investors
    - June 2016, DAO code 'hacked' and $50 million siphoned into various accounts (child DAOs?)
    - Ethereum organisers partially reversed the hack by adjusting the blockchain records
      - Immutable?
      - 'Code is law'? Not a hack?
    - Human readable for understandable meaning?
    - Software tools for provable meaning? Not Jscript?

Examples

- Financial services use-cases
  - **Derivatives**
    - Barclays and R3 pilot for interest rate swaps
    - DTCC and banks trial for credit default swaps
  - Syndicated **loans**
    - Credit Suisse, R3 and other pilot for syndicated loans – automating aspects of loan creation, settlement and secondary trading
  - **Trade settlement** and **KYC**
    - Blockchain ledger to record ownership and smart contract to effect trade clearing and settlement
    - ASX and a number of other exchanges are conducting trials

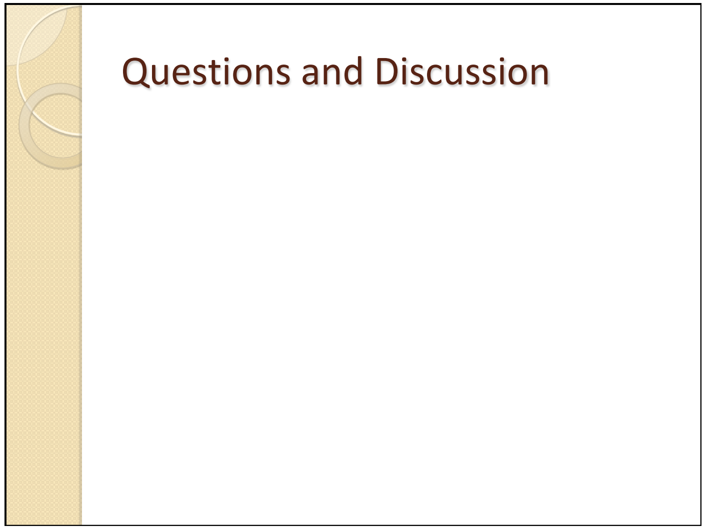
Examples - Broader application

- International trade
  - **Automated payments** and **title transfer**
  - Based on location triggers
  - eg Wave
    - Storing bills of lading on blockchain
- **Escrow**
  - Bitcoin does basic escrow – multisig: 2 of 3 to sign
- Renewable energy micro grid
  - **Peer to peer trading** of electricity in real time



Examples - Broader application

- “**Initial coin offerings**” (ICO) and tokens
  - Fundraising using coins:
    tokens that function like a digital currency
  - Coins / tokens give holder rights:
    eg, profit share, services
  - Tokens freely tradeable
    - Rights follow the tokens
  - eg Gnosis
    - Raised US$13m in 12 minutes
    - No working product yet
    - Bubble? Sudden devaluation?
    - Should be treated like a Financial Investment?



Questions and Discussion

Thanks

David Vaile
Allens Hub for Technology, Law and Innovation, Law Faculty
d.vaile@unsw.edu.au
http://cyberlawcentre.org/comp4920/

https://flipboard.com/@unsecurity
‘Blockchain, bitcoin & virtual currencies’