Who am I?

- PhD in Physics
- Postdoc in Mathematics @UniMelb
- Curtin Institute for Computation
- Part of a team of Computational Specialists
- Not exactly a blockchain expert
Outline

- Introduce the blockchain
- Dive into Bitcoin
- Introduce basic ideas behind Smart Contracts
What is the blockchain?
Is there a definition?

- Unfortunately there's no agreed definition
- Nakamoto introduces the digital currency Bitcoin in 2008
- He never uses the term *blockchain*
- Now used to describe any technology inspired by Bitcoin
Or too many definitions?

- A shared ledger?
- A distributed database?
- A consensus protocol?

Hard to separate it from the original use case: digital currencies
Digital currencies

- A form of electronic cash
  - Independent from any financial institution
  - Require no central bank or intermediary
- Internet lets us talk freely with anyone
- Can it also let us trade freely with anyone?
- Bitcoin is the first complete answer to this problem
Bitcoin (ELI5 version)

- A software you install on your computer
- Maintains a peer-to-peer network
- Lets you send/receive transactions to/from any user
- All transactions are shared by all nodes and can be verified
- https://bitcoin.org
The making of Bitcoin
The problem

- Alice and Bob are stamp collectors
- Bob has a stamp that Alice wants
- Alice doesn't have anything that Bob wants
- Alice will have to repay *in the future*

Images credit Ilya Grigorik "Minimum Viable Block Chain"
Verifying authenticity

- Use a digital signature to verify the authenticity of a transaction
- Just like normal signatures but you can't cut and paste them
- Each signature is tied to the document it signs
A ledger for two

- A&B can exchange signed transactions like above
- A&B can compute their balance by taking the sum of transactions
Manage-à-trois

- How can Bob transfer his balance to John?
Cryptographic hash functions

<table>
<thead>
<tr>
<th>Input</th>
<th>Digest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fox</td>
<td>DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17</td>
</tr>
<tr>
<td>The red fox jumps over the blue dog</td>
<td>0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC</td>
</tr>
<tr>
<td>The red fox jumps over the blue dog</td>
<td>8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819</td>
</tr>
<tr>
<td>The red fox jumps over the blue dog</td>
<td>FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45</td>
</tr>
<tr>
<td>The red fox jumps over the blue dog</td>
<td>8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C</td>
</tr>
</tbody>
</table>
Manage-à-trois

- How can Bob transfer his balance to John?

- John can go to Alice and ask her for payment, even though Alice wasn't present!
Double-spending

Both John and Katy will go to Alice asking for their payment!
Distributed consensus problem

- Ledger need to be shared and in sync
- One can wait until each transaction is acknowledged
  - by everybody (unanimous consensus)
  - by a quorum (e.g. 50%) acknowledge
- Only works in a closed system
- Open system is vulnerable to the Sybil attack
"On the Internet, nobody knows you're a dog."
Sybil attack

One can generate fake "identities" and trick any system based on quorum
Proof-of-work

- Bitcoin's original solution
- Anyone can vote to confirm a transaction
- Casting a vote is made expensive
- Cost adjusted to be more than value gained by attacking the system
Proof-of-work #2

- To validate a transaction, one needs to
  - find a number
  - that added to the transaction data
  - and passed through a hash-function
  - gives something that start with zeroes
- Basically a lottery that requires a lot of CPU power
Alice gave Bob a Red Stamp (attempt 1) cfd1fc23...
Alice gave Bob a Red Stamp (attempt 2) 7a744558...
Alice gave Bob a Red Stamp (attempt 3) bd4024a8...
Alice gave Bob a Red Stamp (attempt 4) 9c70e8c0...
Alice gave Bob a Red Stamp (attempt 5) 6dd74f3f...
Alice gave Bob a Red Stamp (attempt 6) 8ae41e6c...
Alice gave Bob a Red Stamp (attempt 7) 15811e32...
Alice gave Bob a Red Stamp (attempt 8) d5b9ec52...
Alice gave Bob a Red Stamp (attempt 9) ae552078...
Alice gave Bob a Red Stamp (attempt 10) 1aeb7a1c...
Alice gave Bob a Red Stamp (attempt 11) 79dc0892...
Alice gave Bob a Red Stamp (attempt 12) bfc39562...
Alice gave Bob a Red Stamp (attempt 13) 3a73b5de...
Alice gave Bob a Red Stamp (attempt 14) cf39b99e...

Alice gave Bob a Red Stamp (attempt 15) 02d1cd9f...
Transaction blocks

- Participants in the network incur a cost to validate transactions
- Then they must have an economic incentive
Bitcoin mining

- Anyone can make a profit by verifying transactions
- More participants make a stronger network
Conflicts
Verification

- Deeper is a transaction, lower the chances it will be reverted
- Reverted ~ "unverified"
- Bitcoin adjusts proof-of-work so a block takes ~10min
Bitcoin summary

- Completely distributed and decentralised network
- Self-sustainable thanks to right incentives
- Anyone can send transactions to anyone
- Transactions "eventually guaranteed"
Pain-points

- By design, anybody can verify transactions
  - No true anonymity, only "pseudonymity"
- By design, transactions are irreversible
  - More like barter, no one to complain to
- Security is vital, your computer is your money
Smart contracts
- Bitcoin network
  - verifies transactions
  - updates the ledger
  - ~executes the transaction
- What about a more complex transaction?
  - Call option
  - Right to buy a commodity at some time for a certain price
- What about paying a recurring bill?
The Ethereum platform

- Started in 2015
- Software similar to Bitcoin
- Built-in currency Ether, just like Bitcoin
- Smart contract platform
- You can write programs that define the rules of your game
- These contracts are executed by the network
- In a reliable and verifiable way
Decentralised applications

- Digital signatures system that ensure authenticity and proof of existence used by the Luxembourg Stock Exchange
- Digital rights management for music
- Digital tokens that can be exchanged or traded
- Smart-locks and IoT
Crowdfunding

- Digital tokens can be used for crowdfunding
- Contract creates 100 tokens
- Contract trades those tokens for Ether
- Contract allows me to spend the Ethers
- Contract trades tokens for final product when available
The DAO

- Stands for *Decentralized autonomous organization*
- Venture capital fund
- Implemented as an open-source smart-contract
- Crowdfunded via a token sale in May 2016, ~$120M
The DAO

- During July 2016 Hackers exploited a bug in the smart-contract
- A third of the fund got stolen
- Ethereum community split in two
- Majority decided to fix the bug
- New version doesn't recognise the "theft" transaction as valid
- Stolen funds where reappropriated
- History got rewritten
Moral

- distributed consensus between machines ✔
- distributed consensus between humans ✗
Questions?