Blockchain in the Life Sciences

Stephen Downes

National Research Council Canada

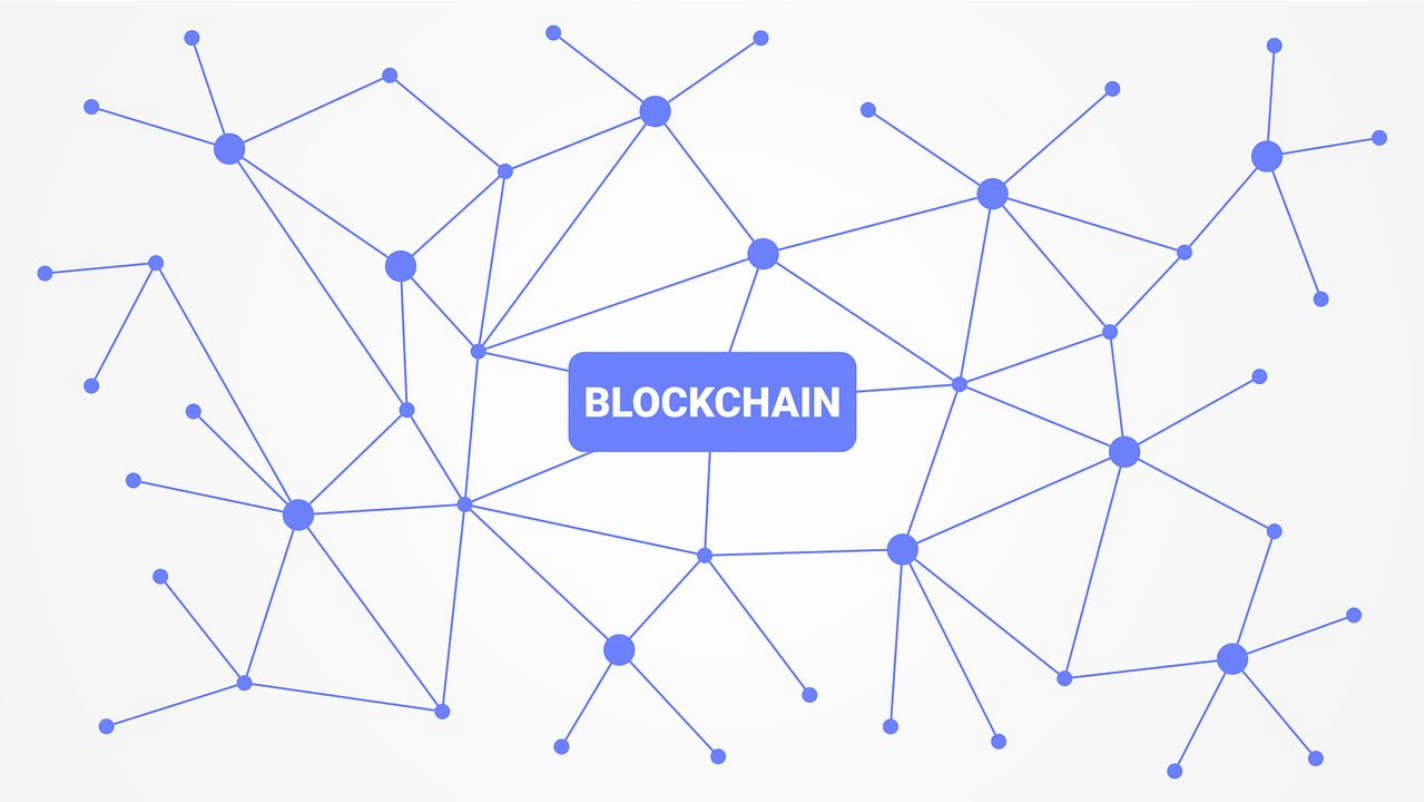
May 30, 2018

Areas of Application

- Electronic Health Record
- Medical Inventory
- Certification and Compliance
- Medical Research Data

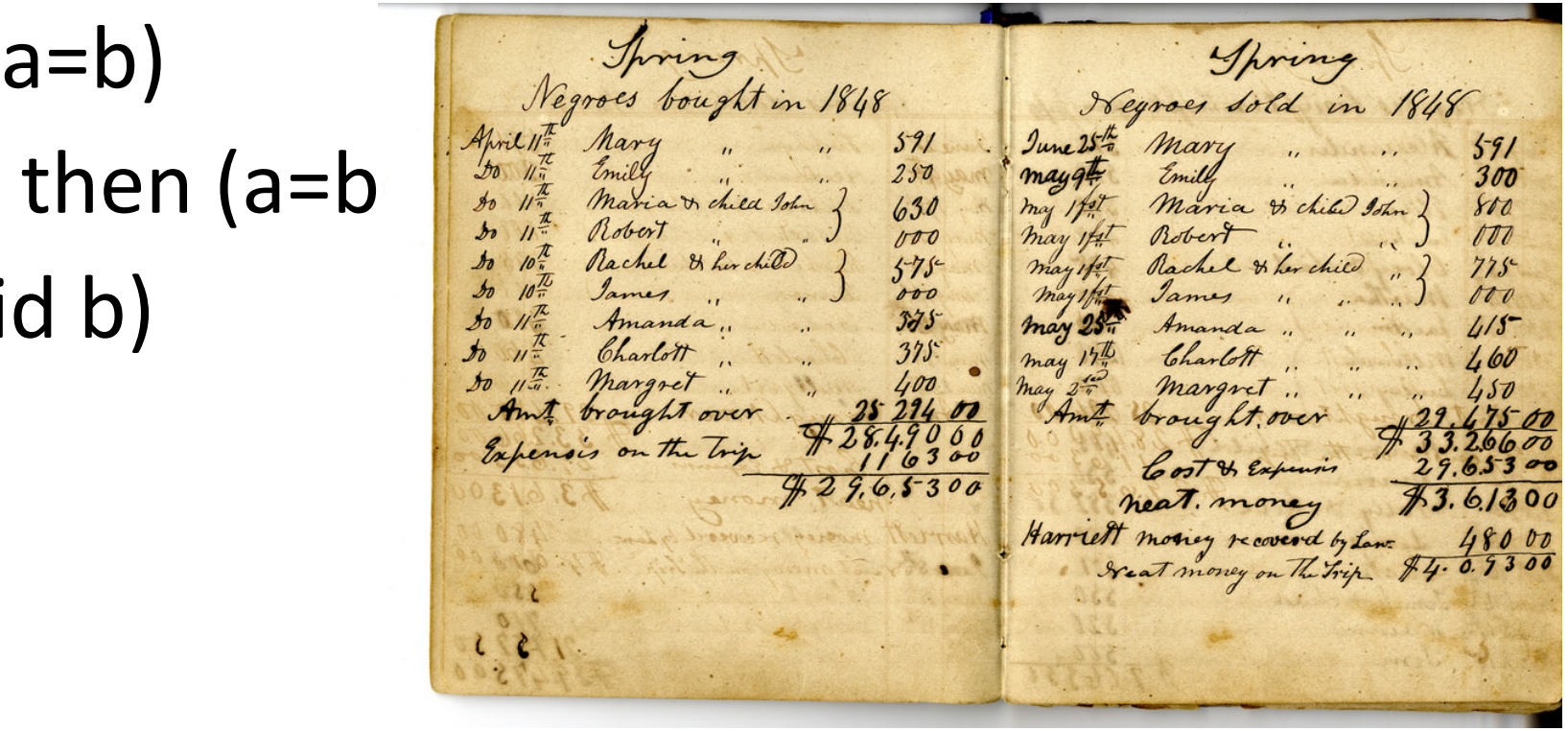
What is Blockchain?

‘A permanent distributed consensus-based ledger’



Ledger

- Transactions (a=b)
- Contracts (if c then (a=b
- Activities (a did b)



Spring

Negroes bought in 1848

April 11th	Mary	" "	591
Do 11th	Emily	" "	250
Do 11th	Maria & child John	"	630
Do 11th	Robert	"	000
Do 10th	Rachel & her child	"	575
Do 10th	James	"	000
Do 11th	Amanda	" "	375
Do 11th	Charlott	" "	375
Do 11th	Margret	" "	400
Amt brought over			25 294 00
			$ 28.490 00
Expenses on the Trip			1163 00
			$ 29.653 00

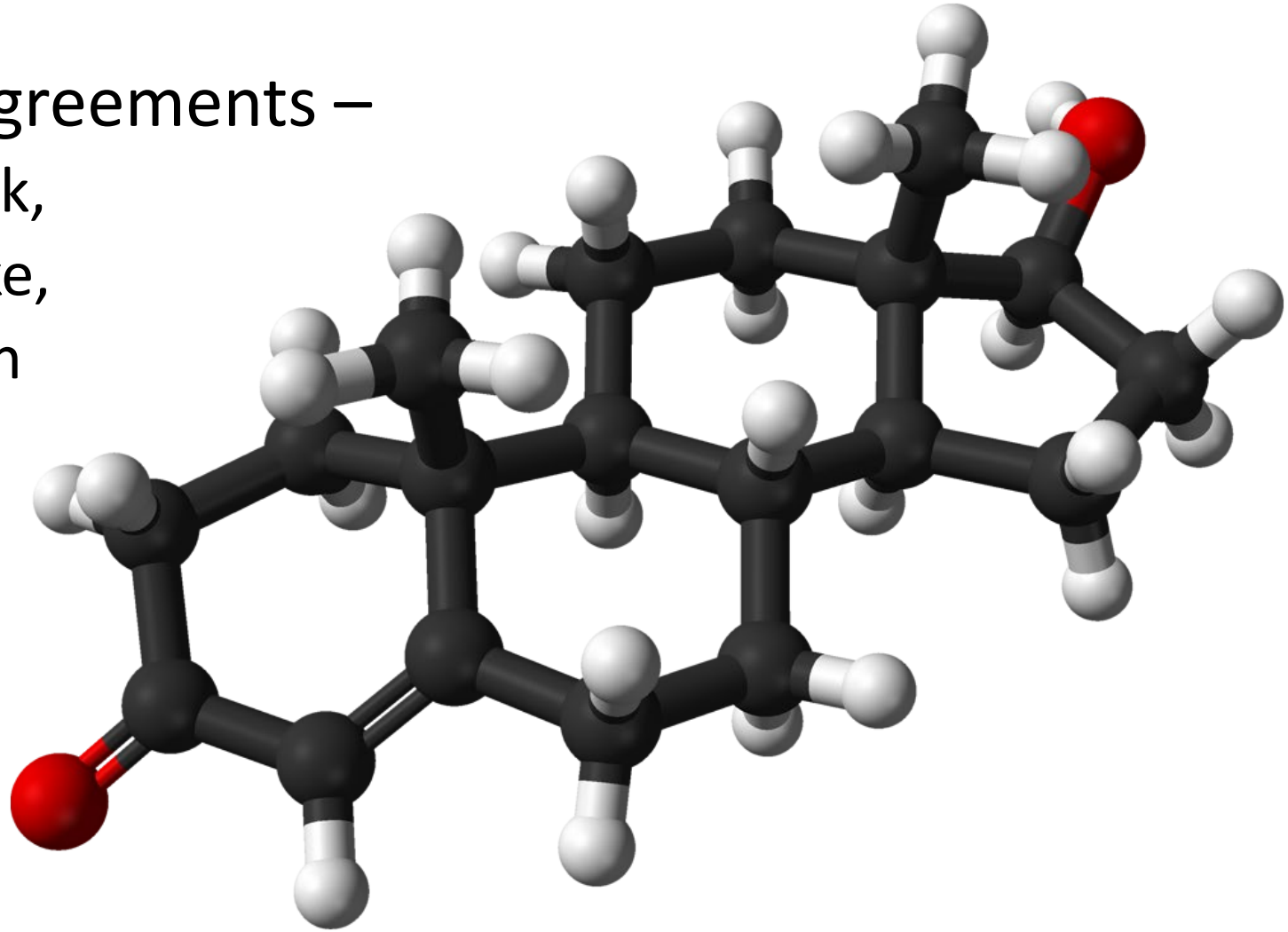
Spring

Negroes sold in 1848

June 25th	Mary	" "	591
may 9th	Emily	" "	300
may 1st	Maria & child John	"	880
may 1st	Robert	"	000
may 1st	Rachel & her child	"	775
may 1st	James	"	000
may 25th	Amanda	" "	415
may 17th	Charlott	" "	460
may 2nd	Margret	" "	450
Amt brought over			29.475 00
			$ 33.266 00
Cost & Expenses			29.653 00
neat money			$ 3.613 00
Harriett	money recovered by Law		480 00
	neat money on the Trip		$ 4.093 00

Consensus

- Methods of agreements –
  - proof of work,
  - proof of stake,
  - authorization

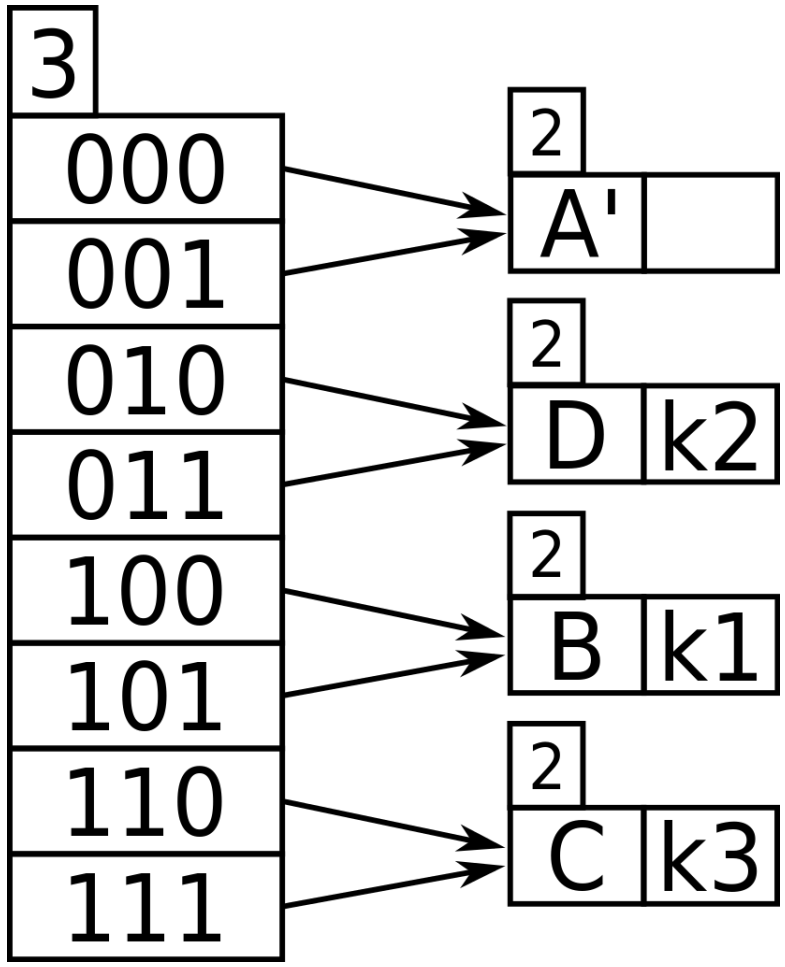


Distributed

- One ledger with many owners vs:
  - One big ledger owned by someone
  - Many individual & separate ledgers

Permanent

- Write-only, verification ensured by hashing



Public vs Private Blockchains

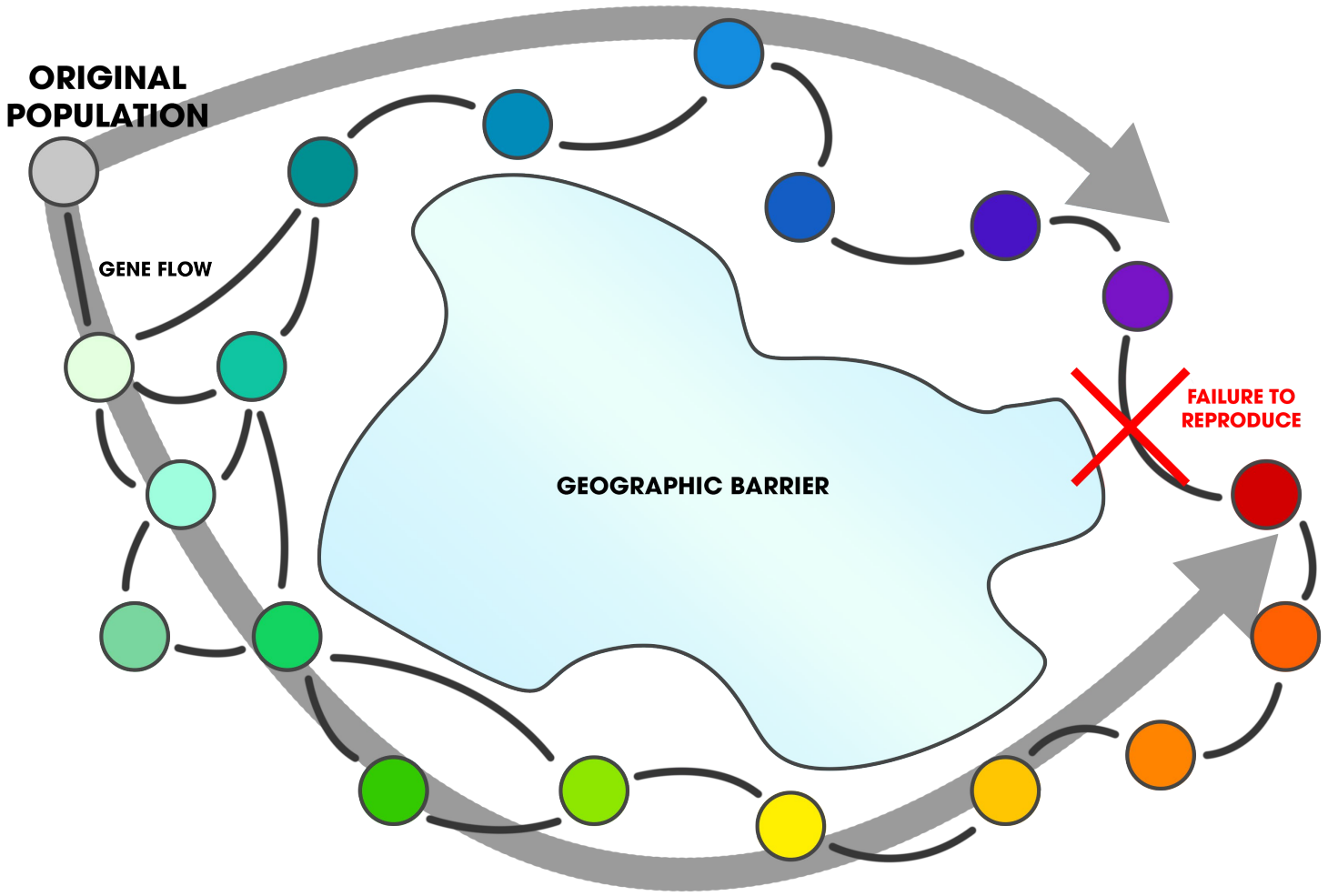
- Public
  - For example: Bitcoin
  - Transactions are viewable by anyone
  - Participant identity is more difficult to control
- Private
  - For example: Hyperledger Fabric
  - Network members are known but transactions are secret
- Permissioned
  - anyone to join the permissioned network after verification of identity
  - allocation of select and designated permissions to perform only certain activities on the network.

Requirements for Life Sciences Blockchains

- Identity / Authentication – know who is contributing, track information to source
- Permission-based – not just anyone contributes, different participants have different rights
- Consensus – based on authorization, not proof of work
- Privacy – records are encrypted, cannot be accessed without authorization and key

Issues

- Data-entry overhead
- Betamax vs VHS
- Digital overhead – processing and data requirements
- Privacy and security



The Future

- Public encrypted write-only records are mainstream
- We will all have digital signatures / keys
- Automation of data entry / internet of things
- Multiple interconnected blockchains / interoperability

Bitcoin Address

SHARE

1A5GqrNbpo7xwpt1VQVvcA5yzoEcgaFvff

Private Key

SECRET

KxSRZnttMtVhe17SX5FhPqWpKAEgMT9T3R6Eferj3sx5frM6obqA

https://commons.wikimedia.org/wiki/File:A_paper_printable_Bitcoin_wallet_consisting_of_one_bitcoin_address_for_receiving_and_the_corresponding_private_key_for_spending.png

Stephen Downes
National Research Council Canada
http://www.downes.ca