Demystifying Blockchain & Digital Tokens: A Primer

Presentation by: **Prof. R.A. Farrokhnia**
Columbia Business & Engineering Schools
Advanced Projects & Applied Research in Fintech

Welcome & Agenda

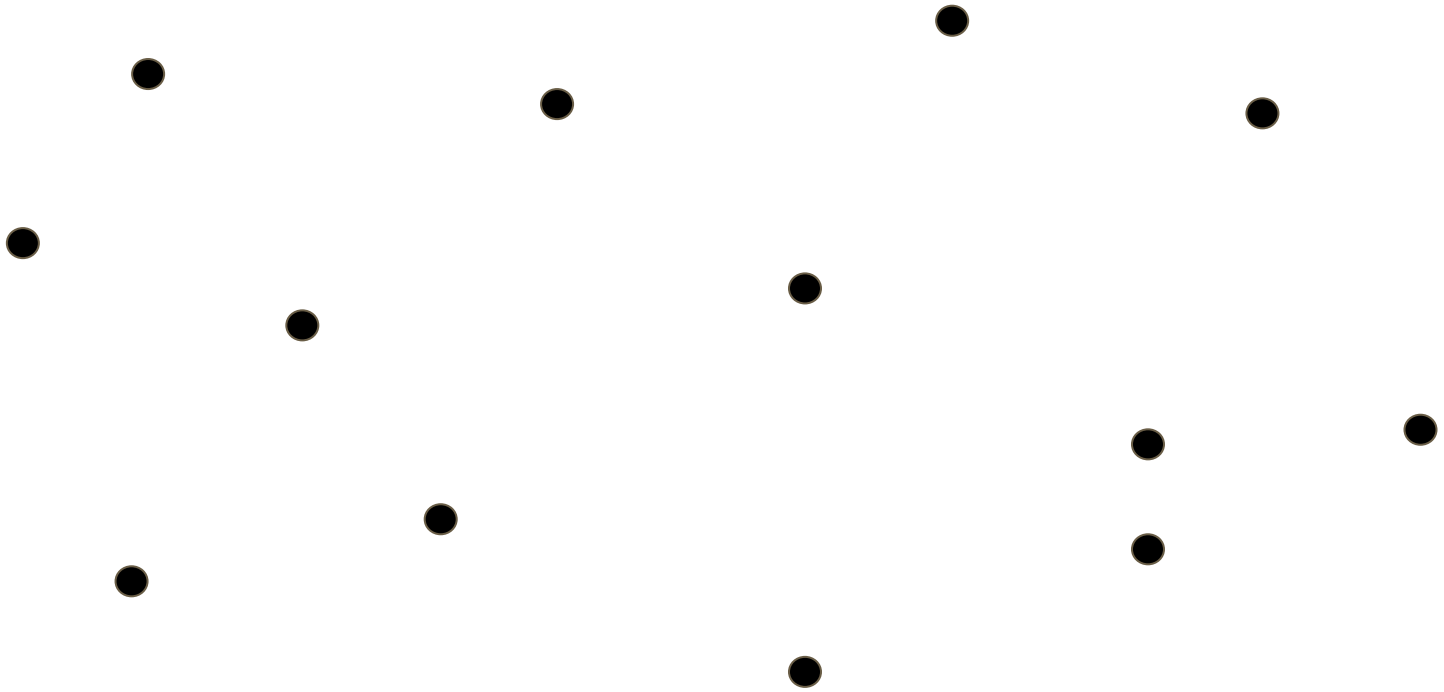
Before we begin …
DISCLAIMERS & PROTOCOLS

I. Networks

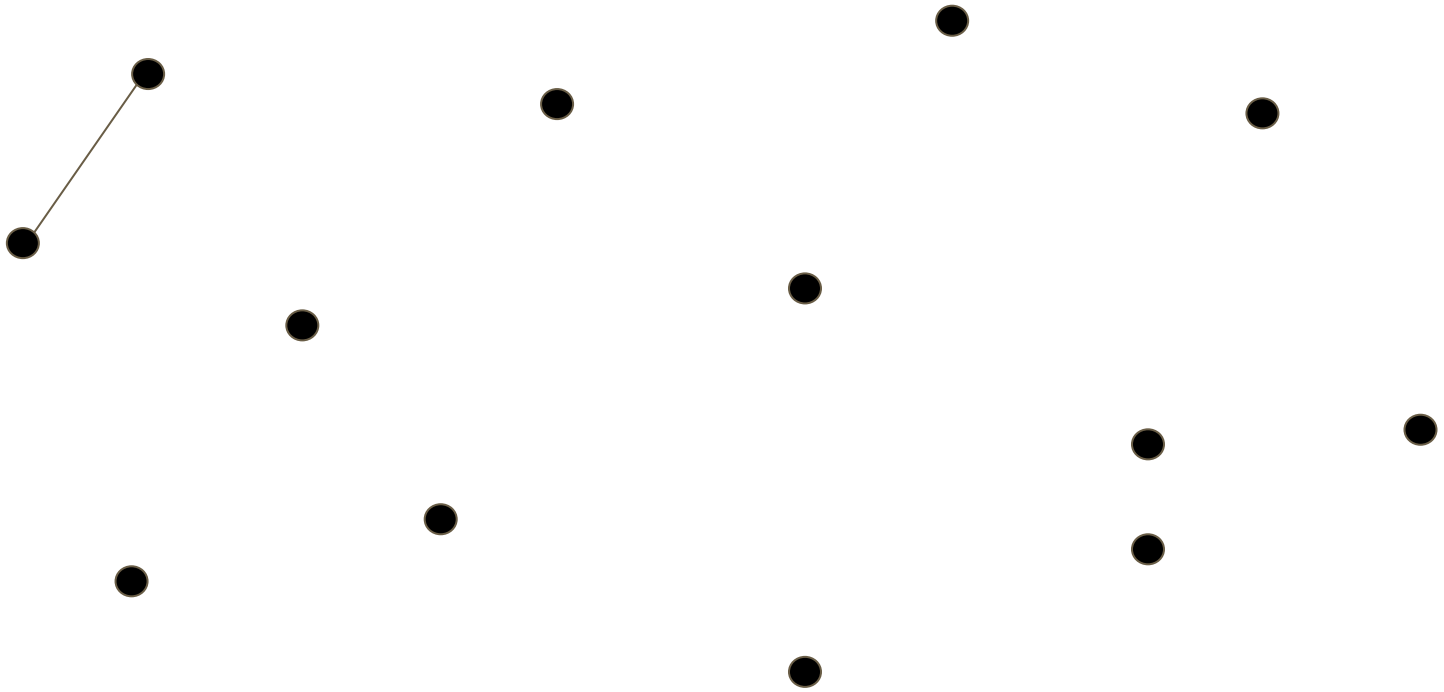
How does the internet work?
Why do we need to protect it?

A few words on networks … in the context of order, complexity, and resiliency

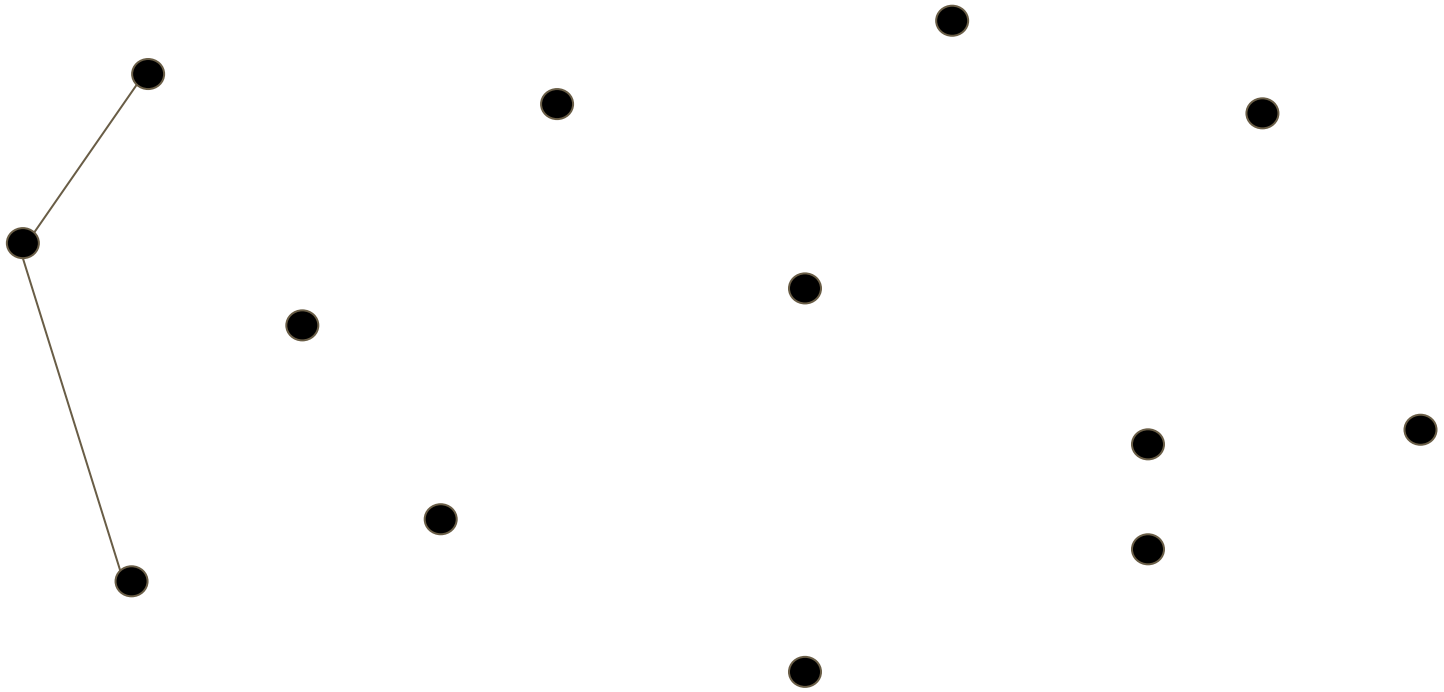
Networks: a collection of connected nodes



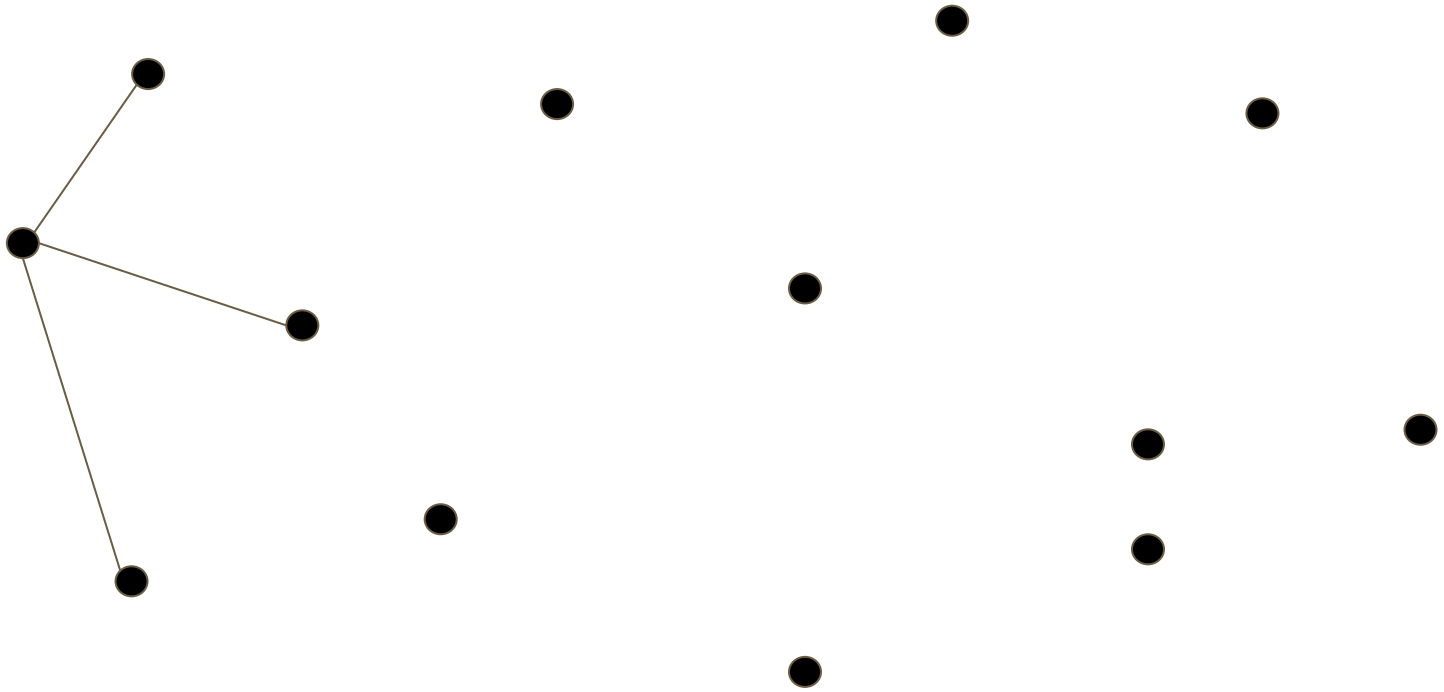
Networks: a collection of connected nodes



Networks: a collection of connected nodes

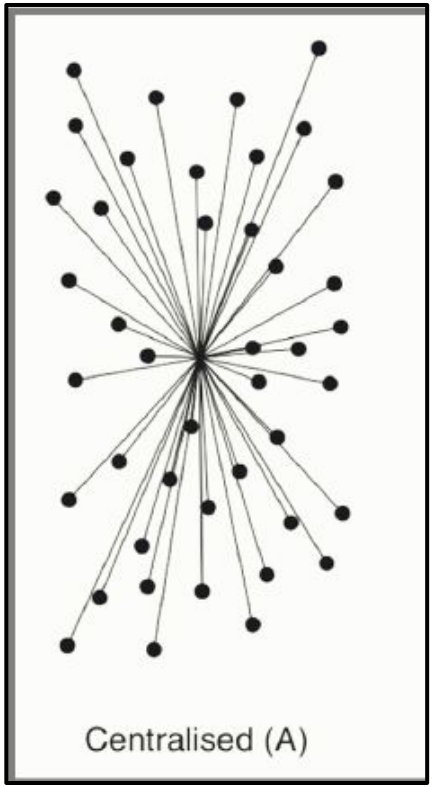


Networks: a collection of connected nodes

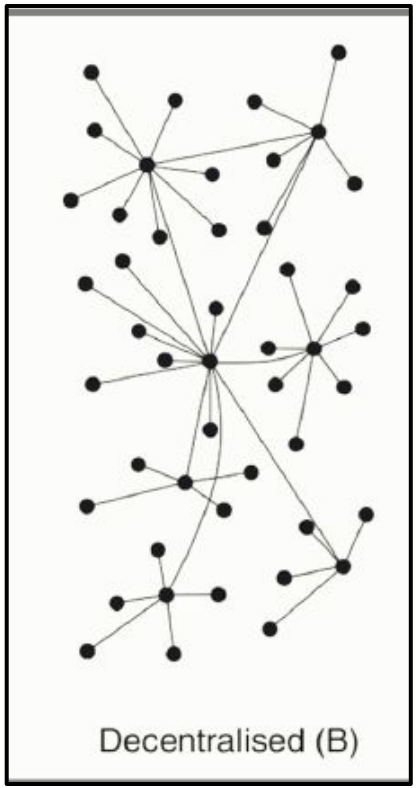


Centralized (vs. Decentralized vs. Distributed)

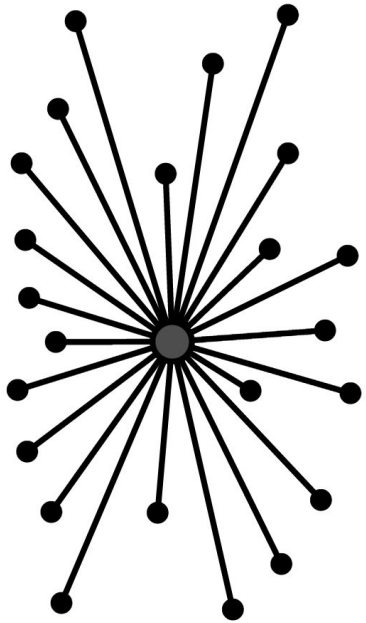
Centralized (vs. Decentralized vs. Distributed)



Centralized vs. Decentralized (vs. Distributed)

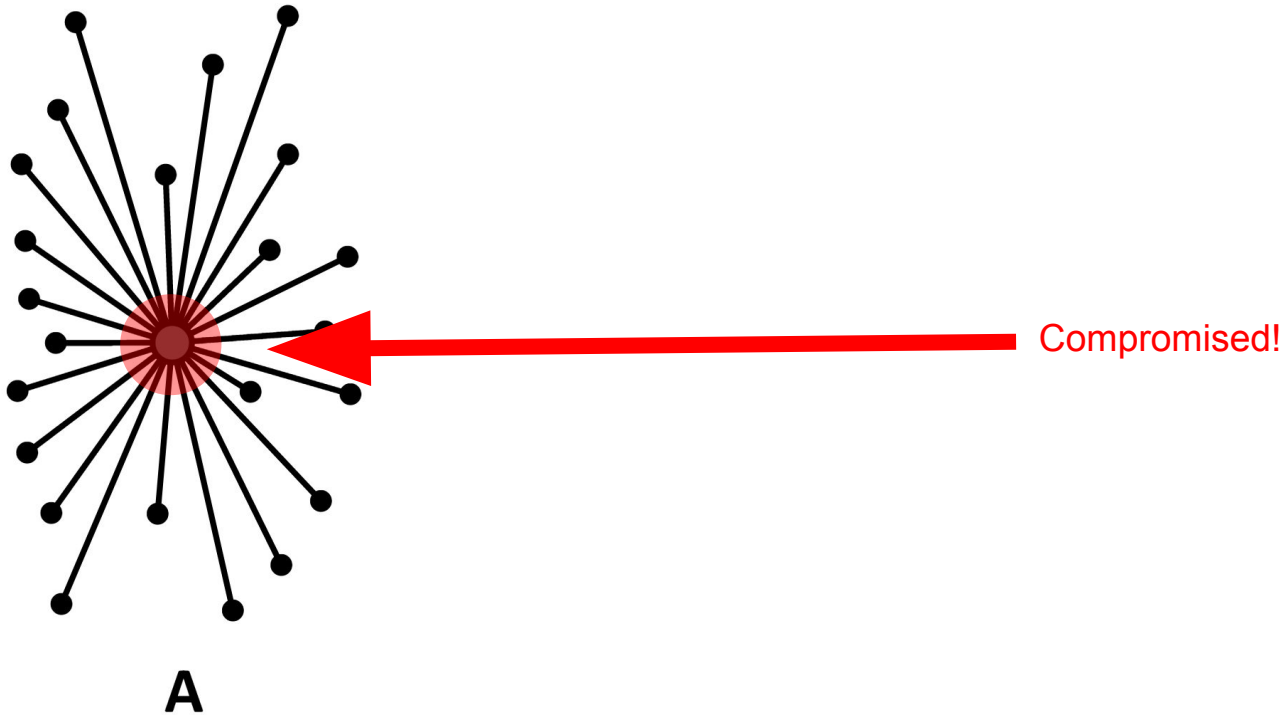


Centralized vs. Decentralized

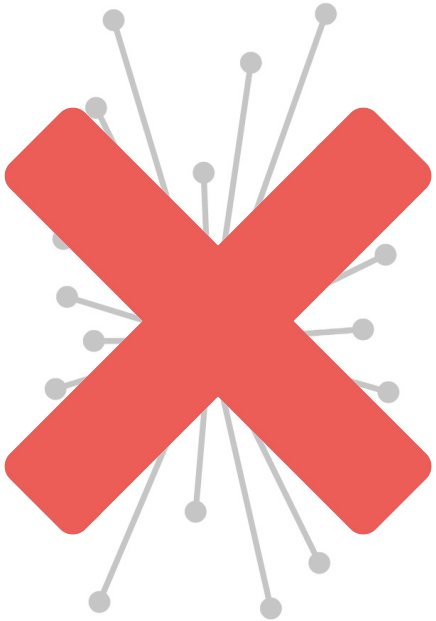


A

What if the central node is compromised?

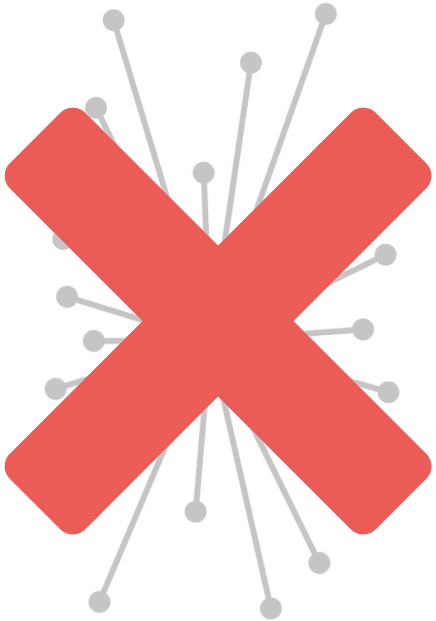


What Can We Do?



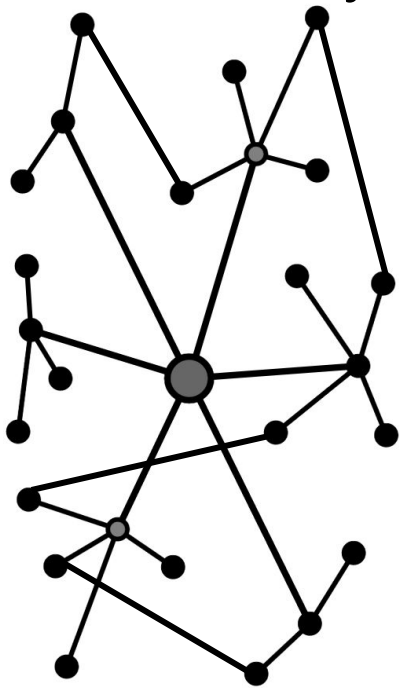
A

What Can We Do?



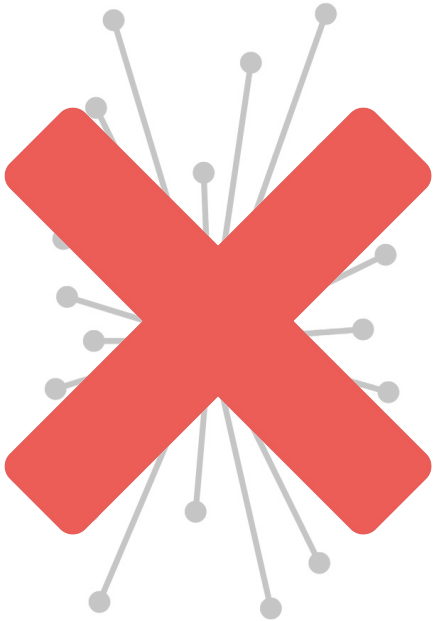
A

Decentralized System



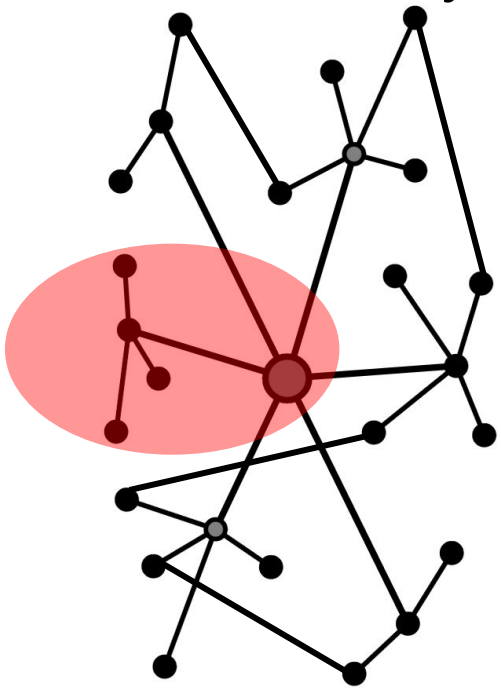
B

What Can We Do?



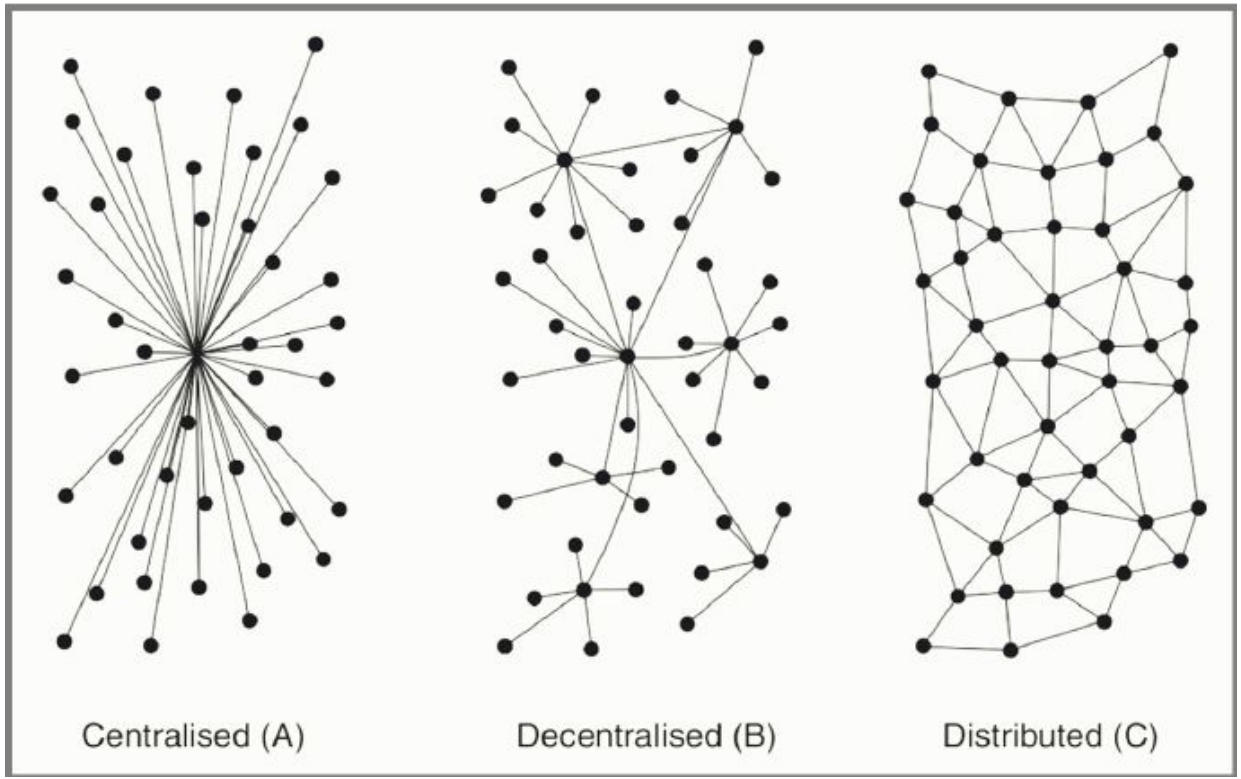
A

Decentralized System



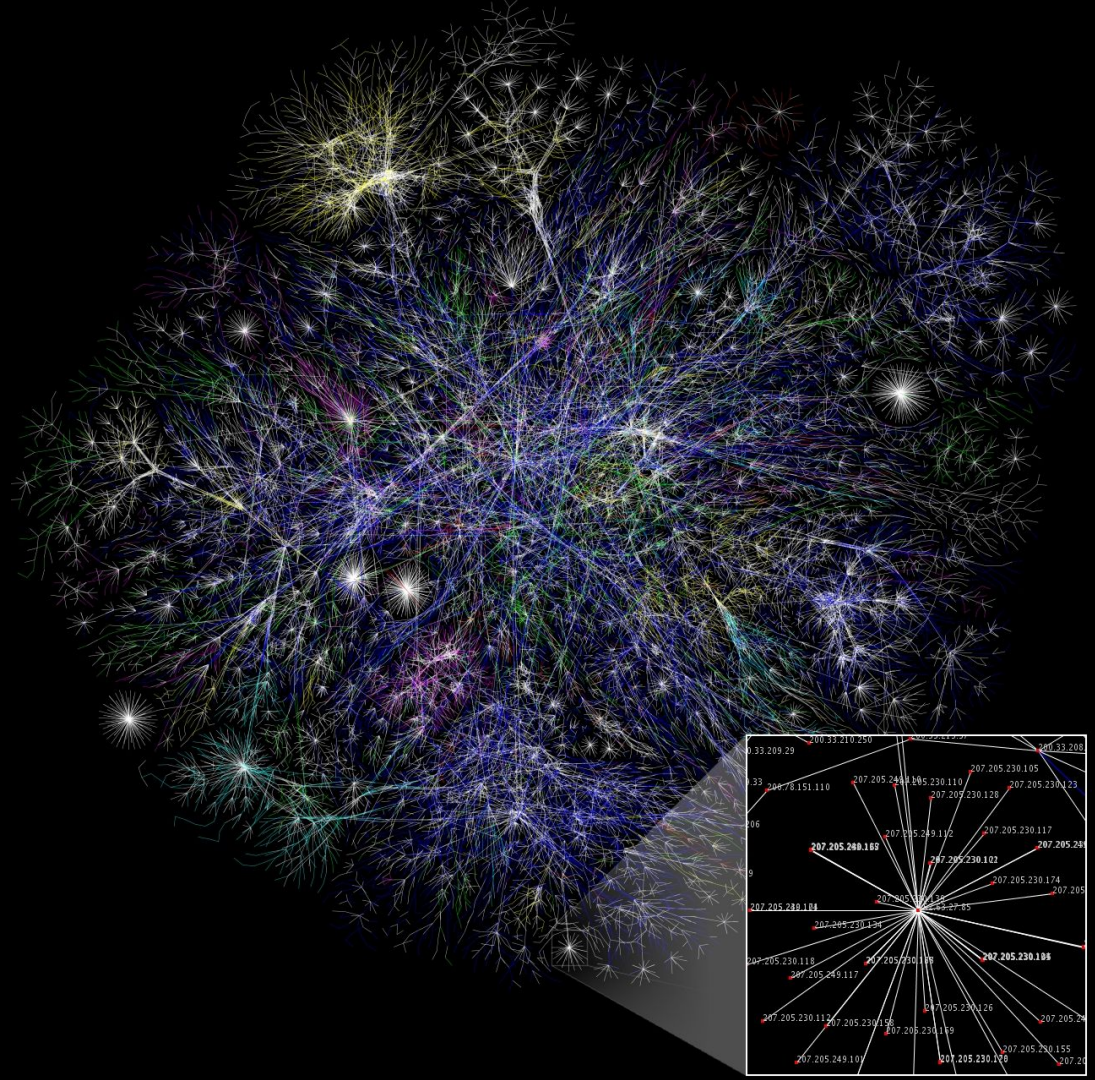
B

Centralized vs. Decentralized vs. Distributed



Real Decentralized Technologies

Internet


207.205.230.105
207.205.230.110
207.205.230.123
207.205.230.128
207.205.230.117
207.205.230.102
207.205.230.174
207.205.230.105
207.205.230.118
207.205.230.126
207.205.230.155
207.205.230.120

Real Decentralized Technologies

Internet

Bitcoin

Another ingredient we need to run networks: PROTOCOLS

A few words on Protocols

- TCP/IP
- SMTP
- IMAP
- POP
- FTP
- HTTP
- HTTPS/TLS
- UDP
- WLAN
- DNS .... and many more!

All Communication needs protocols!

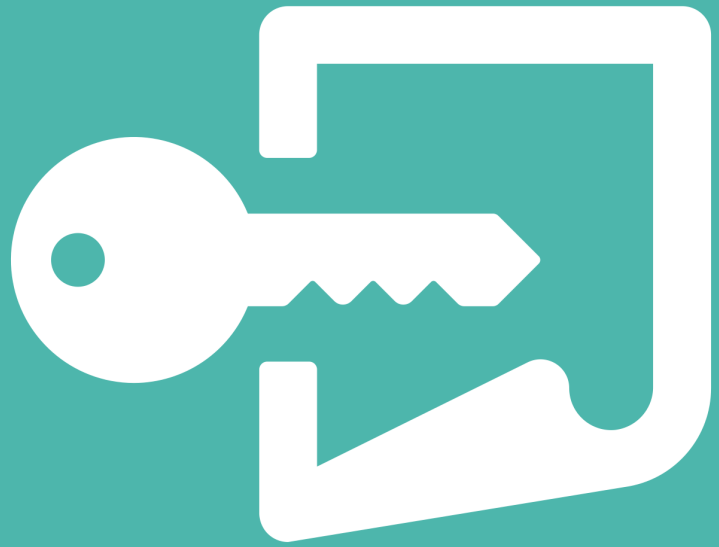
All Communication needs protocols!

All Communication needs protocols!

All Communication needs protocols!

0. Please Don’t Tell

A brief primer on the codes and ciphers used throughout history to protect information.



Plaintext vs. Ciphertext

Plaintext	`I love the sun`
Ciphertext	`w jd7h bmg vns`

Cipher Shift (or substitution), aka Caesar Cipher

Plaintext	`I love the sun`
Ciphertext	`? ???? ??? ???`

Cipher Shift (zero or no shift)

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	N	C	P	Q	R	S	T	U	V	W	X	Y	Z

Cipher Shift (zero or no shift)

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	N	C	P	Q	R	S	T	U	V	W	X	Y	Z

Cipher Shift (shift of one)

Plaintext Alphabet			C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	N	C	P	Q	R	S	T	U	V	W	X	Y	Z

Cipher Shift (shift of one)

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	

Cipher Shift (+1)

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Plaintext `i love the sun`

Ciphertext `??????????????`

Cipher Shift (+1)

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

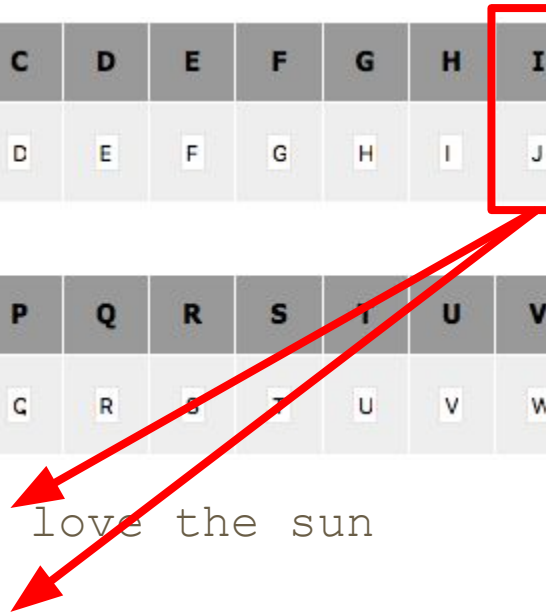
Plaintext `i love the sun`

Ciphertext

Cipher Shift (+1)

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	O	P	Q	R	S	T	U	V	W	X	Y	Z	A



Plaintext `i love the sun`

Ciphertext `j`

Cipher Shift (+1)

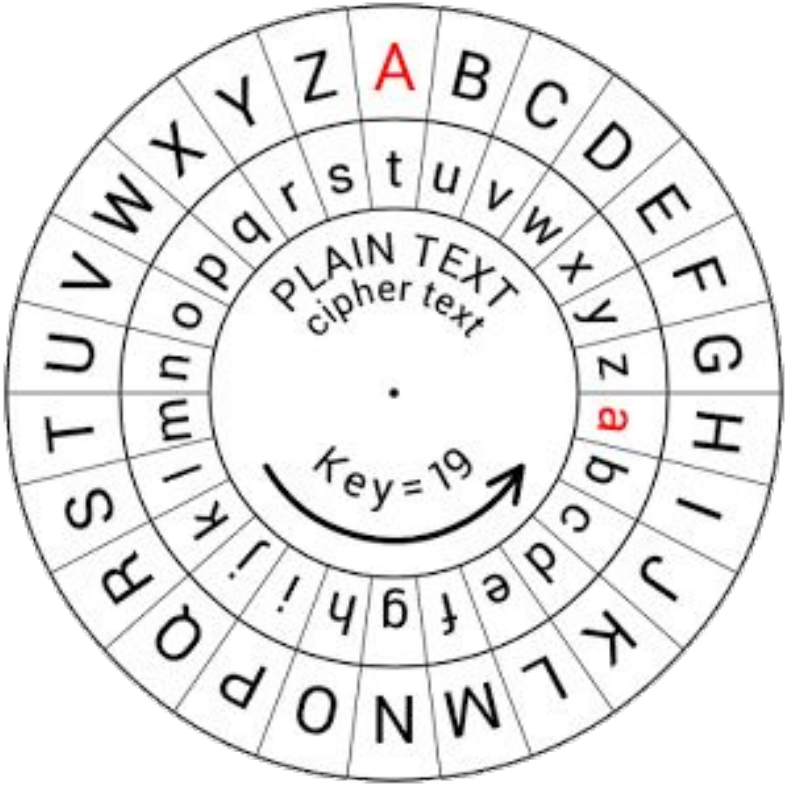
Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N

Plaintext Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext Alphabet	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Plaintext `i love the sun`

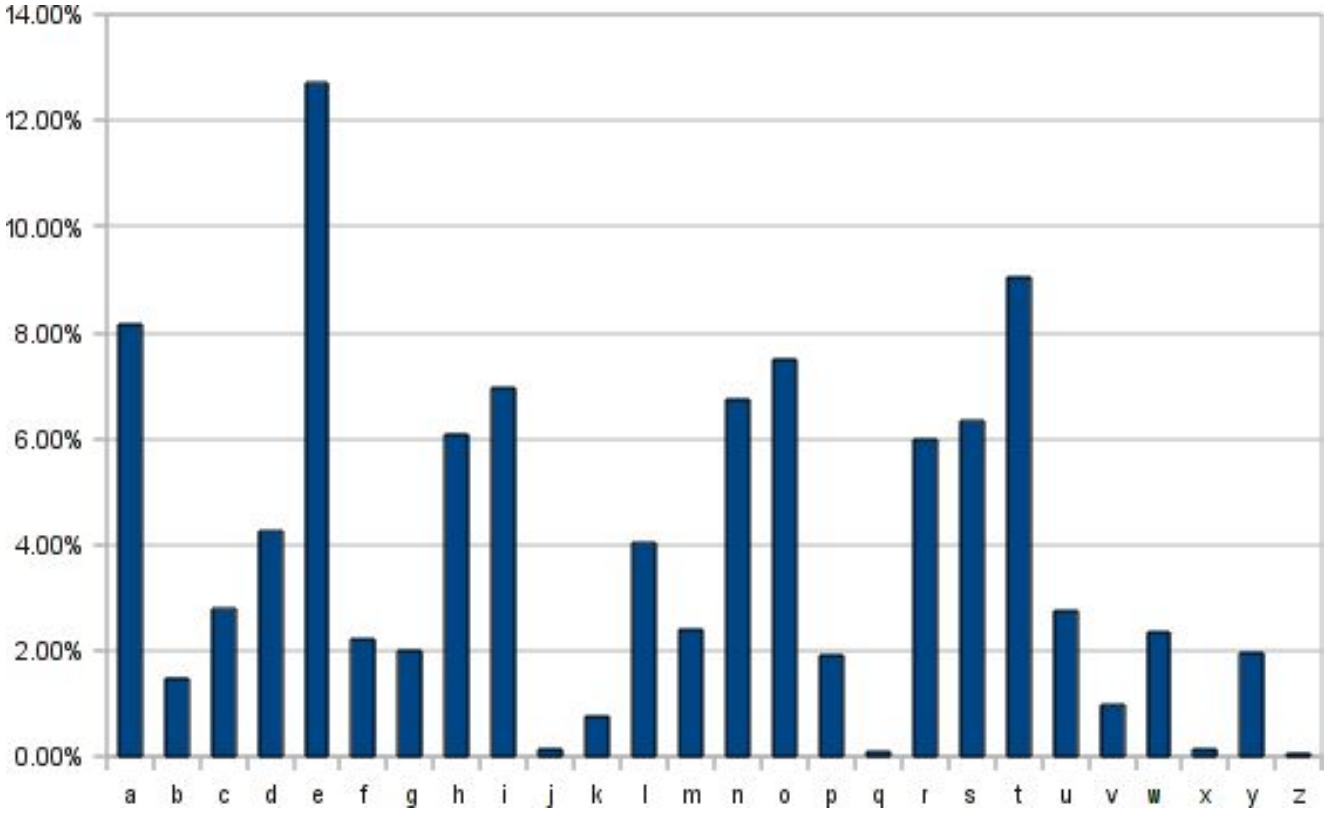
Ciphertext `j mpwf uif tvo`

Cipher Shift Wheel



Cipher Shift Decoded (or rather, decrypted!)

Cipher Shift Decoded (or rather, decrypted!)



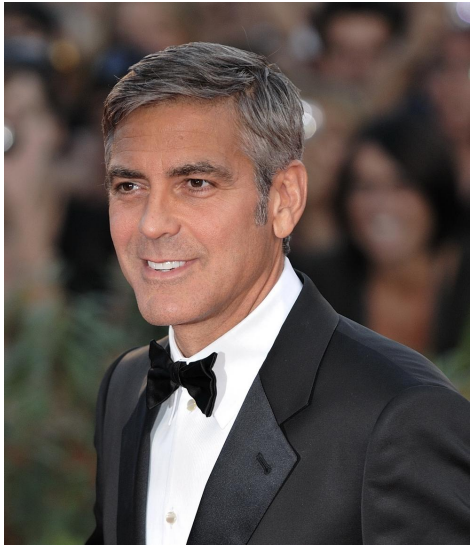
Breaking code (by hand): frequency & other tricks

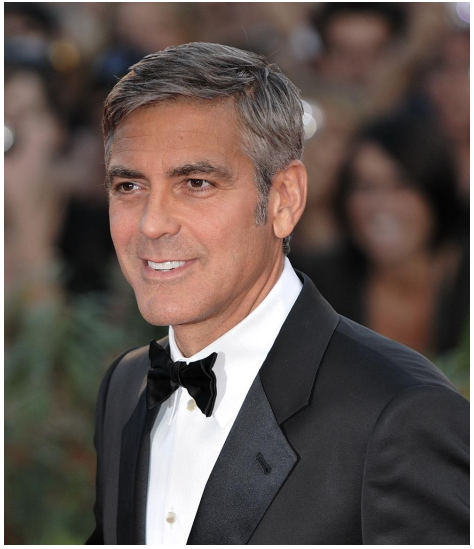
MPQZCP HP NLY ELWV LMZFE ESP DAPNTQTND ZQ XZOPCY NCJAEZRCLASJ, MWZNVNSLTYD, ZC MTENZTY, HP XFDE QTCDE ELWV LMZFE ESP CZWP ZQ XLESPXLETND, FYOPCDELYOTYR SZH TE TD LAAWTPO LYO SZH TE TD QFYOLXPYELW EZ LWW ESLE EPNSYZWZRJ LTXD EZ LNSTPGP.

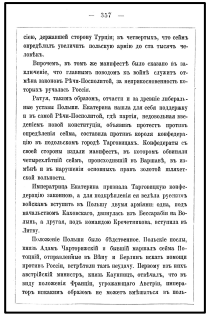
But how to safely and securely transmit the cipher-shift "key"?

A clever thought-experiment to transmit key, esp to those you haven't met before!

How it works?







— 557 —

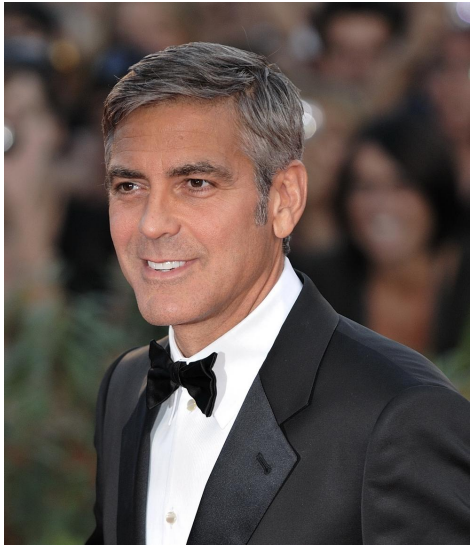
сан, державшей сторону Турции; въ четвертыхъ, что себѣ опредѣлили увеличить польскую армію до ста тысячъ человѣкъ.

Впрочемъ, въ томъ же манифестѣ было сказано объ заключеніи, что главнымъ поводомъ къ войнѣ служитъ отказъ полковъ Рѣчи-Посполитой, за неприкосновенность которыхъ ручалась Россія.

Ропотъ, такимъ образомъ, отчасти и въ древнемъ либеральномъ устоѣ Польши. Екатерина нашла для себя поддержку и въ самой Рѣчи-Посполитой, гдѣ партія, недовольная нѣдавнимъ новой конституціи, объявила протестъ противъ опредѣленія себя, составила противъ короля конфедерацію изъ подольскихъ городъ Тарговицкихъ. Конфедераты съ своей стороны издали манифестъ, въ которомъ обвиняли четырехлѣтній сеймъ, происходившій въ Варшавѣ, въ измѣнѣ и въ нарушеніи основныхъ правъ золотой шляхетской вольности.

Императрица Екатерина признала Тарговицкую конфедерацію законною, а для подкрѣпленія ея послала русскихъ войскъ вступить въ Польшу двумя арміями: одна, подъ начальствомъ Каховскаго, двинулась изъ Бессарабіи въ Волынь, а другая, подъ командою Кречетникова, вступила въ Литву.

Положеніе Польши было обдуманное. Польскіе послы, князь Адамъ Чарторыйскій и бывшій маршалъ сейма Потоцкій, отправленные въ Вѣну и Берлинъ искать помощи противъ Россіи, встрѣтили тамъ неудачу. Первому изъ нихъ австрійскій министръ, князь Кауницъ, отвѣчалъ, что въ виду положенія Франціи, угрожающаго Австріи, императоръ никакихъ обѣщаній не можетъ поѣшиться въ поль-



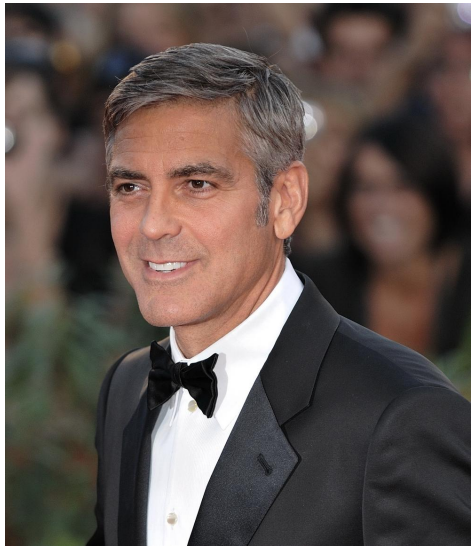
сан, державшей сторону Турціи; въ четвертыхъ, что себѣ опредѣлили увеличить польскую армію до ста тысячъ человѣкъ.

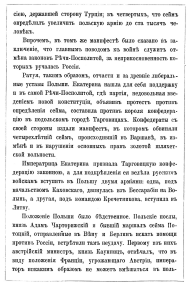
Впрочемъ, въ томъ же манифестѣ было сказано объ заключеніи, что главнымъ поводомъ къ войнѣ служитъ оставленіе покойною Рѣчью-Посполитой, за неприкосновенность которой ручалась Россія.

Ратуя, такимъ образомъ, отчасти и за древніе либеральные устои Польши, Екатерина пошла для себя поддержку и въ самой Рѣчи-Посполитой, гдѣ партія, недовольная послѣдними новой конституціи, объявила протестъ противъ опредѣленія себя, составила противъ короля конфедерацію изъ подольскихъ городовъ Тарговицкихъ. Конфедераты съ своей стороны издали манифестъ, въ которомъ обвиняли четырехлѣтній сеймъ, происходившій въ Варшавѣ, въ измѣнѣ и въ нарушеніи основныхъ правъ золотой шляхетской вольности.

Императрица Екатерина признала Тарговицкую конфедерацію законною, а для подкрѣпленія ея послала русскихъ войскахъ вступить въ Польшу двумя арміями: одна, подъ начальствомъ Каховскаго, двинулась изъ Бессарабіи на Волынь, а другая, подъ командою Кречетникова, вступила изъ Литвы.

Положеніе Польши было обдуманное. Польскіе послы, князь Адамъ Чарторыйскій и бывшій маршалъ сейма Потоцкій, отправленные въ Вѣну и Берлинъ искать помощи противъ Россіи, встрѣтили тамъ неудачу. Первому изъ нихъ австрійскій министръ, князь Кауницъ, отвѣчалъ, что въ виду положенія Франціи, угрожающаго Австріи, императоръ никакихъ обѣщаній не можетъ поѣшиться въ поль-





— 557 —

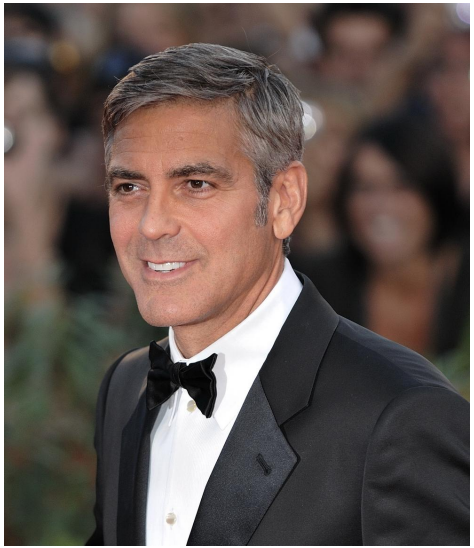
сан, державшей сторону Турции; въ четвертыхъ, что собиралась удвоить увеличить польскую армію до ста тысячъ человѣкъ.

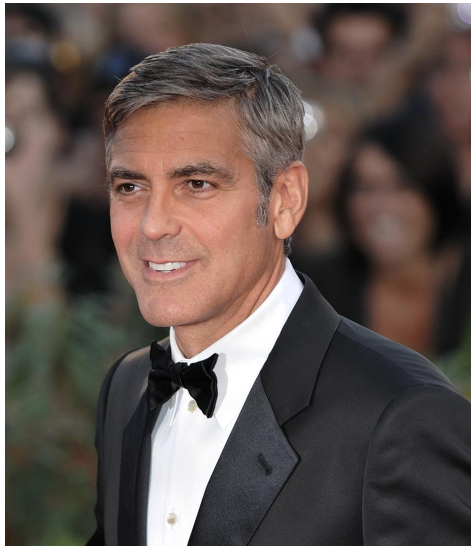
Вирочемъ, въ томъ же манифестѣ было сказано объ заключеніи, что главнымъ поводомъ къ войнѣ служитъ оставленіе покойною Рѣчью-Посполитой, за неприсоединенность которой ратовала Россія.

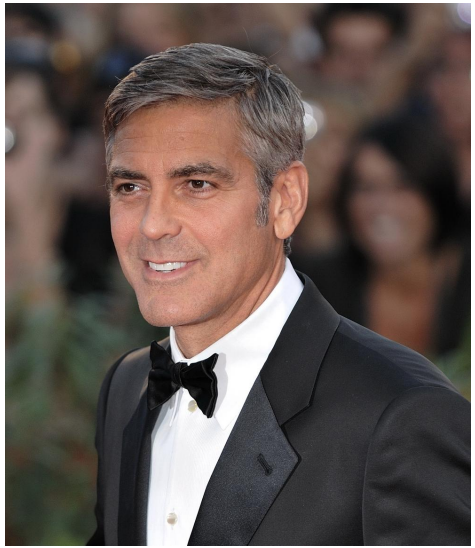
Ратуя, такимъ образомъ, отчасти и за древніе либеральные устои Польши, Екатерина искала для себя поддержку и въ самой Рѣчи-Посполитой, гдѣ партія, недовольная послѣднею новой конституціей, объявила протестъ противъ опредѣленія себя, составила противъ короля конфедерацію изъ подольскихъ городъ Тарговицкихъ. Конфедераты съ своей стороны издали манифестъ, въ которомъ обвиняли четырехлѣтній сеймъ, происходившій въ Варшавѣ, въ измѣнѣ и въ нарушеніи основныхъ правъ золотой шляхетской вольности.

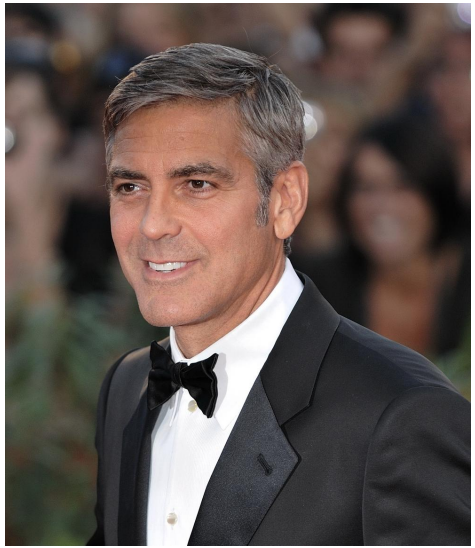
Императрица Екатерина признала Тарговицкую конфедерацію законною, а для подкрѣпленія ея послала русскихъ войскахъ вступить въ Польшу двумя арміями: одна, подъ начальствомъ Каховскаго, двинулась изъ Бессарабіи на Волынь, а другая, подъ командою Кречетникова, вступила въ Литву.

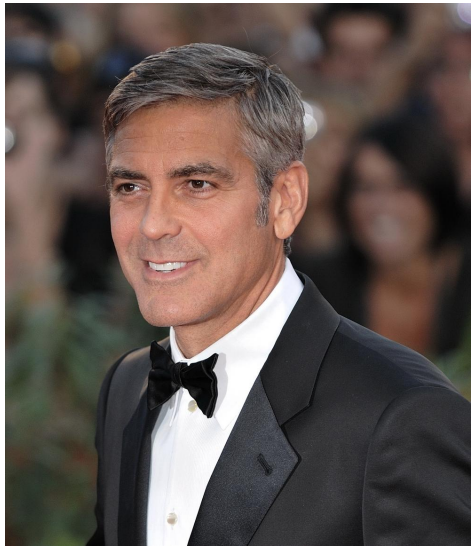
Положеніе Польши было обдуманное. Польскіе послы, князь Адамъ Чарторыйскій и бывшій маршалъ сейма Потоцкій, отправленные въ Вѣну и Берлинъ искать помощи противъ Россіи, встрѣтили тамъ неудачу. Первому изъ нихъ австрійскій министръ, князь Кауницъ, отвѣчалъ, что въ виду положенія Франціи, угрожающаго Австріи, императоръ никакихъ обязанностей не можетъ имѣть къ поль-

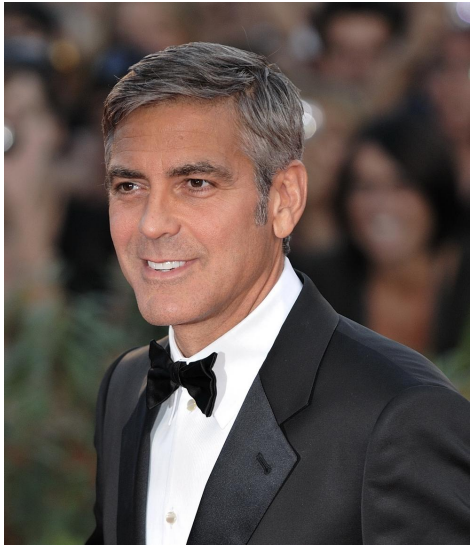


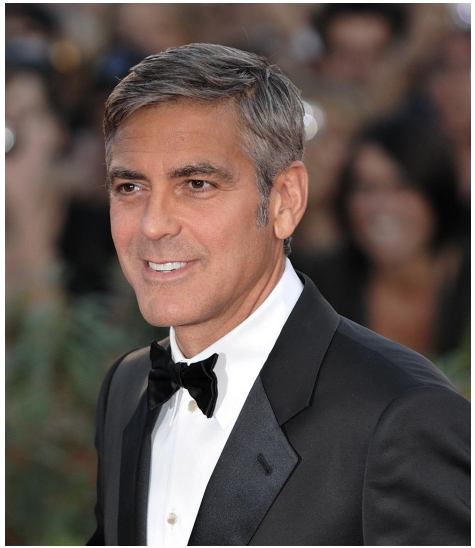


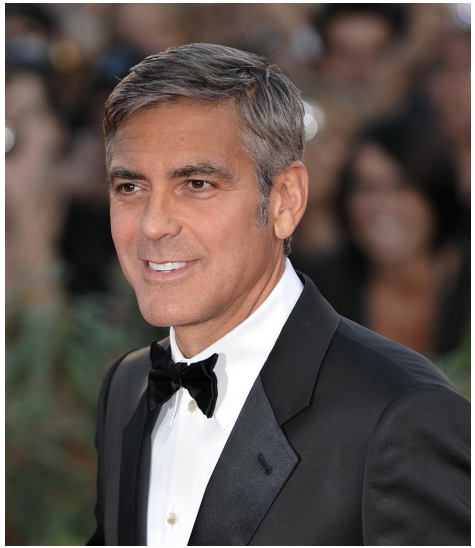


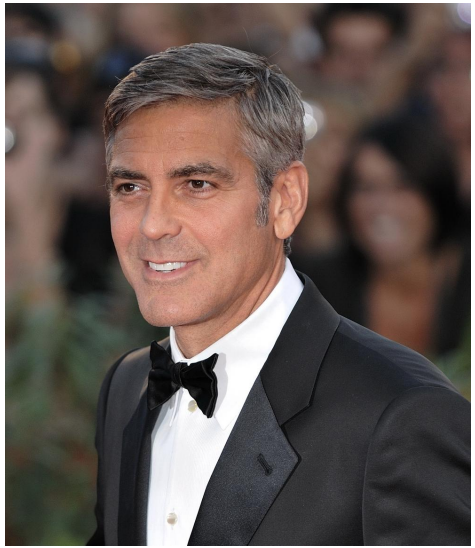


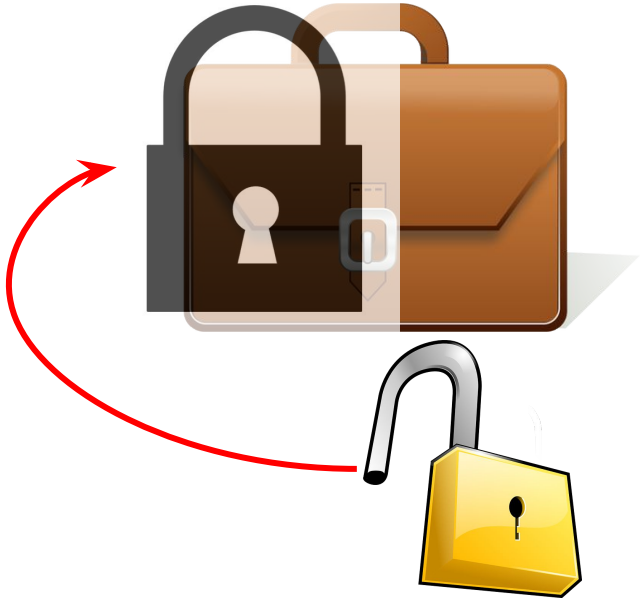


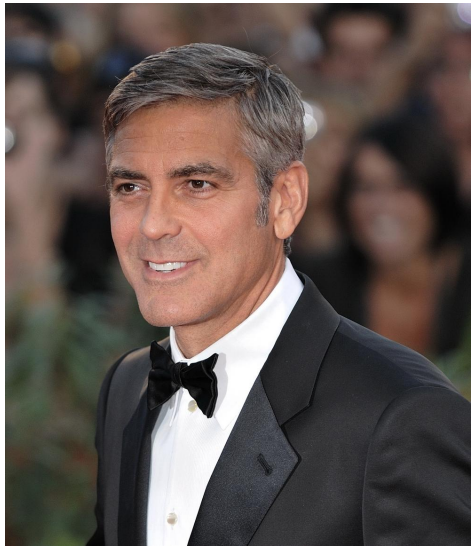


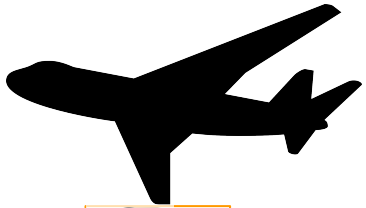


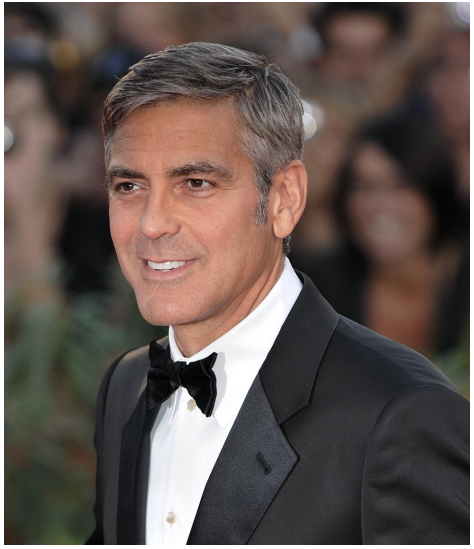


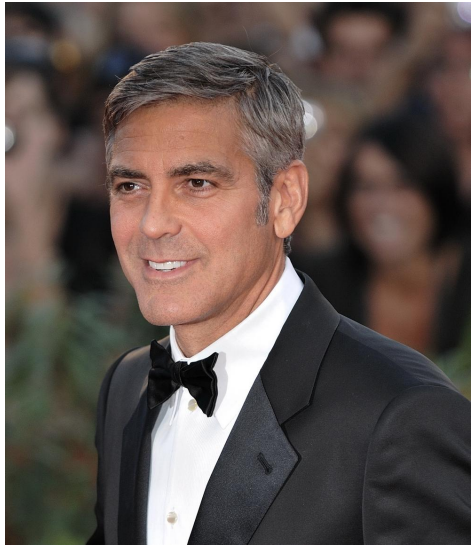


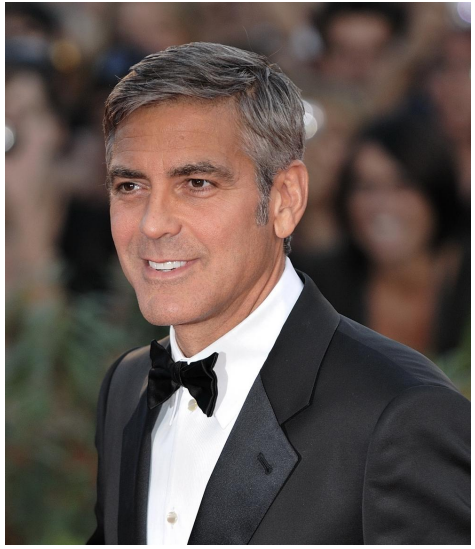


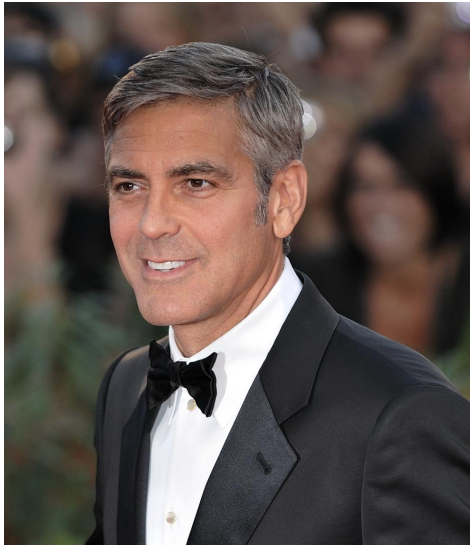


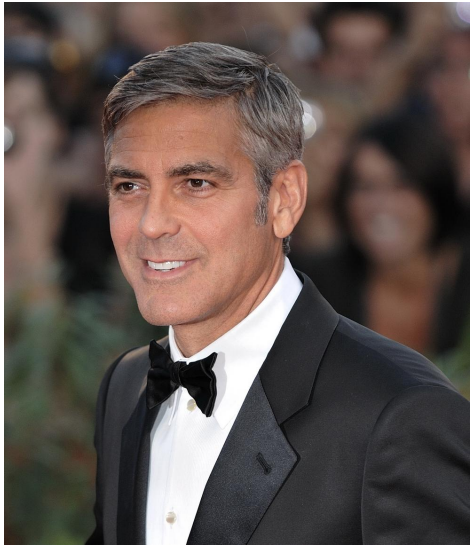


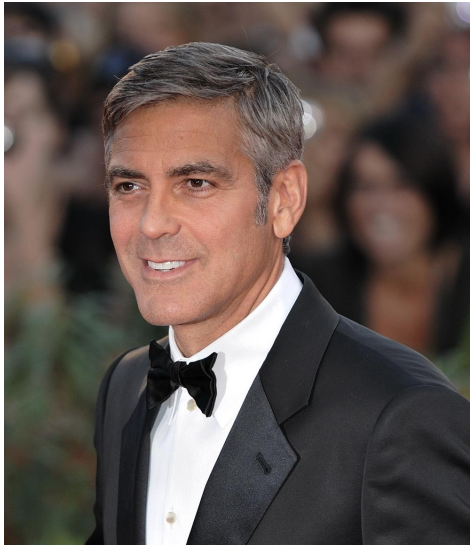


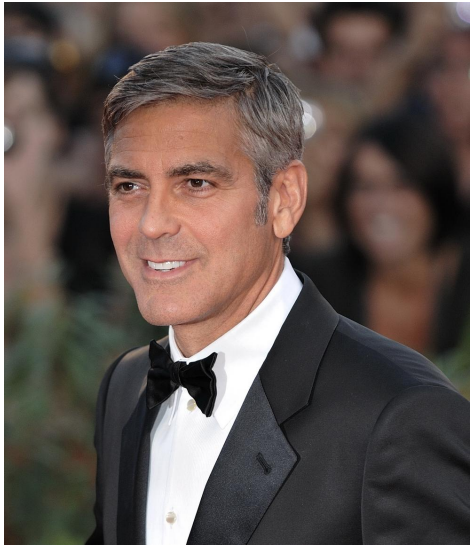


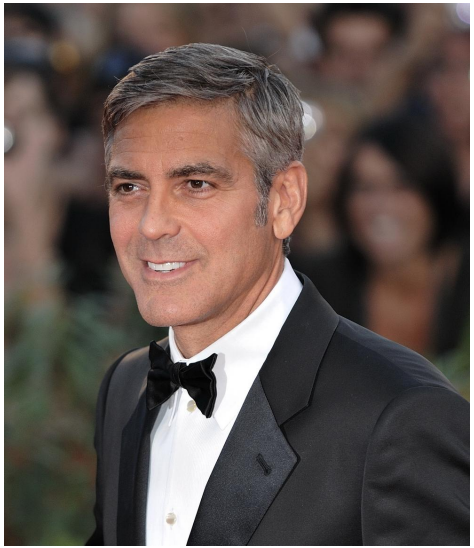


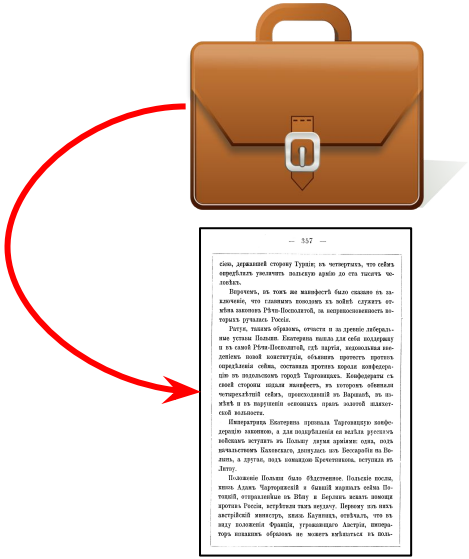






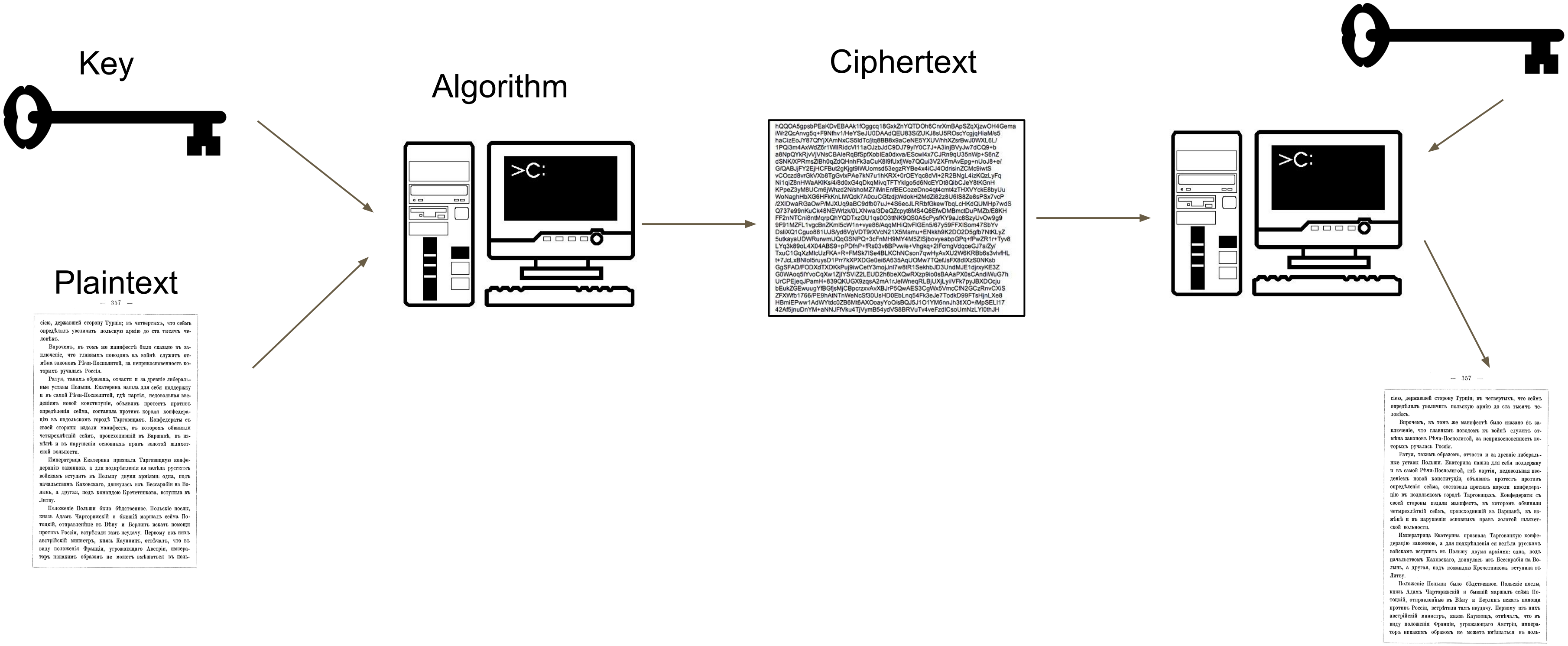





— 357 —
сію, державшей сторону Турціи; онъ четвертилъ, что себѣ опредѣлилъ увеличить польскую армію до ста тысячъ человѣкъ.
Впрочемъ, въ томъ же манифестѣ было сказано въ заключеніе, что главнымъ походомъ къ войнѣ служитъ отмѣна законовъ Рѣчи-Посполитой, за непринадлежность которыхъ ручалась Россія.
Ратуя, такимъ образомъ, отчасти и за древніе либеральные устои Польши, Екатерина тѣмъ самымъ подкапывалась и къ самой Рѣчи-Посполитой, гдѣ партія, недовольная внутреннимъ новой конституціи, объявила протестъ противъ опредѣленій сейма, составила противъ короля конфедерацію въ подольскомъ городѣ Тарговицахъ. Конфедераты съ своей стороны издали манифестъ, въ которомъ обвиняли четырехлѣтній сеймъ, происходящій въ Варшавѣ, въ измѣнѣ и въ нарушеніи основныхъ правъ золотой шляхетской вольности.
Императрица Екатерина признала Тарговицкую конфедерацію законною, а для подкрѣпленія ея велѣла русскимъ войскамъ вступить въ Польшу двумя арміями: одна, подъ начальствомъ Каховскаго, двинулась изъ Бессарабіи на Волынь, а другая, подъ командою Кречетникова, вступила въ Литву.
Положеніе Польши было обдуманное. Польскіе послы, князь Адамъ Чарторижскій и бывшій маршалъ сейма Потоцкій, отправленные въ Вѣну и Берлинъ искать помощи противъ Россіи, встрѣтили тамъ неудачу. Первому изъ нихъ австрійскій министръ, князь Кауницъ, отвѣчалъ, что въ виду положенія Франціи, угрожающаго Австріи, императоръ никакимъ образомъ не можетъ вмѣшаться въ поль-

Isn’t that cool? We exchanged a secret (encrypted) message without having to agree to and exchange keys beforehand!

Digital Cryptography - Sequence Matters!



One encryption on top of another! Remember LIFO?

A clever way to transmit key, in particular to those you haven't met before!

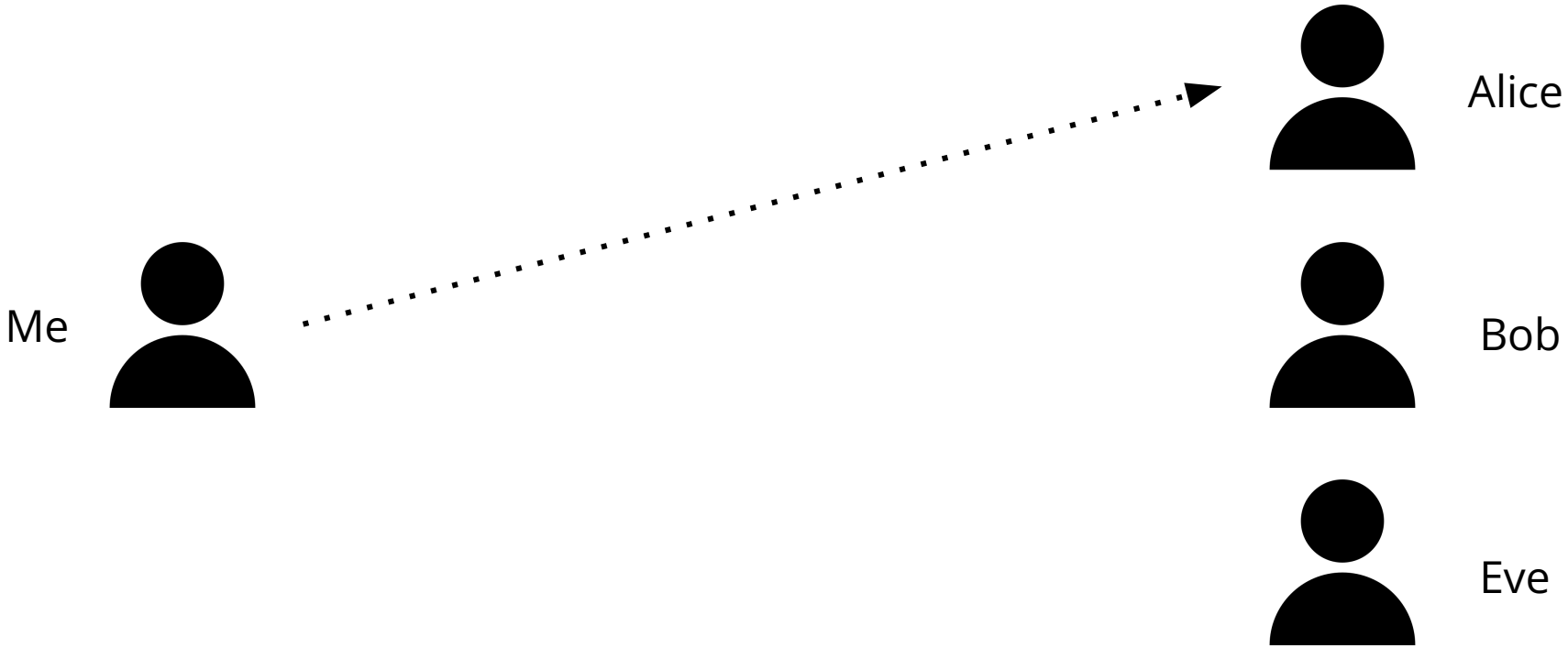
"irreversible" solution = Public + Private Key Pairs

“irreversible” solution = Public + Private Key Pairs

Main Key Pair Attributes:

- Related, but separate (each unique on its own)
- They are unique to each person/user
- When one locks, only the other one can unlock
- Do NOT share private key … ever!

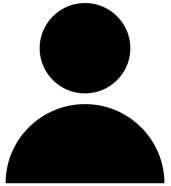
Sending an Encrypted Message with Key Pairs



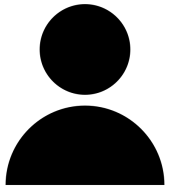
Sending an Encrypted Message with Key Pairs

Sending an Encrypted Message with Key Pairs

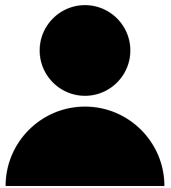
Me



Alice

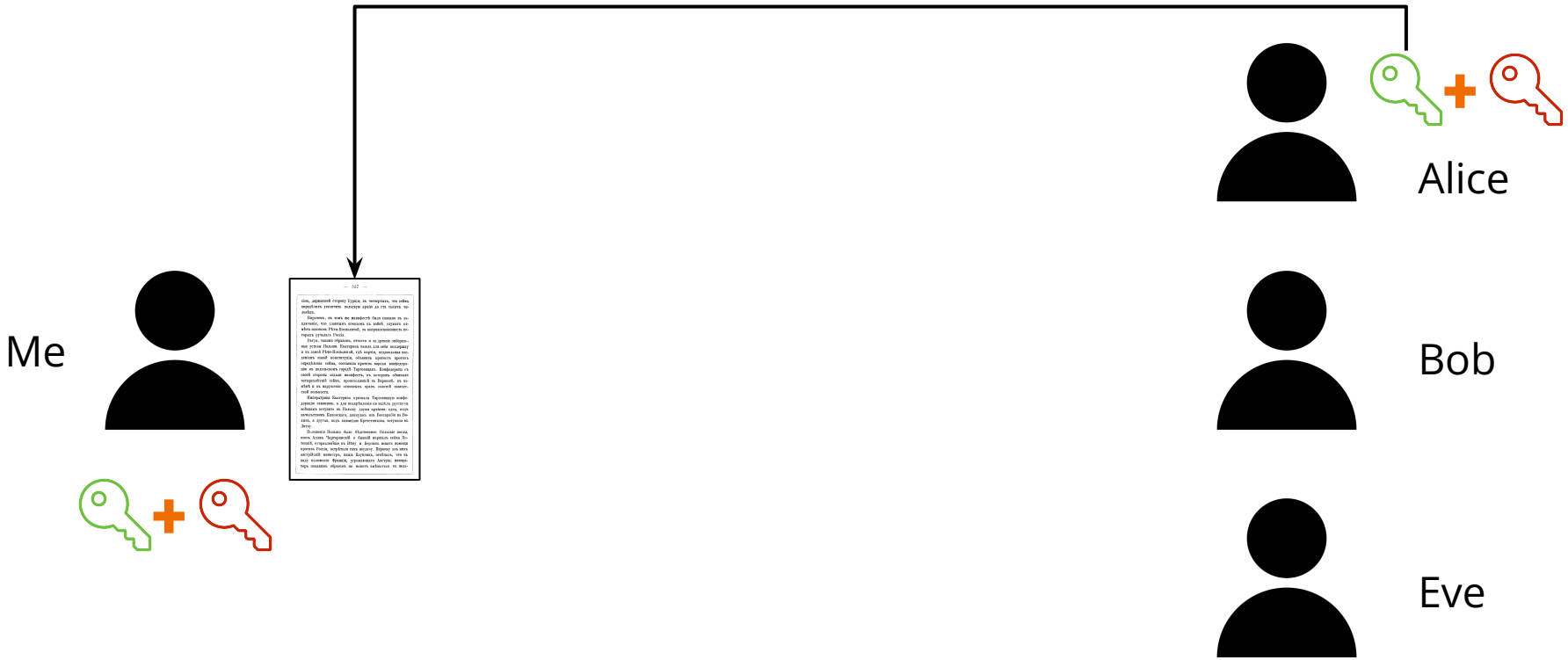


Bob



Eve

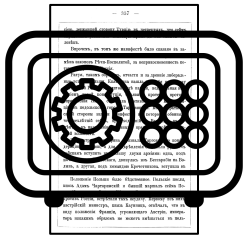
Sending an Encrypted Message with Key Pairs

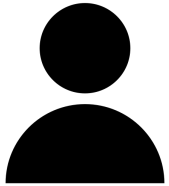


Sending an Encrypted Message with Key Pairs

Sending an Encrypted Message with Key Pairs

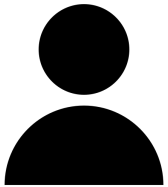
Sending an Encrypted Message with Key Pairs

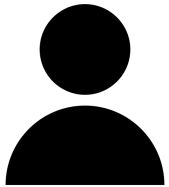




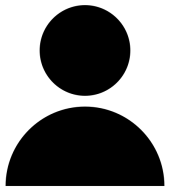
Alice

Me



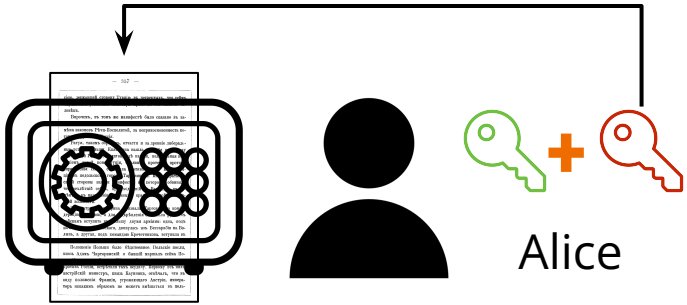


Bob



Eve

Sending an Encrypted Message with Key Pairs



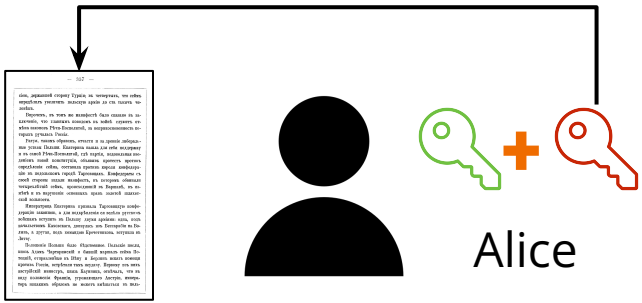
Alice

Bob

Eve

Me

Sending an Encrypted Message with Key Pairs



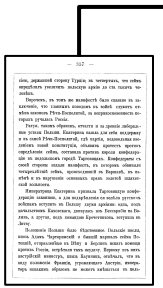
Alice

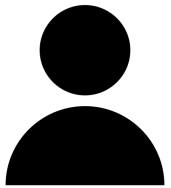
Me

Bob

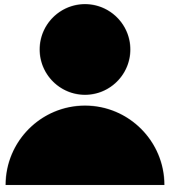
Eve

Sending an Encrypted Message with Key Pairs

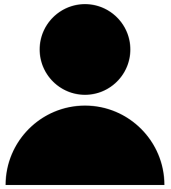




Alice

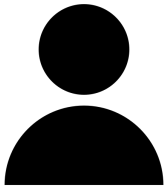


Bob



Eve

Me



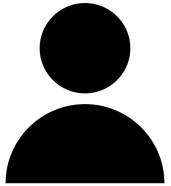
Isn’t that super cool?

But how about the following scenario …

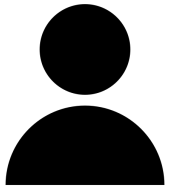
Sending an Encrypted Message with Key Pairs

Sending an Encrypted Message with Key Pairs

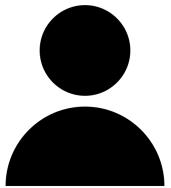
Me



Alice



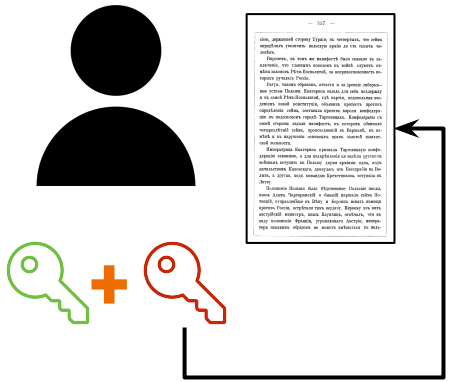
Bob



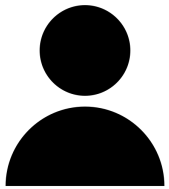
Eve

Sending an Encrypted Message with Key Pairs

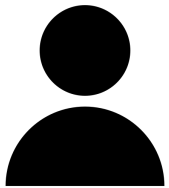
Me



Alice



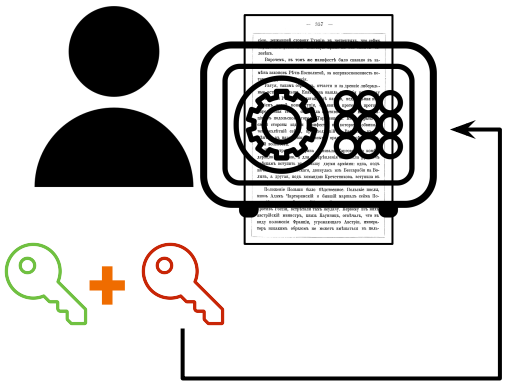
Bob



Eve

Sending an Encrypted Message with Key Pairs

Me



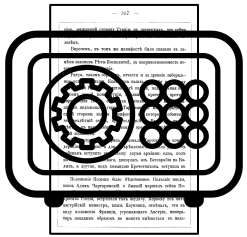
Alice

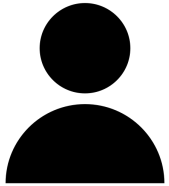
Bob

Eve

Sending an Encrypted Message with Key Pairs

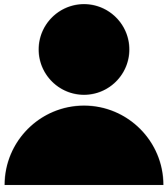
Sending an Encrypted Message with Key Pairs

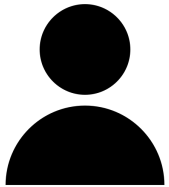




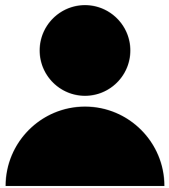
Alice

Me





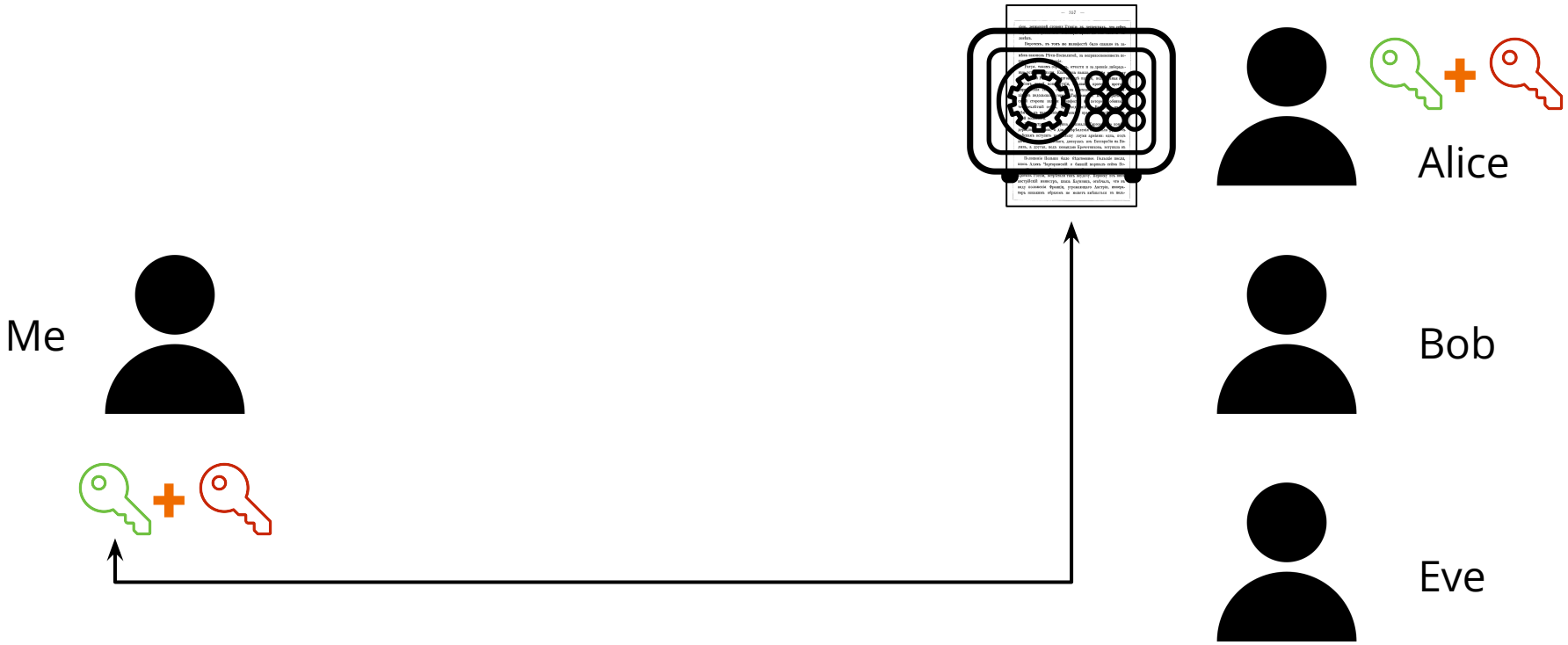
Bob



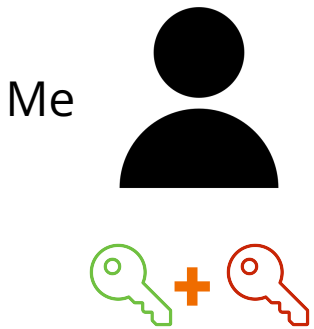
Eve

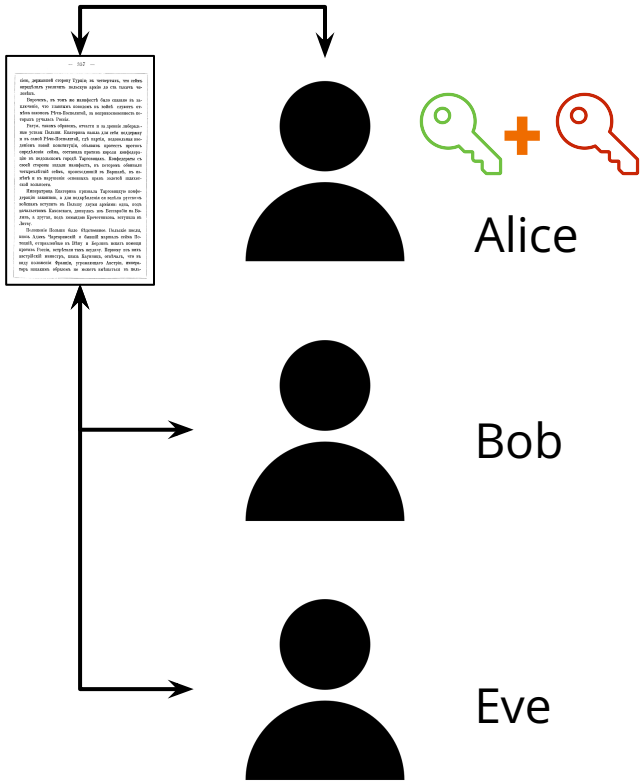
Who can decrypt this message?
What do you need to do it?

Sending an Encrypted Message with Key Pairs



Sending an Encrypted Message with Key Pairs





Who can decrypt this message? EVERYONE
What do you need to do it? MY PUBLIC KEY

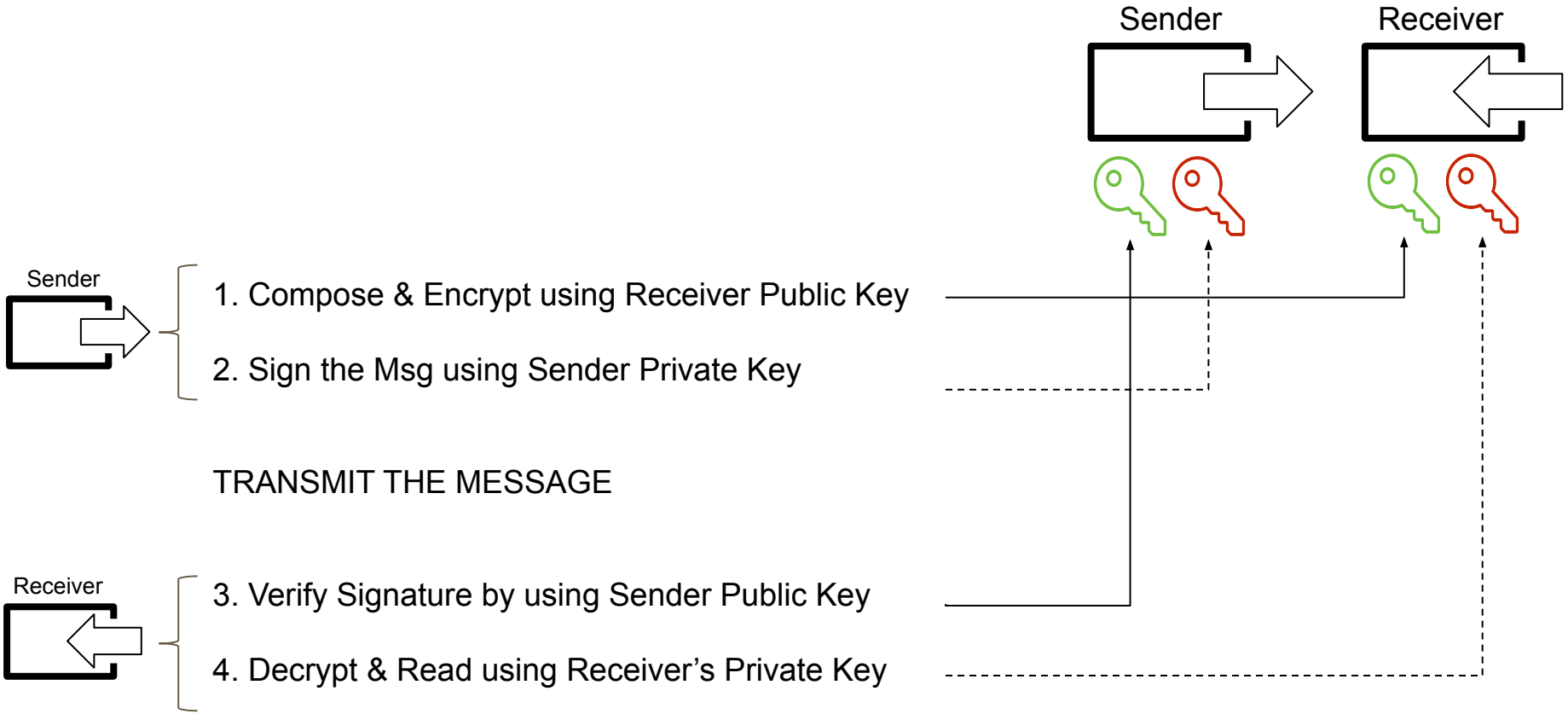
Wouldn’t that be stupid?

Who can decrypt this message? EVERYONE
What do you need to do it? MY PUBLIC KEY

Wouldn't that be stupid?
OR WOULD IT?!

Digital Signatures …
Proving Authorship

How to encrypt, sign, transmit, and decrypt a msg



IV. Math to the Rescue

One-way functions, secure hashing and SHA-256

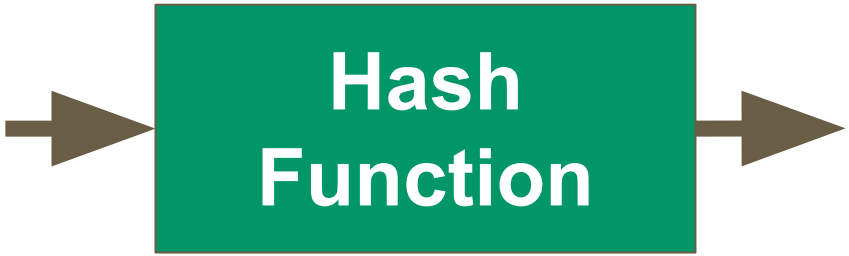
Functions in Math

- Simply put, a function is a (mathematical) operation ...
- ... one input equals to one output
- f(x) where x is the input value
- Example:
  - our function is “Doubling” →
  - f(x) = 2x →
  - Take an input, then double it (or multiply by 2)
  - For x=**4 (i.e. input is 4)**, then the **output is 8**
- But then a funny thing happens ...

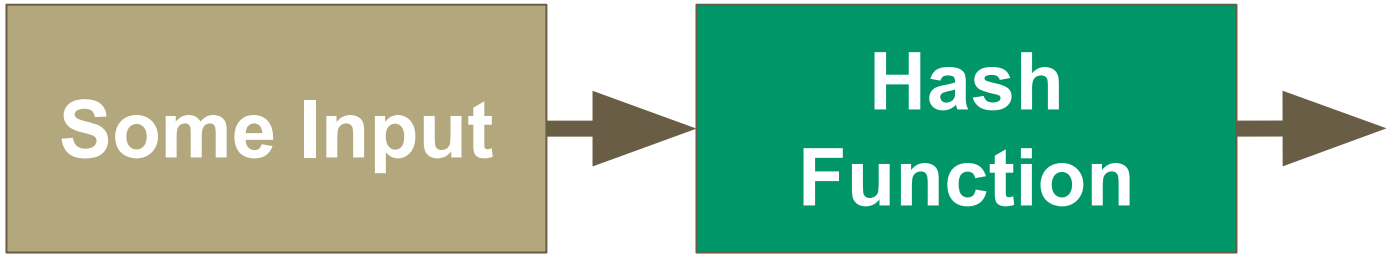
Functions in Math

- Let's look at this "funny" business ...
- ... our function is still "Doubling" →
- So what if I give you the output only? Can you figure out the input?
- OF COURSE ... we'll just reverse the function
- Example:
  - our function is "Doubling" →
  - f(x) = 2x →
  - If the output is **16**, then the input is ...
  - **8** :-)
- Most functions in math are Two-way Functions (reversible), but ...
- Some functions are one-way (e.g., hashing functions)

Hashing (One Way Functions)



Hashing (One Way Functions)

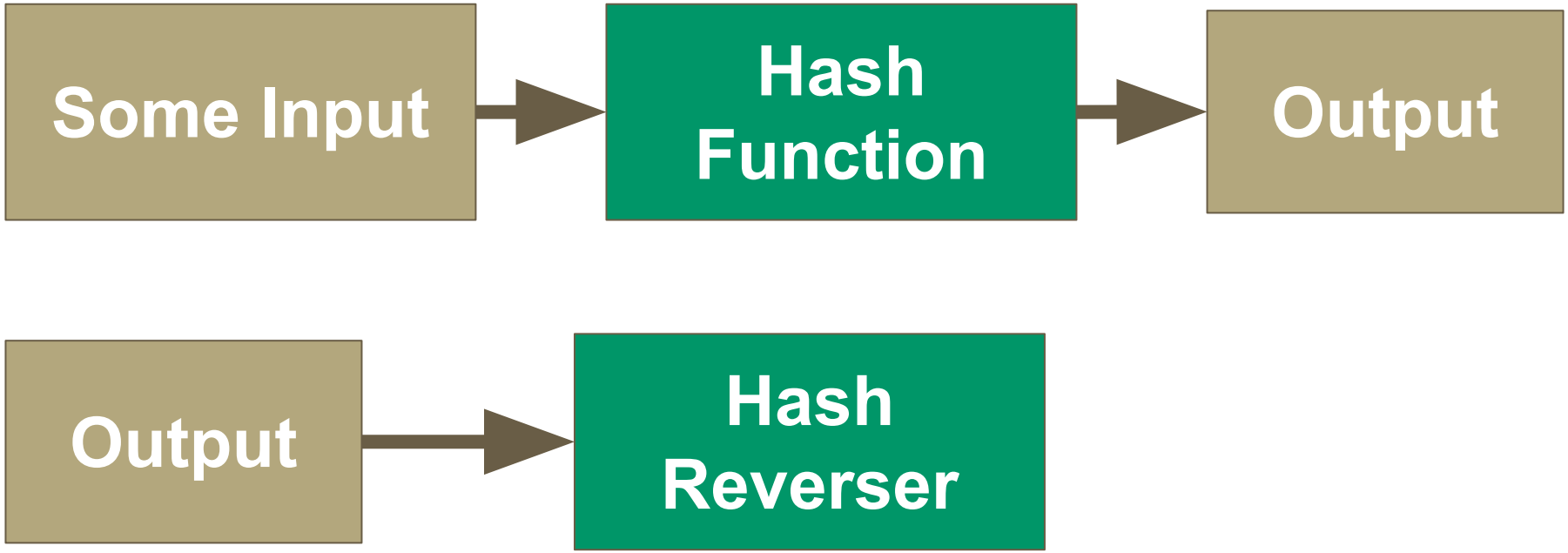


Hashing (One Way Functions)

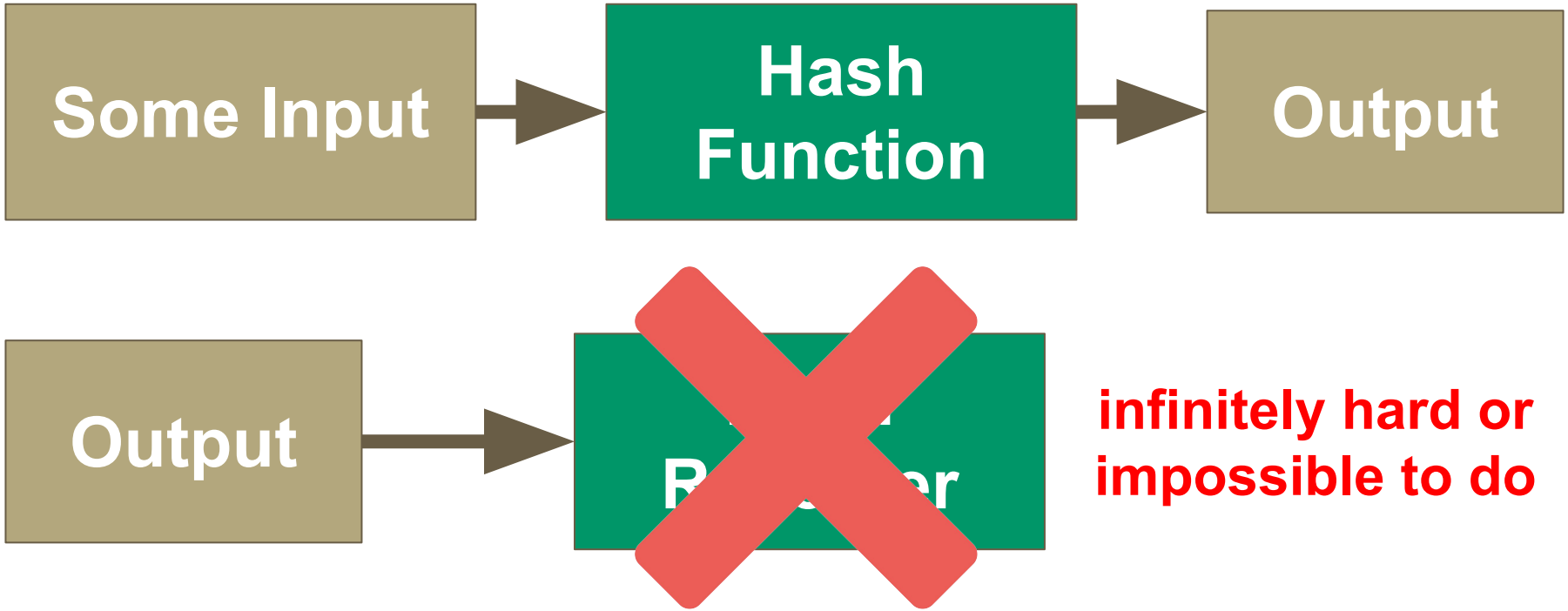
Hashing (One Way Functions)

Output

Hashing (One Way Functions)



Hashing (One Way Functions)



Great example of a One-way Function …

Real-World One-Way Function (Hashing Function)

Real-World One-Way Function (Hashing Function)

SuperPages.com 195

Cartage New England Inc
26 Allen Ln Ipswich 01938.....978 356-9960
Cartagema Lydia
18 Jewett Ros 02131.....617 323-7639
Cartagena Avith
9 Bancroft Rox 02119.....617 442-9780
B Hyd 02136.....617 361-5253
Jessica 50 Decatur Cha 02129.....617 241-0152
Lucilla 174 Harvard Cam 02139.....617 491-5621
M 95 Rowe Ros 02131.....617 323-9713
Melvin 501 Green Cam 02139.....617 576-1061
Carte Nicholas
18 Appleton Boston 02116.....617 695-6996
Cartegena O 4 Milford Bos 02118.....617 338-8219
Carten Thos J Sr & Claire
1 Paradise Rd Mil 02186.....617 698-6163
Thomas & Kathleen
50 Thompson Ln Mil 02186.....617 696-6919
Carter A Ros 02131.....617 327-2257
A Roxbury.....617 442-5230
A 31 Bethune Wy Roxbury 02119.....617 442-1219
A 260 Putnam Av Cambridge 02139.....617 492-4174
A M 255 Maschsts Av Bos 02115.....617 266-7153
Carter F 24 Hillock Ros 02131.....617 327-1105
Faye & Ricky
357 Columbus Av Bos 02116.....617 437-7331
Francis S 134 Temple W Rox 02132..617 323-6781
Franklin & Anne
221 Mt Auburn Cam 02138.....617 354-0798
Fred 42 Haverford Jam 02130.....617 524-3078
Fred 96 Hinckley Rd Mil 02186.....617 698-1343
G & R 8 Verdun Dor 02124.....617 436-8906
G T 27 Franklin Av Som 02145.....617 623-7121
Gayle 25 Frontenac Dor 02124.....617 825-0322
Geo S 115 Moss Hill Rd Jam 02130.....617 522-3215
George 125 Nashua Bos 02114.....617 367-9548
Carter Halliday Associate
107 S Street Bos 02111.....617 456-1689
Carter Harry F
26 Runng Brk Rd W Rox 02132.....617 325-5465
Carter Hide Co Inc
146 Summer Bos 02110.....617 542-7987
Carter Hilary 61 Harvey Cam 02140.....617 876-2750
Horace
241 Walnut Av Roxbury 02119.....617 442-5307
Howard Jr 26 Notre Dme Rox 02119.617 445-5552

Real-World One-Way Function (Hashing Function)

SuperPages.com 195

Cartage New England Inc
26 Allen Ln Ipswich 01938.....978 356-9960
Cartagema Lydia
18 Jewett Ros 02131.....617 323-7639
Cartagena Avith
9 Bancroft Rox 02119.....617 442-9780
B Hyd 02136.....617 361-5253
Jessica 50 Decatur Cha 0212[illegible].....617 241-0152
Lucilla 174 Harvard Cam 0213[illegible].....617 491-5621
M 95 Rowe Ros 02131.....617 323-9713
Melvin 501 Green Cam 02139.....617 576-1061
Carte Nicholas
18 Appleton Boston 02116.....617 695-6996
Cartegena O 4 Milford Bos 021[illegible].....617 338-8219
Carten Thos J Sr & Claire
1 Paradise Rd Mil 02186.....617 698-6163
Thomas & Kathleen
50 Thompson Ln Mil 02186.....617 696-6919
Carter A Ros 02131.....617 327-2257
A Roxbury.....617 442-5230
A 31 Bethune Wy Roxbury 0211[illegible].....617 442-1219
A 260 Putnam Av Cambridge 02[illegible]39.....617 492-4174
A M 255 Maschsts Av Bos 021[illegible].....617 266-7153
Carter F 24 Hillock Ros 02131.....617 327-1105
Faye & Ricky
357 Columbus Av Bos 02116.....617 437-7331
Francis S 134 Temple W Rox 02132..617 323-6781
Franklin & Anne
221 Mt Auburn Cam 02138.....617 354-0798
Fred 42 Haverford Jam 02130.....617 524-3078
Fred 96 Hinckley Rd Mil 02186.....617 698-1343
G & R 8 Verdun Dor 02124.....617 436-8906
G T 27 Franklin Av Som 02145.....617 623-7121
Gayle 25 Frontenac Dor 02124.....617 825-0322
Geo S 115 Moss Hill Rd Jam 02130.....617 522-3215
George 125 Nashua Bos 02114.....617 367-9548
Carter Halliday Associate
107 S Street Bos 02111.....617 456-1689
Carter Harry F
26 Runng Brk Rd W Rox 02132.....617 325-5465
Carter Hide Co Inc
146 Summer Bos 02110.....617 542-7987
Carter Hilary 61 Harvey Cam 02140.....617 876-2750
Horace
241 Walnut Av Roxbury 02119.....617 442-5307
Howard Jr 26 Notre Dme Rox 02119.617 445-5552

Our Function is =
for a given input, find the output

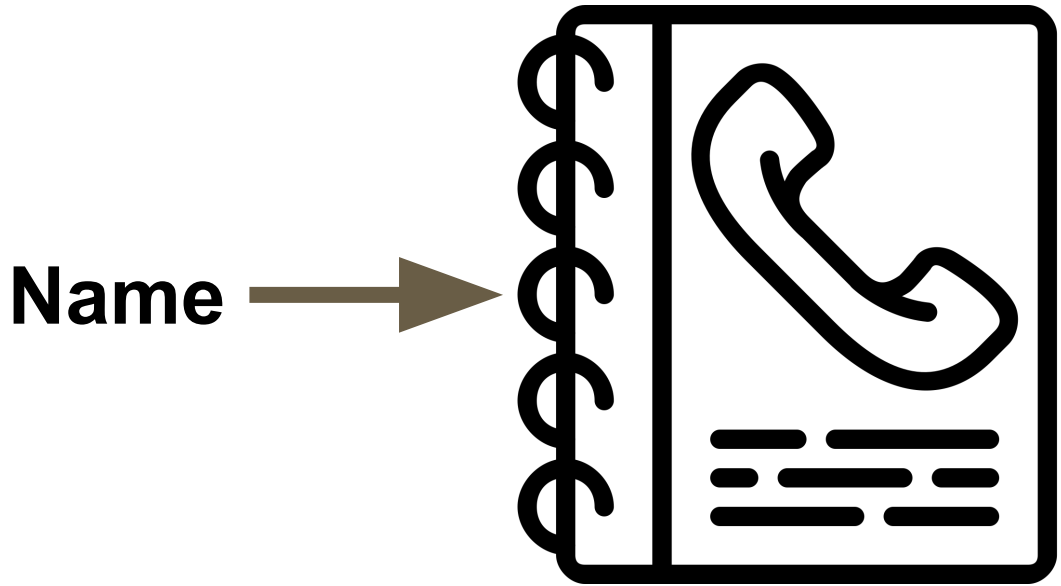
Our Function is =

for a given input (name) $\longrightarrow$

find the output (corresponding phone number)

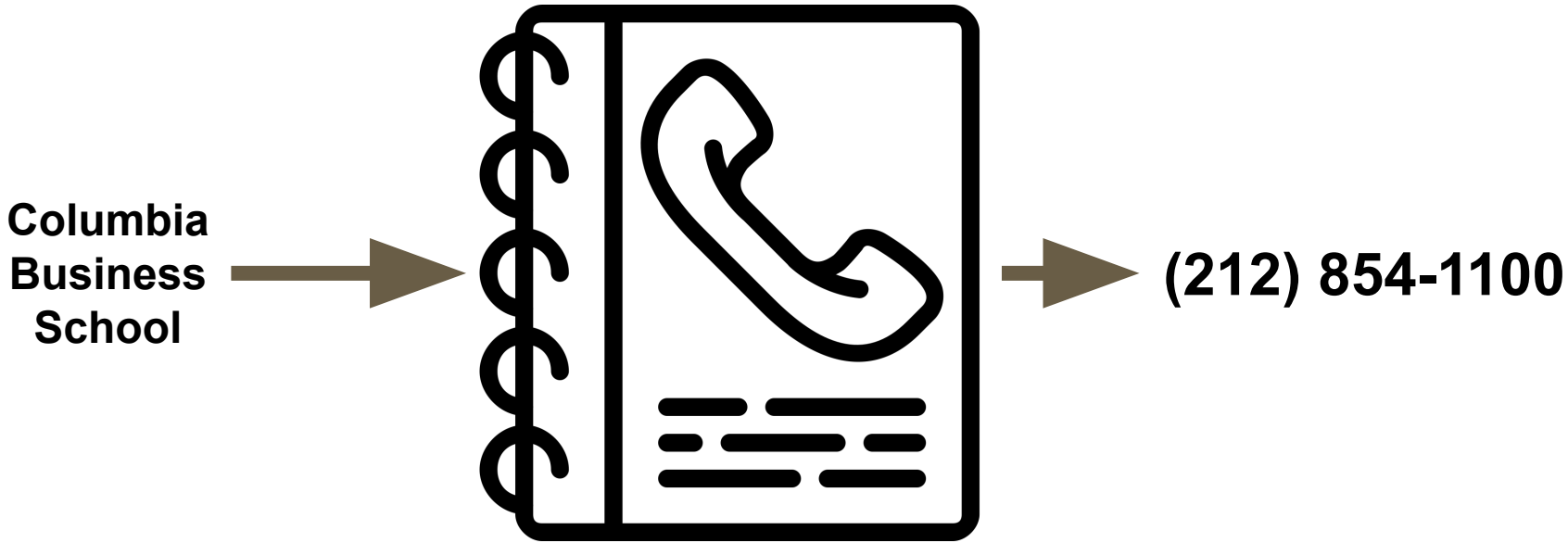
A Real-World Hashing Function

A Real-World Hashing Function



A Real-World Hashing Function

A Real-World Hashing Function



Our Reverse Function is =
for a given input (phone number) ⟶
find the output (corresponding name)

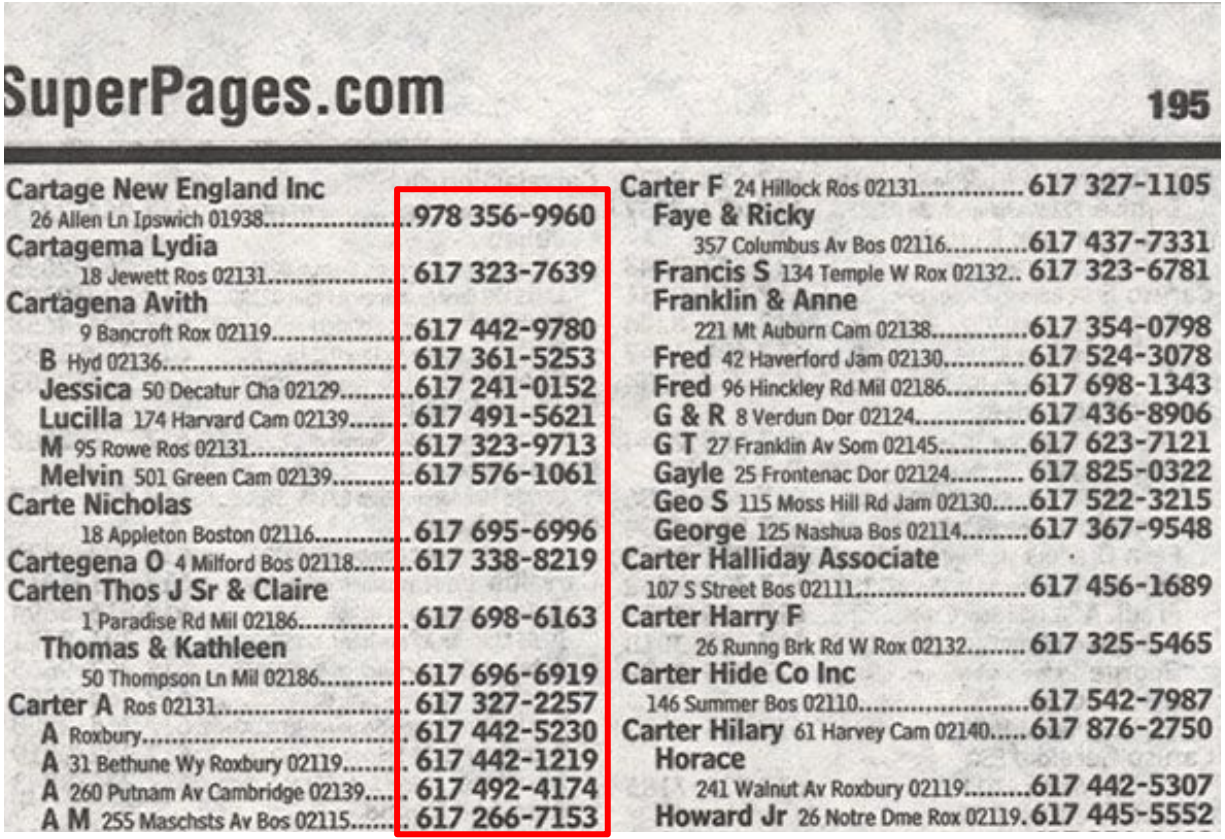
A Real-World Hashing Function

(212) 854-5553

A Real-World Hashing Function

(212) 854-5553

Real-World One-Way Function (Hashing Function)

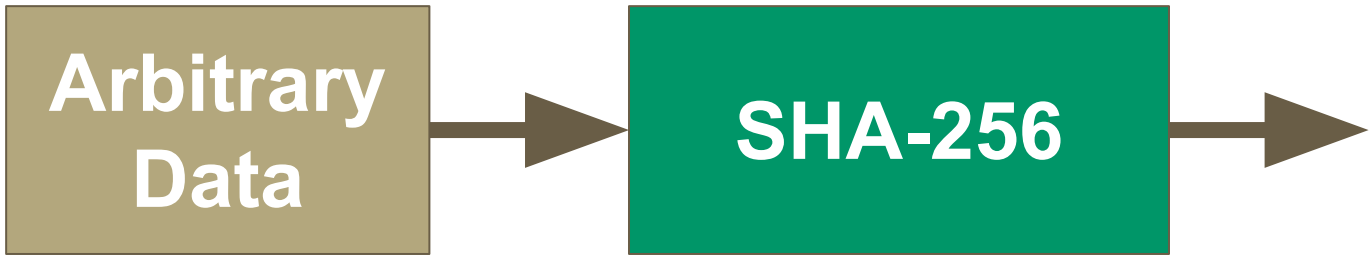


SuperPages.com 195

Cartage New England Inc
26 Allen Ln Ipswich 01938.....978 356-9960
Cartagema Lydia
18 Jewett Ros 02131.....617 323-7639
Cartagena Avith
9 Bancroft Rox 02119.....617 442-9780
B Hyd 02136.....617 361-5253
Jessica 50 Decatur Cha 02129.....617 241-0152
Lucilla 174 Harvard Cam 02139.....617 491-5621
M 95 Rowe Ros 02131.....617 323-9713
Melvin 501 Green Cam 02139.....617 576-1061
Carte Nicholas
18 Appleton Boston 02116.....617 695-6996
Cartegena O 4 Milford Bos 02118.....617 338-8219
Carten Thos J Sr & Claire
1 Paradise Rd Mil 02186.....617 698-6163
Thomas & Kathleen
50 Thompson Ln Mil 02186.....617 696-6919
Carter A Ros 02131.....617 327-2257
A Roxbury.....617 442-5230
A 31 Bethune Wy Roxbury 02119.....617 442-1219
A 260 Putnam Av Cambridge 02139.....617 492-4174
A M 255 Maschsts Av Bos 02115.....617 266-7153
Carter F 24 Hillock Ros 02131.....617 327-1105
Faye & Ricky
357 Columbus Av Bos 02116.....617 437-7331
Francis S 134 Temple W Rox 02132..617 323-6781
Franklin & Anne
221 Mt Auburn Cam 02138.....617 354-0798
Fred 42 Haverford Jam 02130.....617 524-3078
Fred 96 Hinckley Rd Mil 02186.....617 698-1343
G & R 8 Verdun Dor 02124.....617 436-8906
G T 27 Franklin Av Som 02145.....617 623-7121
Gayle 25 Frontenac Dor 02124.....617 825-0322
Geo S 115 Moss Hill Rd Jam 02130.....617 522-3215
George 125 Nashua Bos 02114.....617 367-9548
Carter Halliday Associate
107 S Street Bos 02111.....617 456-1689
Carter Harry F
26 Runng Brk Rd W Rox 02132.....617 325-5465
Carter Hide Co Inc
146 Summer Bos 02110.....617 542-7987
Carter Hilary 61 Harvey Cam 02140.....617 876-2750
Horace
241 Walnut Av Roxbury 02119.....617 442-5307
Howard Jr 26 Notre Dme Rox 02119.617 445-5552

Secure Hashing Algo (used in Bitcoin & others)

Secure Hashing Algo (used in Bitcoin & others)



Secure Hashing Algo (used in Bitcoin & others)

Secure Hashing Algo (used in Bitcoin & others)

0 → 2^256

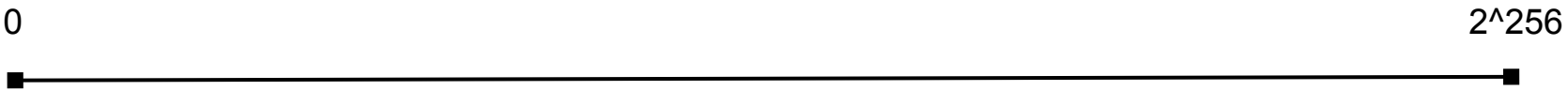
SHA-256

SHA-256 hash: a number with the range:

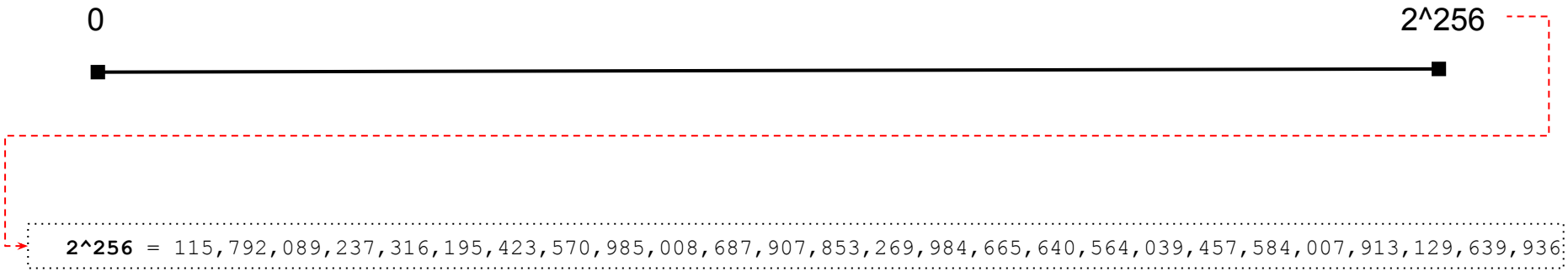
$$0 \rightarrow 2^{256}$$

2^256 = 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936

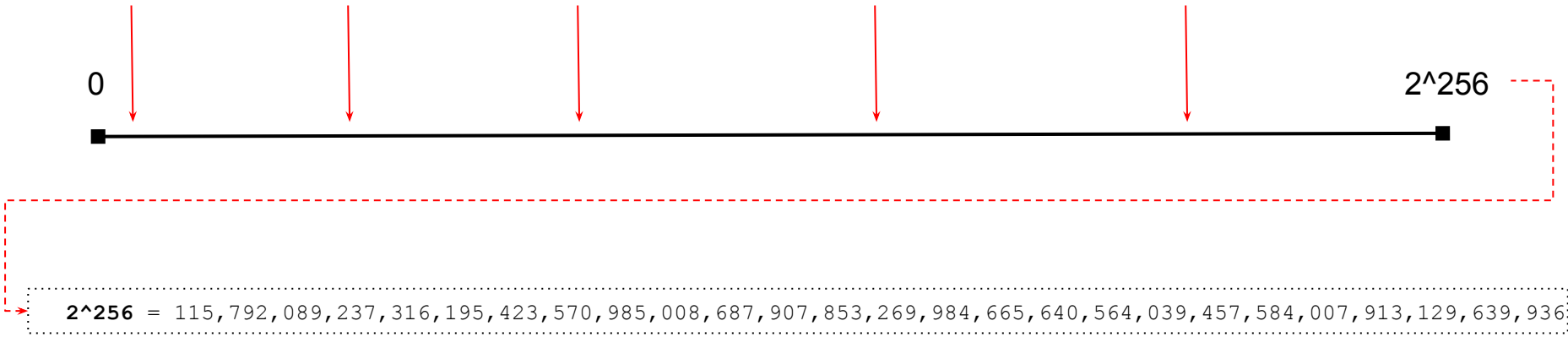
SHA-256 Hash



SHA-256 Hash: a continuous number line



SHA-256 Hash: a continuous number line



SHA-256: points on the long line

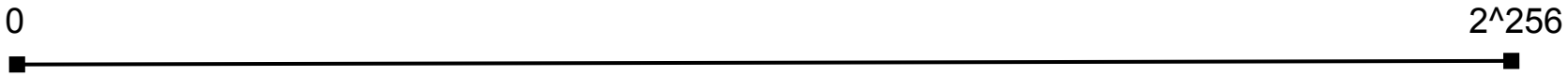
Each point would be consisting of many digits:

0
1
2
3
4
8
25
9387
23430174432
57098500868790785
731619542357098500868790785326998466564
485326998466590785989574881374897138479854664524049 2
1157920892373161954235709850086879078532699846656405640394575840079131296 39

Numerical Encoding

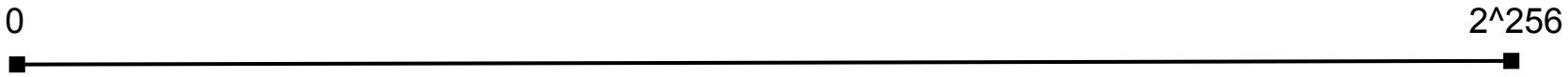
	Example	Digits Used
Decimal Number	`2128541100`	`0123456789`
Hexadecimal Number	`7edef5ac`	`0123456789abcdef`

SHA-256 Hash



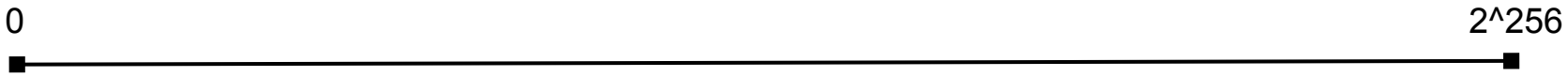
Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000

SHA-256 Hash



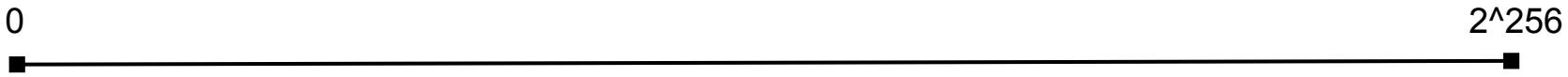
Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001

SHA-256 Hash



Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002

SHA-256 Hash



Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002
9	0000000000000000000000000000000000000000000000000000000000000009

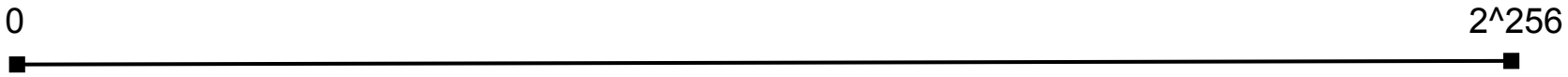
SHA-256 Hash

Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002
9	0000000000000000000000000000000000000000000000000000000000000009
10	000000000000000000000000000000000000000000000000000000000000000a

SHA-256 Hash

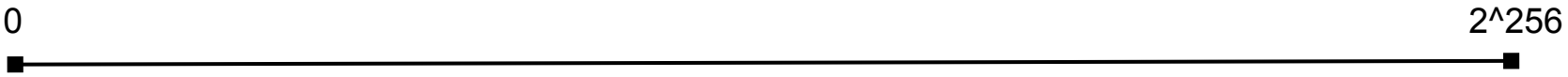
Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002
9	0000000000000000000000000000000000000000000000000000000000000009
10	000000000000000000000000000000000000000000000000000000000000000a
11	000000000000000000000000000000000000000000000000000000000000000b
15	000000000000000000000000000000000000000000000000000000000000000f

SHA-256 Hash



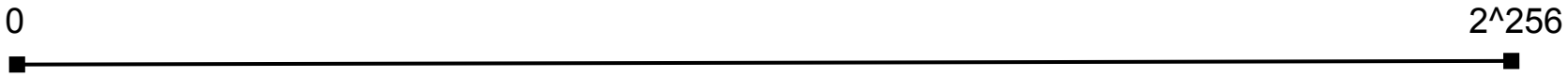
Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002
9	0000000000000000000000000000000000000000000000000000000000000009
10	000000000000000000000000000000000000000000000000000000000000000a
11	000000000000000000000000000000000000000000000000000000000000000b
15	000000000000000000000000000000000000000000000000000000000000000f
16	0000000000000000000000000000000000000000000000000000000000000000 **10**

SHA-256 Hash



Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002
9	0000000000000000000000000000000000000000000000000000000000000009
10	000000000000000000000000000000000000000000000000000000000000000a
11	000000000000000000000000000000000000000000000000000000000000000b
15	000000000000000000000000000000000000000000000000000000000000000f
16	0000000000000000000000000000000000000000000000000000000000000010
17	0000000000000000000000000000000000000000000000000000000000000011

SHA-256 Hash



Decimal	HexaDecimal
0	0000000000000000000000000000000000000000000000000000000000000000
1	0000000000000000000000000000000000000000000000000000000000000001
2	0000000000000000000000000000000000000000000000000000000000000002
9	0000000000000000000000000000000000000000000000000000000000000009
10	000000000000000000000000000000000000000000000000000000000000000a
11	000000000000000000000000000000000000000000000000000000000000000b
15	000000000000000000000000000000000000000000000000000000000000000f
16	0000000000000000000000000000000000000000000000000000000000000010
17	0000000000000000000000000000000000000000000000000000000000000011
1000	00000000000000000000000000000000000000000000000000000000000003e8

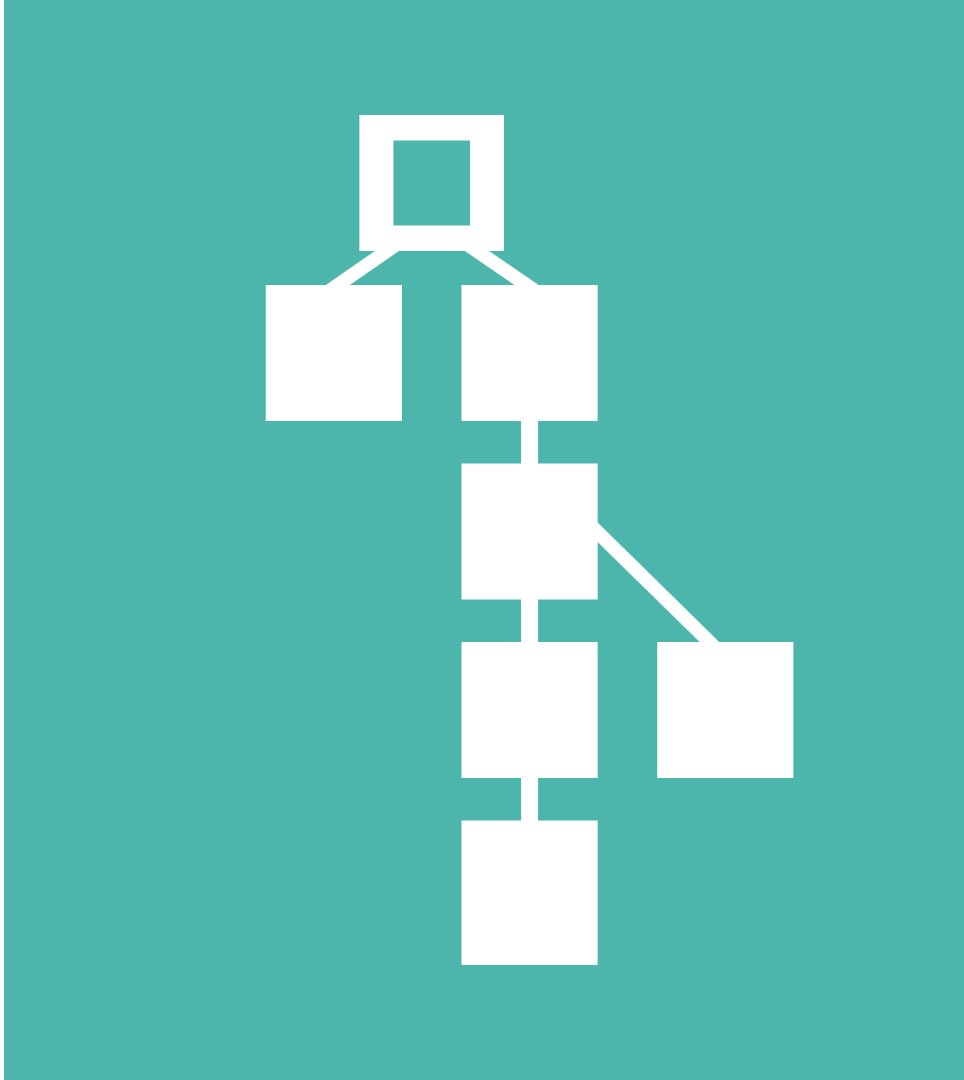
Hashing Demo and Sample Use Case …
… that actually happened with a student!

SHA-256


```
8f434346648f6b96df89dda901c5176b10a6d83961dd3c1ac88b59b2dc327aa4
79f5c65fe815417fe2dc3fdbfbda9dbff7e0ecf63dea6162d4339546e7aa4d49
fd04788626e5f87b3b22b2b855bddaae2f1ee43956232d2fa57c5afa7d3f09b9
d38b38a2dd476e045c299e8ee5d6466834456d97bd592a71746b423a6a05f386
```

IV. Building the Blockchain

Using all we've learned to build an immutable chain of "digital assets" (and more)



Exercise: let's do a deal!

Parties involved:

1. **Bridget Fox (BF); Commercial Bank Corp (CBC); IB**
2. **Robert Farrokhnia (RF); Columbia University (COL); Advisor**
3. **Jeff Dewey (JD); Dewey, Cheatem & Howe (DCH); Law**
4. **Alex Runne (AR); Steel, Runne & Hyde (SRH): Accounting**

We will have lots of documents going back and forth.

Exercise: let's collaborate on a document

Our document naming convention, or protocol:

[type of doc]_[company name]_[author's initials]_[author's employer]_[date: dd/mm/yy]_[version number: v#]

[type of doc]_[company name]_[author's initials]_[author's employer]_[date: dd/mm/yy]_[version number: v#]

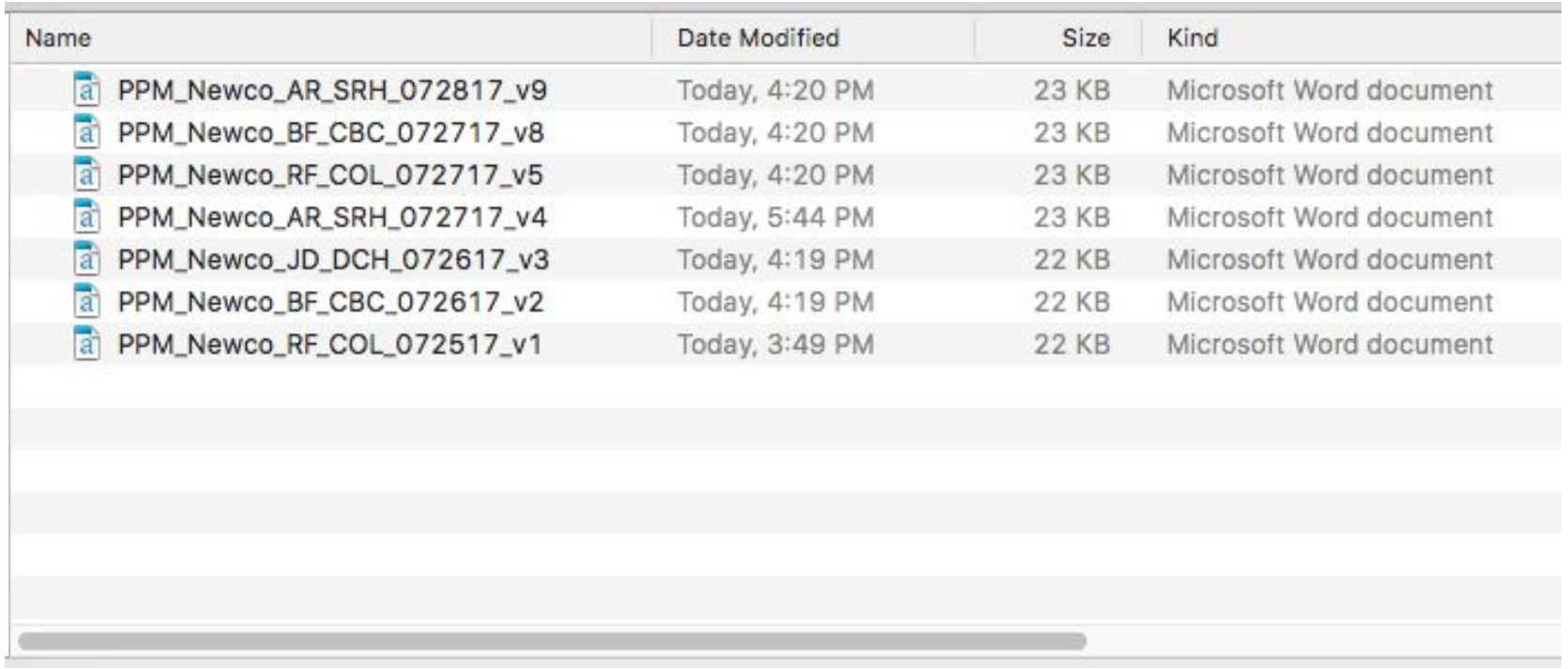
PPM_Newco_RF_COL_010123_v1

[type of doc]_[company name]_[author's initials]_[author's employer]_[date: dd/mm/yy]_[version number: v#]

PPM_Newco_RF_COL_010123_v1

PPM_Newco_BF_CBC_010223_v2

Exercise: naming protocol sorted by “Name”



Name	Date Modified	Size	Kind
PPM_Newco_AR_SRH_072817_v9	Today, 4:20 PM	23 KB	Microsoft Word document
PPM_Newco_BF_CBC_072717_v8	Today, 4:20 PM	23 KB	Microsoft Word document
PPM_Newco_RF_COL_072717_v5	Today, 4:20 PM	23 KB	Microsoft Word document
PPM_Newco_AR_SRH_072717_v4	Today, 5:44 PM	23 KB	Microsoft Word document
PPM_Newco_JD_DCH_072617_v3	Today, 4:19 PM	22 KB	Microsoft Word document
PPM_Newco_BF_CBC_072617_v2	Today, 4:19 PM	22 KB	Microsoft Word document
PPM_Newco_RF_COL_072517_v1	Today, 3:49 PM	22 KB	Microsoft Word document

Exercise: naming protocol sorted by “Date Modified”

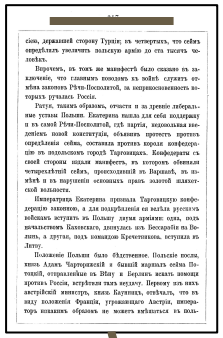
Name	Date Modified	Size	Kind
PPM_Newco_AR_SRH_072717_v4	Today, 5:44 PM	23 KB	Microsoft Word document
PPM_Newco_AR_SRH_072817_v9	Today, 4:20 PM	23 KB	Microsoft Word document
PPM_Newco_BF_CBC_072717_v8	Today, 4:20 PM	23 KB	Microsoft Word document
PPM_Newco_RF_COL_072717_v5	Today, 4:20 PM	23 KB	Microsoft Word document
PPM_Newco_JD_DCH_072617_v3	Today, 4:19 PM	22 KB	Microsoft Word document
PPM_Newco_BF_CBC_072617_v2	Today, 4:19 PM	22 KB	Microsoft Word document
PPM_Newco_RF_COL_072517_v1	Today, 3:49 PM	22 KB	Microsoft Word document

What can do wrong? How to fix the system?

Let's build a blockchain, connecting and linking verified digital files in an immutable way with a shared ledger to keep track of it all that every party can see.

Hash 000...

PPM v1



сію, державшій сторону Турціи; въ четвертыхъ, что сейчасъ опредѣлилъ увеличить польскую армію до ста тысячъ человѣкъ.

Впрочемъ, въ этомъ же манифестѣ было сказано въ заключеніе, что главныхъ поводовъ къ войнѣ, служитъ отказъ заключить Рѣчь-Посполитой, за неприкосновенность которыхъ ручалась Россія.

Ратуя, такимъ образомъ, очистить и за древніе либеральные устои Польши Екатерина нашла для себя поддержку и въ самой Рѣчи-Посполитой, гдѣ партія, недовольная внесеніемъ новой конституціи, объявила протестъ противъ определенія сейма, составила противъ короля конфедерацію въ подольскомъ городѣ Тарговицѣ. Конфедераты съ своей стороны издали манифестъ, въ которомъ обвиняли четырехлѣтній сеймъ, происходящій въ Варшавѣ, въ измѣнѣ и въ нарушеніи основныхъ правъ золотой шляхетской вольности.

Императрица Екатерина признала Тарговицкую конфедерацію законною, а для поддержанія ея вслѣдъ россіяне войсками вступили въ Польшу двумя арміями: одна, подъ начальствомъ Каховскаго, двинулась изъ Бессарабіи на Волынь, а другая, подъ командою Кречетникова, вступила въ Литву.

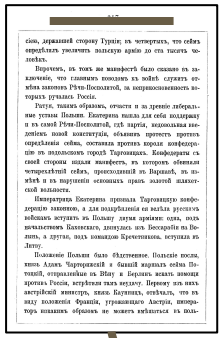
Положеніе Польши было обдуманное. Польскіе послы, князь Адамъ Чарторижскій и бывшій маршалъ сейма Потоцкій, отправленные въ Вѣну и Берлинъ искать помощи противъ Россіи, встрѣтили тамъ неудачу. Первому изъ нихъ австрійскій министръ, князь Кауницъ, отвѣчалъ, что въ виду положенія Франціи, угрожающаго Австріи, императоръ никакимъ образомъ не можетъ вмѣшаться въ поль-

SHA-256

Sign with author Private Key to verify authenticity

Hash 000...

PPM v1



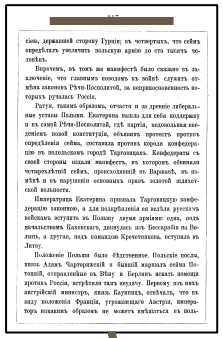
SHA-256

Hash: 09592b438bfe8ac1fd

Sign with author Private Key to verify authenticity

Hash 000...

PPM v1



Verified & Recorded on Distributed Shared Ledger

$$ Reward

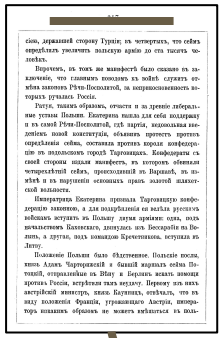
SHA-256

Hash: 09592b438bfe8ac1fd

Sign with author Private Key to verify authenticity

Hash 000...

PPM v1



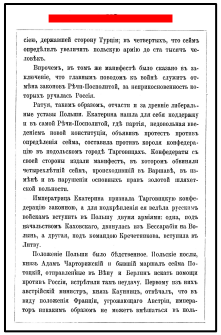
SHA-256

Verified & Recorded on Distributed Shared Ledger

$$ Reward

Hash: 09592b438bfe8ac1fd

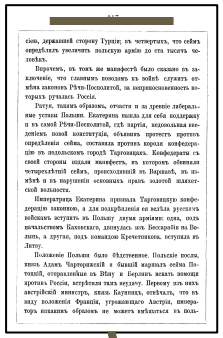
PPM v2



Sign with author Private Key to verify authenticity

Hash 000...

PPM v1



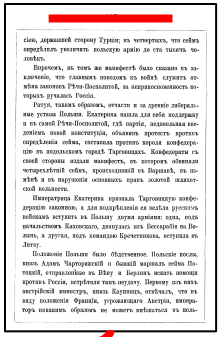
SHA-256

Verified & Recorded on Distributed Shared Ledger

$$ Reward

Hash: 09592b438bfe8ac1fd

PPM v2



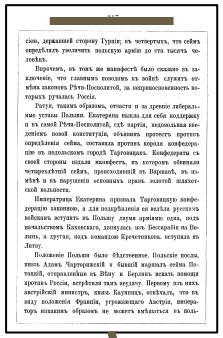
Sign with author Private Key to verify authenticity

SHA-256

Hash: fa1960e7a6b57ee967

Hash 000...

PPM v1



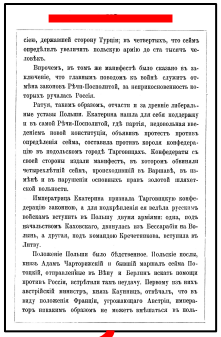
SHA-256

Verified & Recorded on Distributed Shared Ledger

$$ Reward

Hash: 09592b438bfe8ac1fd

PPM v2



Sign with author Private Key to verify authenticity

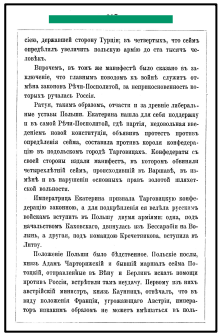
SHA-256

$$ Reward

Verified & Recorded on Distributed Shared Ledger

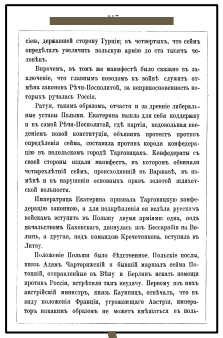
Hash: fa1960e7a6b57ee967

PPM v3



Hash 000...

PPM v1



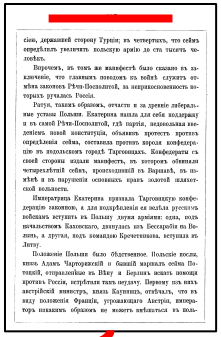
SHA-256

Verified & Recorded on Distributed Shared Ledger

$$ Reward

Hash: 09592b438bfe8ac1fd

PPM v2



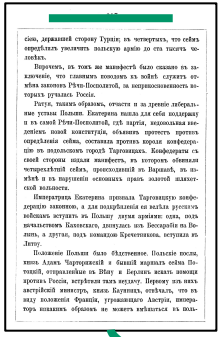
$$ Reward

Verified & Recorded on Distributed Shared Ledger

SHA-256

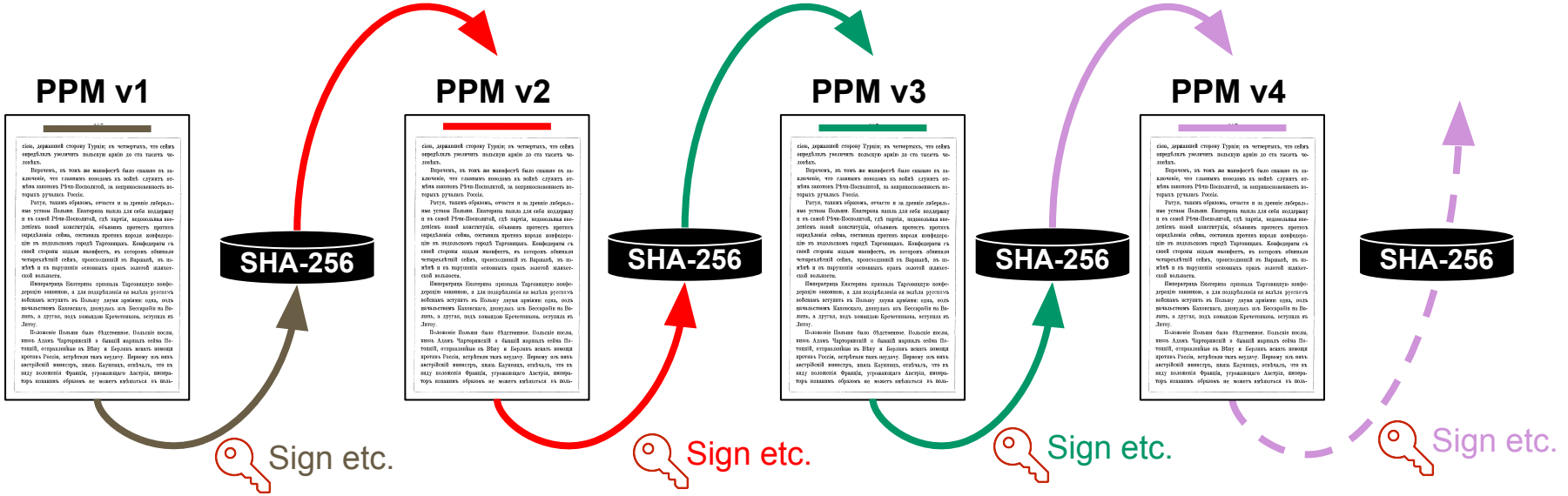
Hash: fa1960e7a6b57ee967

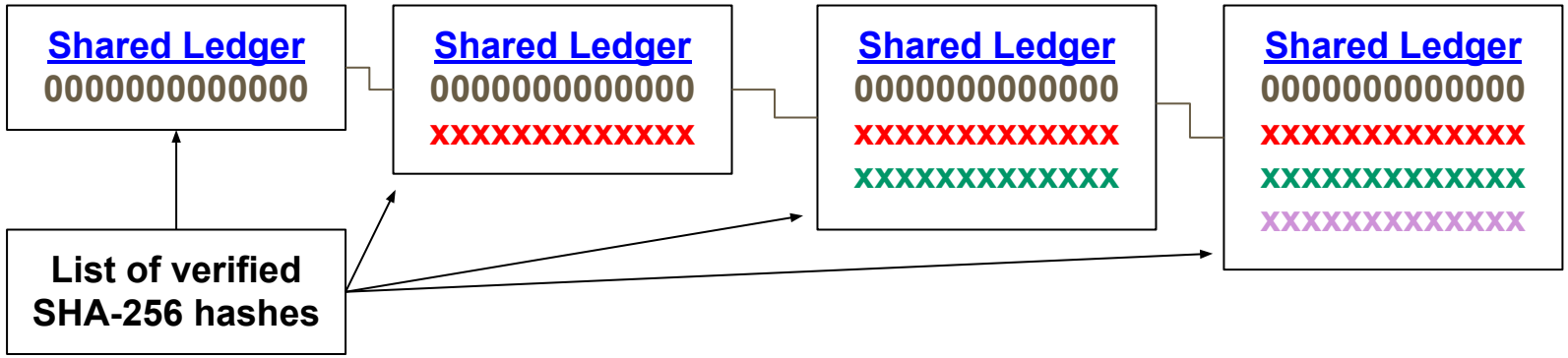
PPM v3



SHA-256

Sign etc.


PPM v1
PPM v2
PPM v3
PPM v4
SHA-256
SHA-256
SHA-256
SHA-256
Sign etc.
Sign etc.
Sign etc.
Sign etc.


Shared Ledger
0000000000000
Shared Ledger
0000000000000
XXXXXXXXXXXXX
Shared Ledger
0000000000000
XXXXXXXXXXXXX
XXXXXXXXXXXXX
Shared Ledger
0000000000000
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
List of verified
SHA-256 hashes

One of the earliest papers on "Blockchain"

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

*Appeared, with minor editorial changes, in *Journal of Cryptology*, Vol. 3, No. 2, pp. 99–111, 1991.

One of the earliest papers on "Blockchain"

How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

*Appeared, with minor editorial changes, in *Journal of Cryptology*, Vol. 3, No. 2, pp. 99–111, 1991.

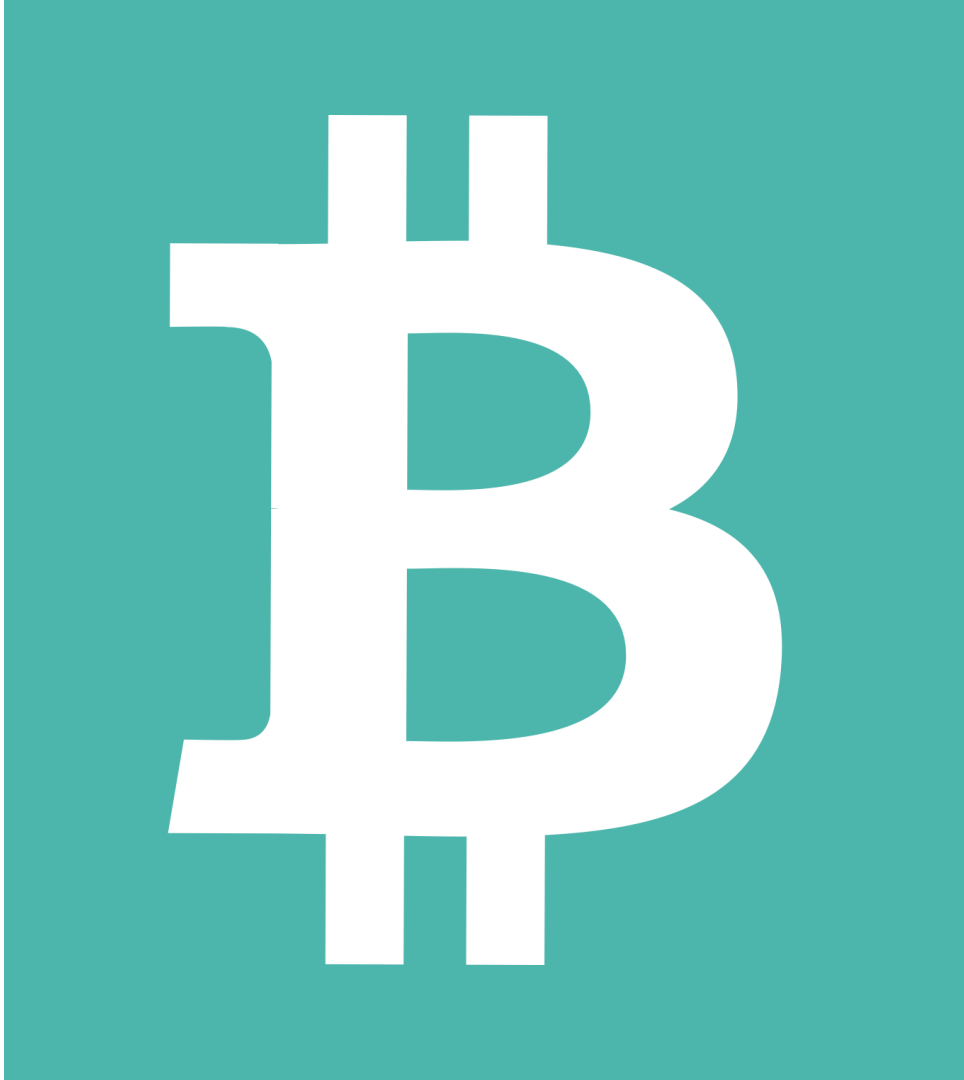
a few examples for the use of
blockchain-based technology and applications
in a few domains (beyond financial services) ...

Question for Class:
What do you think the “killer app” for blockchain will be?

Time permitting … let's discuss an application of blockchain that's seen the broadest use to date … Bitcoin!!

V. Bitcoin

Leveraging the blockchain to create a decentralized digital cryptocurrency.



Let’s set up a standard model:

Alice

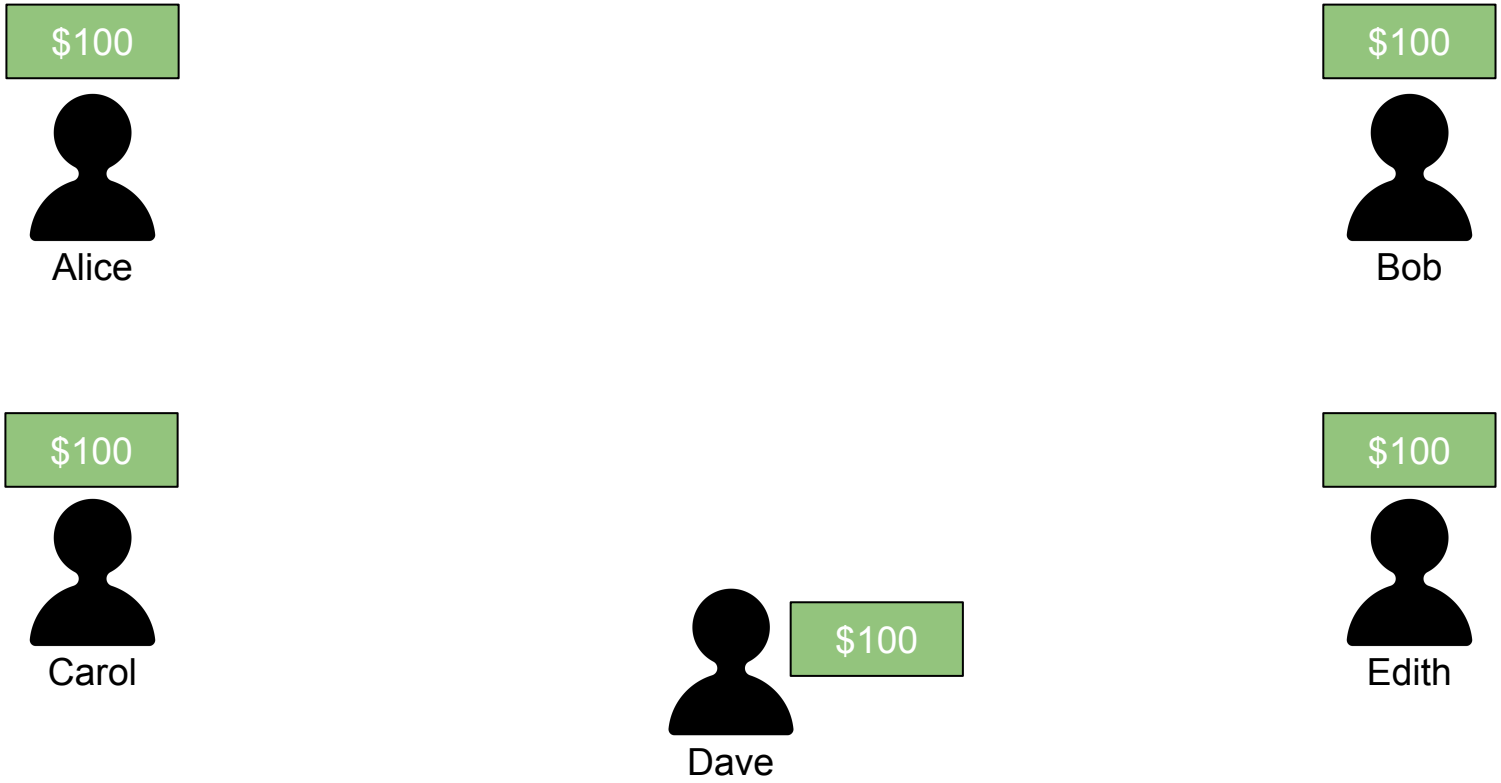
Bob

Carol

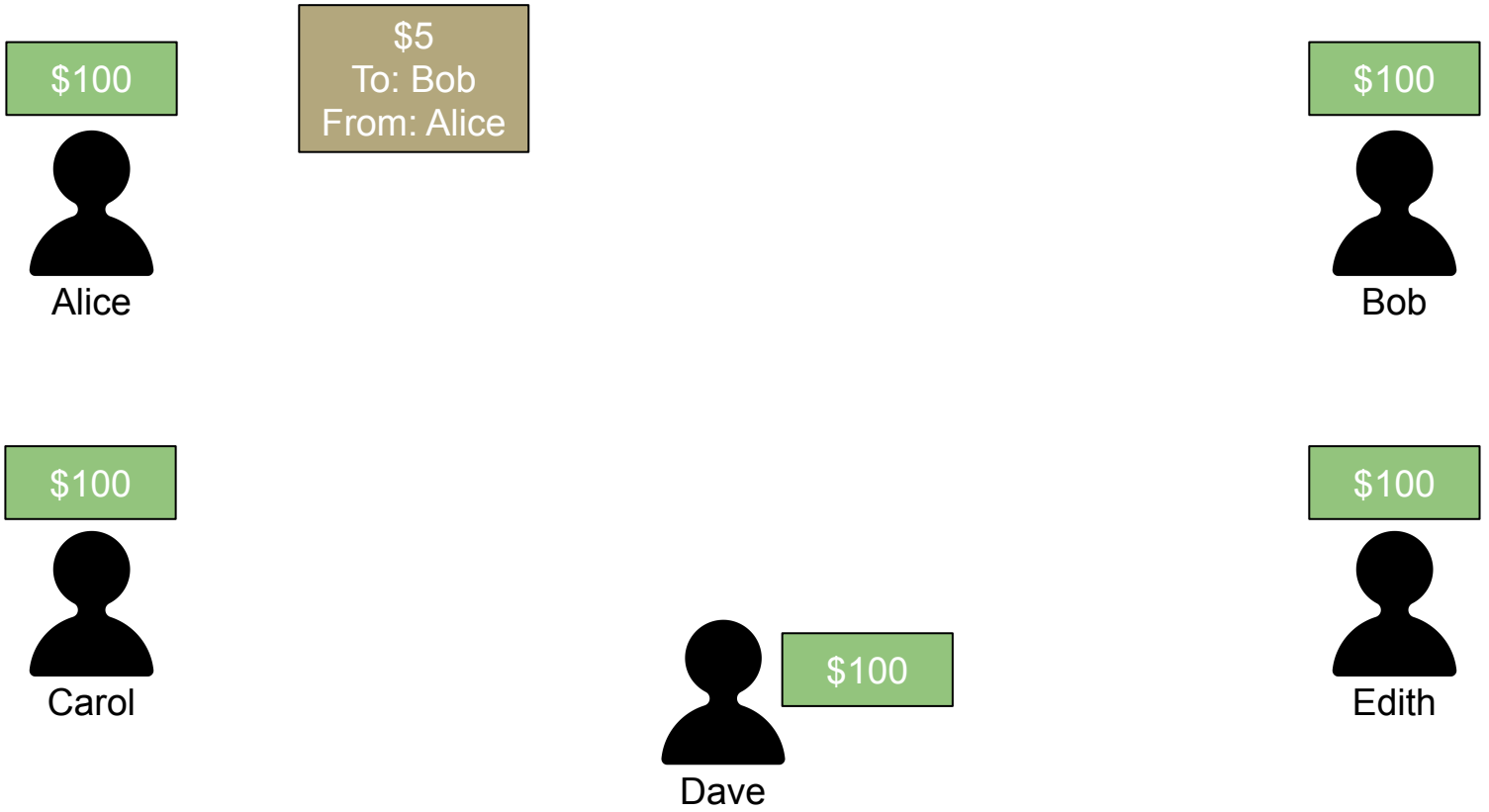
Dave

Edith

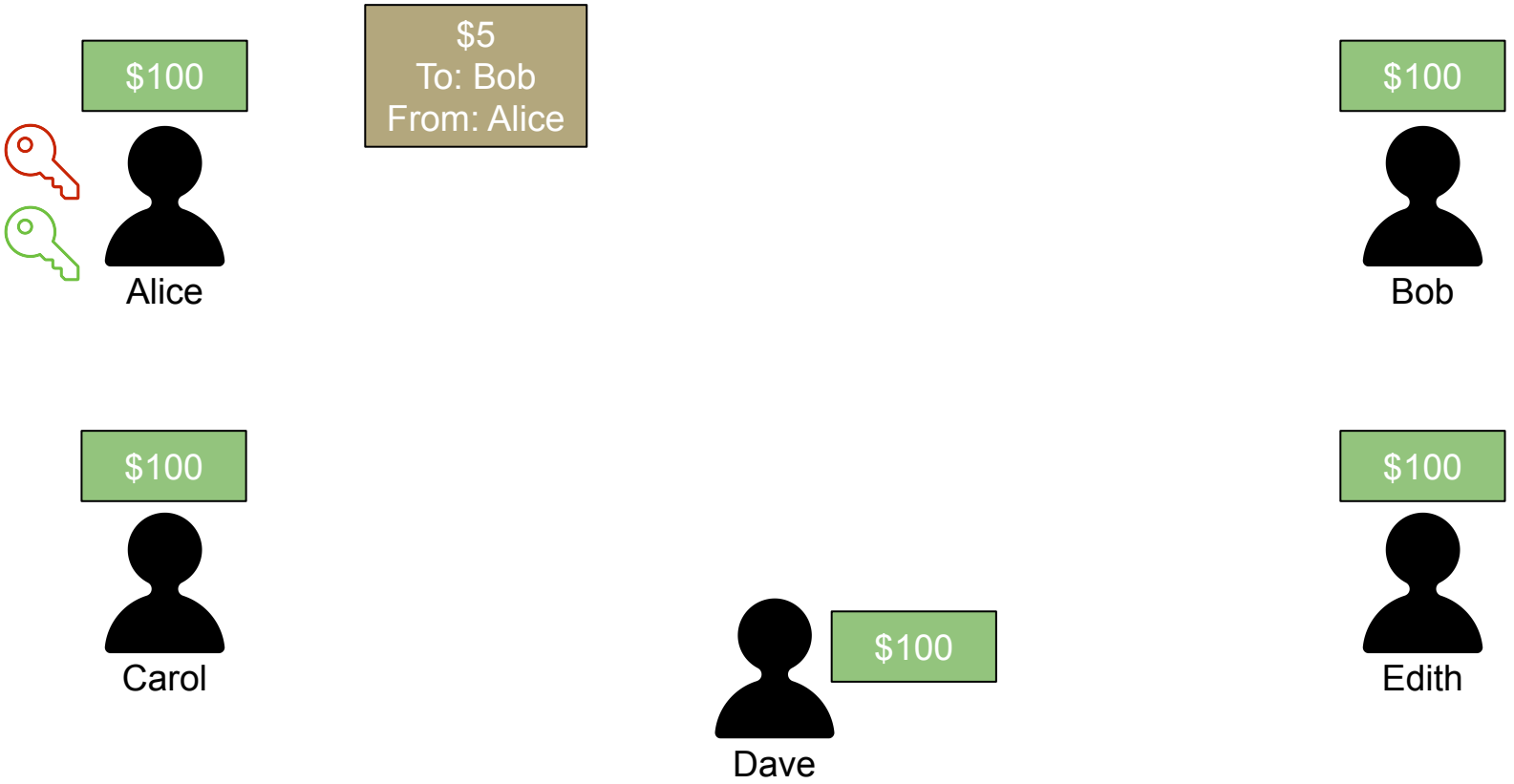
Our Model



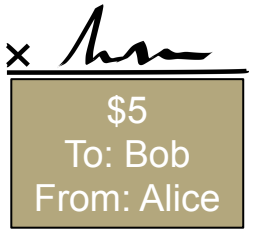
Our Model

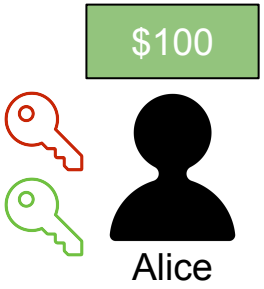

$100
Alice
$5
To: Bob
From: Alice
$100
Bob
$100
Carol
$100
Dave
$100
Edith

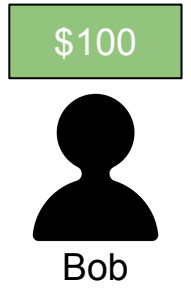
Our Model

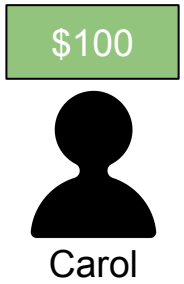

$100
$5
To: Bob
From: Alice
$100
Alice
Bob
$100
$100
$100
Carol
Dave
Edith

Our Model

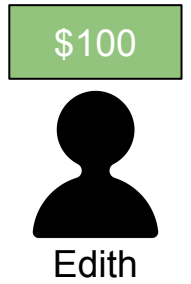

$5
To: Bob
From: Alice


$100
Alice

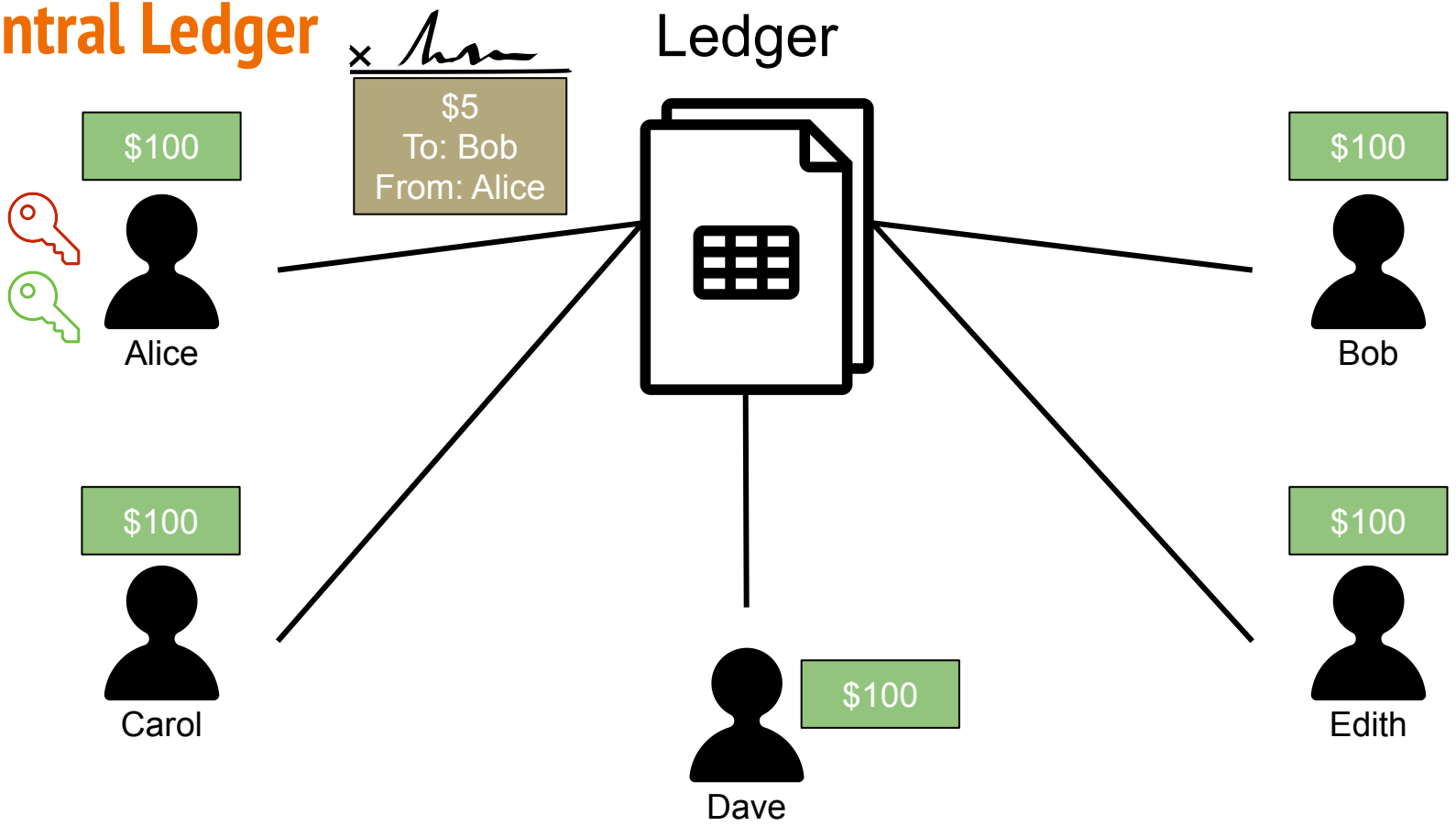

$100
Bob


$100
Carol

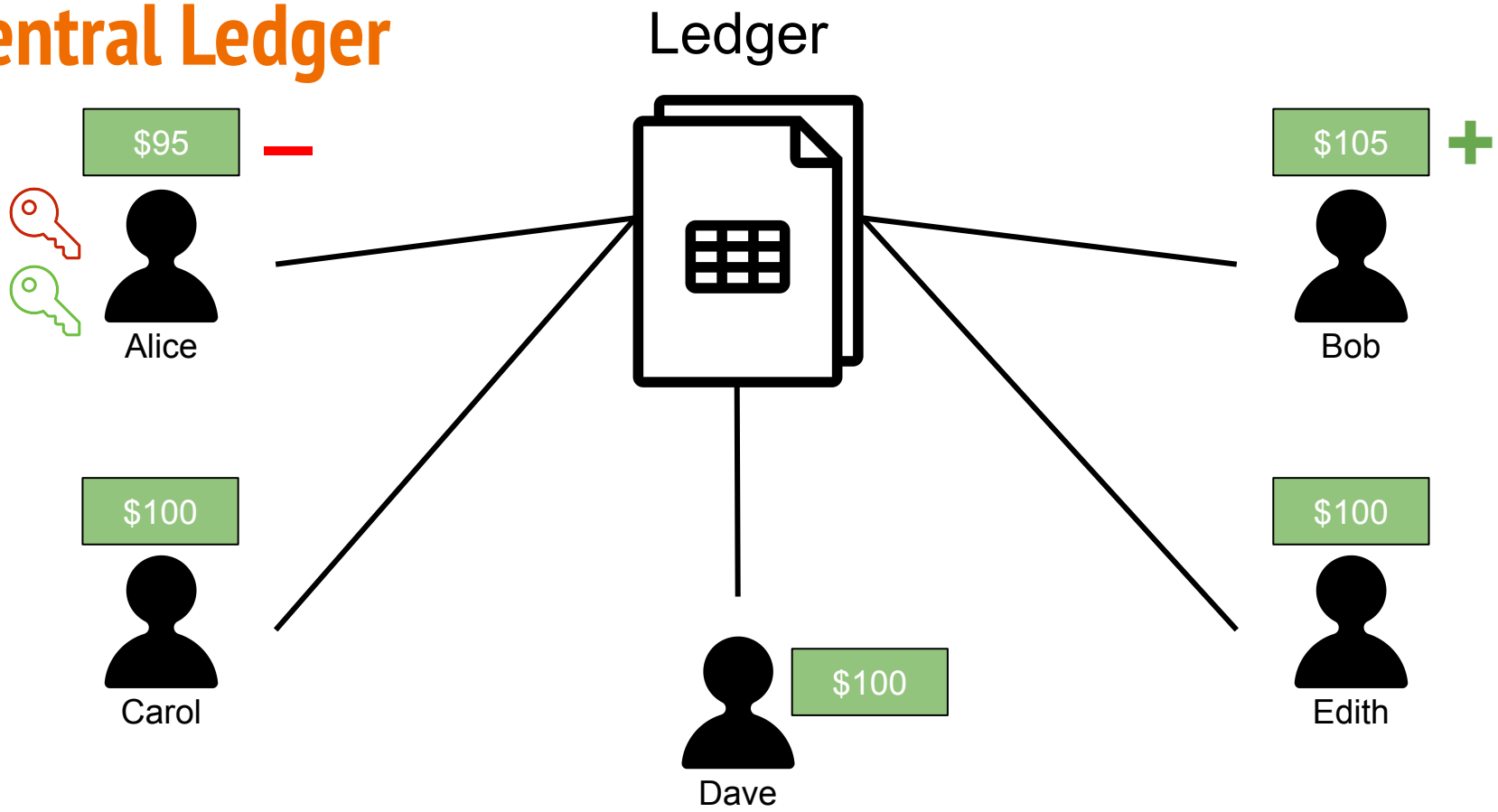

$100
Dave


$100
Edith

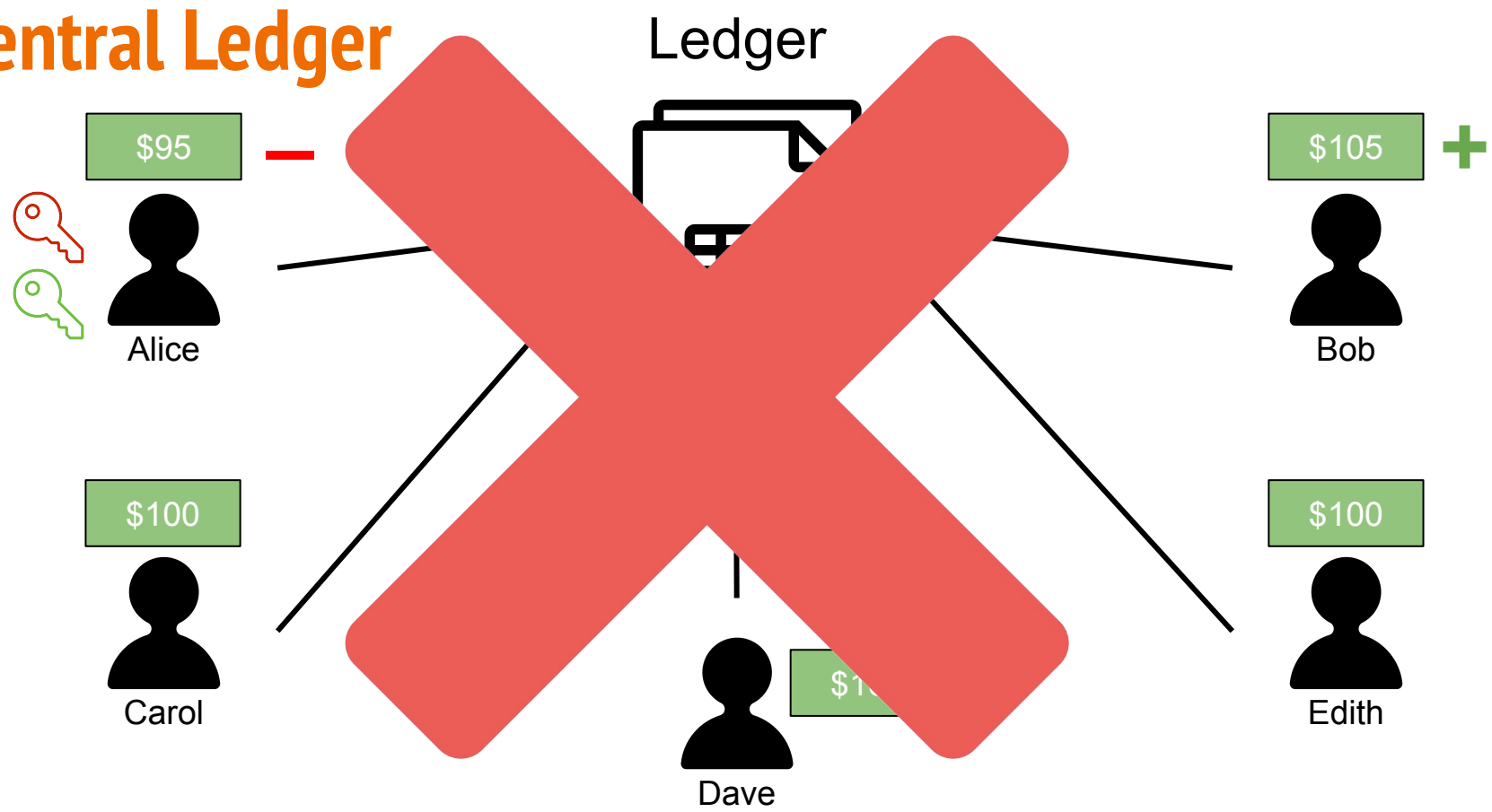
Central Ledger



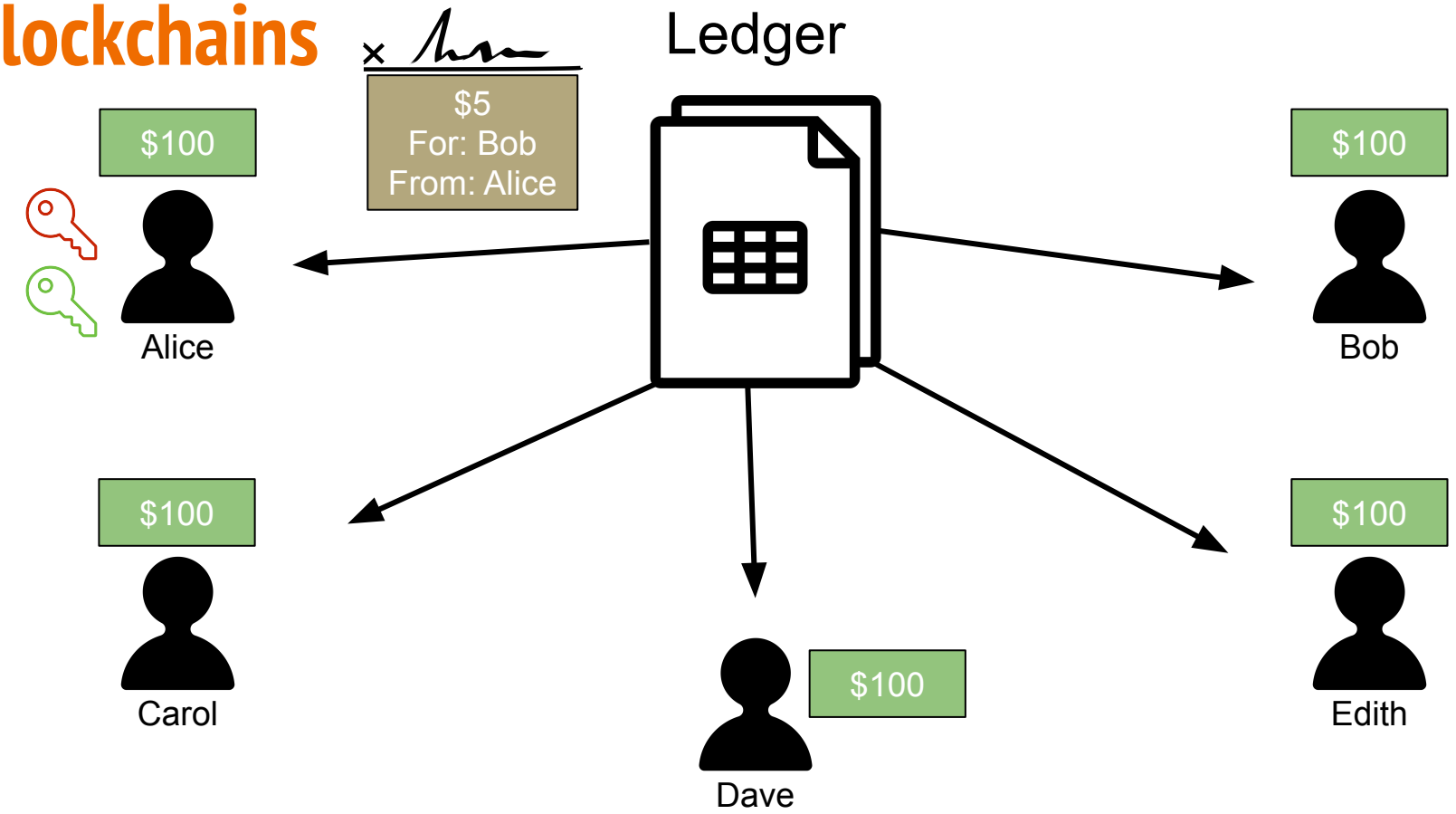
Central Ledger



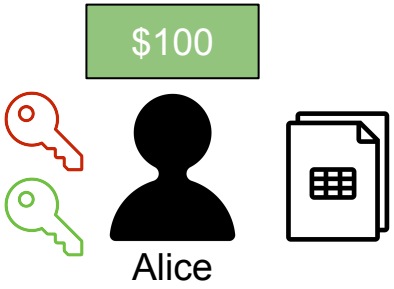
Central Ledger

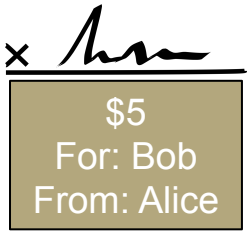


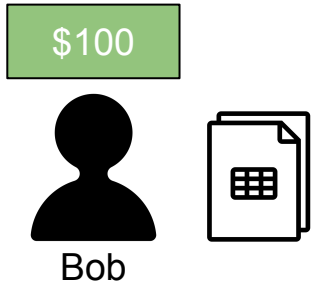
Blockchains

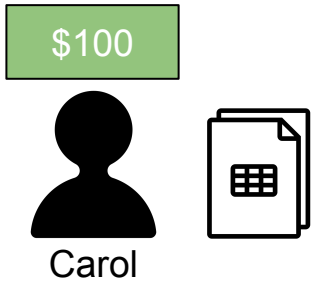


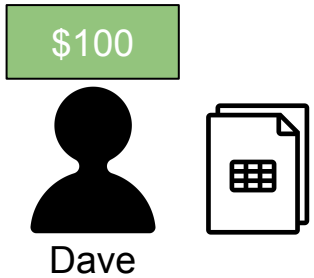
Blockchains

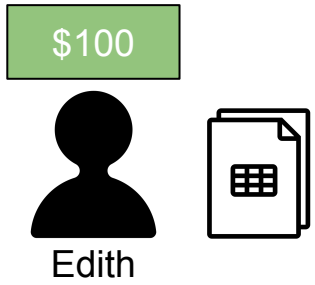




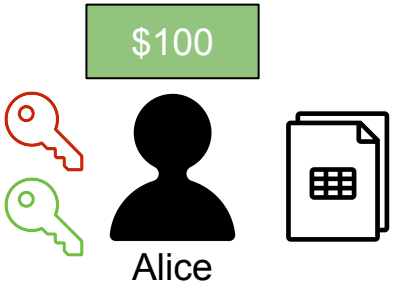


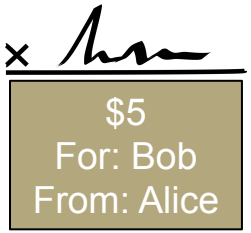


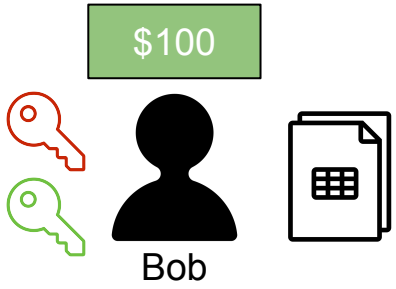


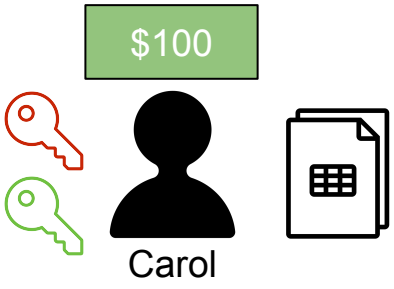


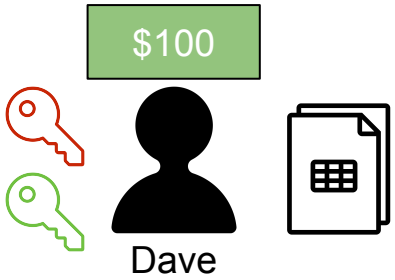
Blockchains

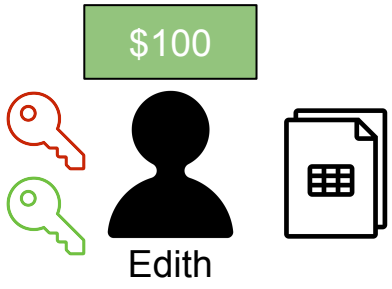




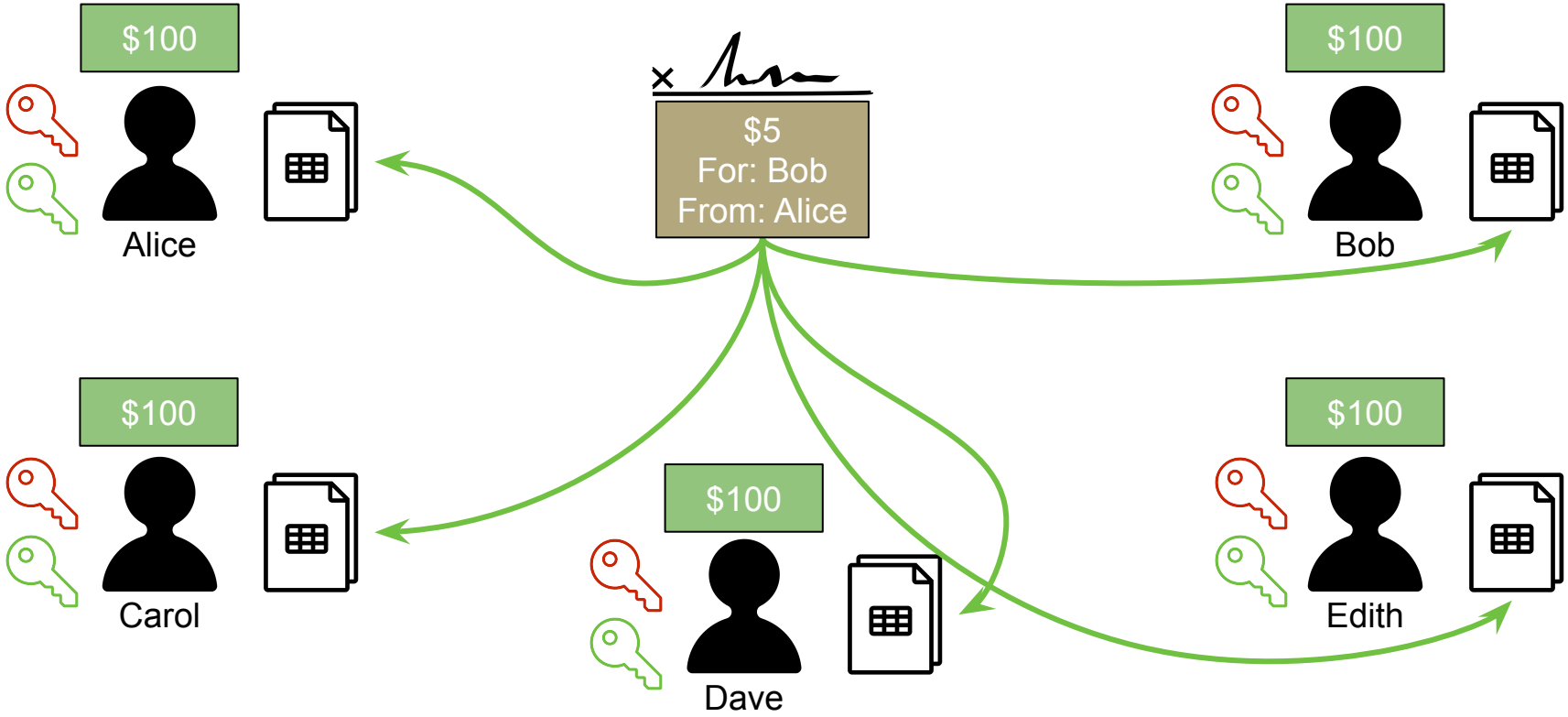




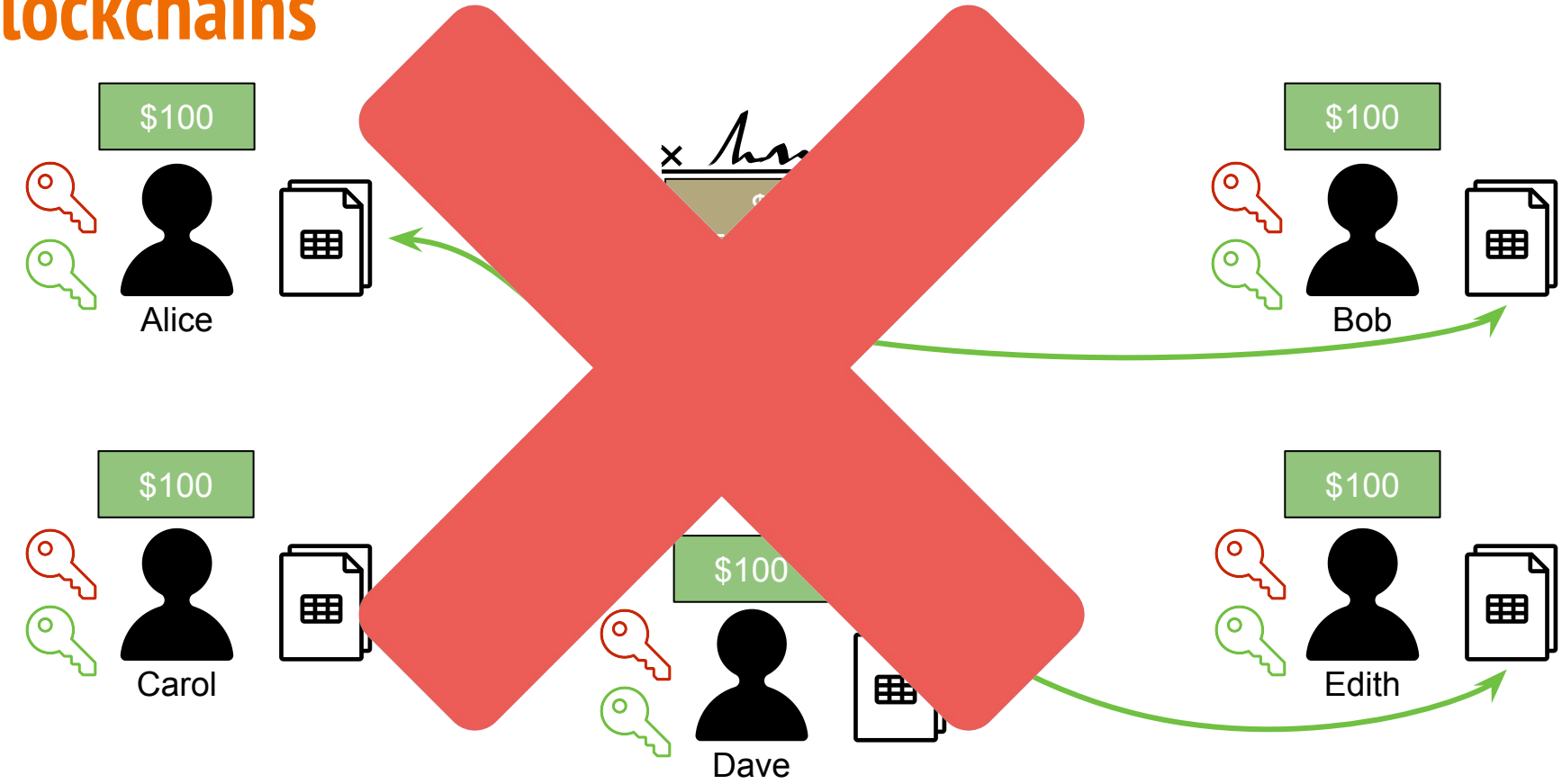




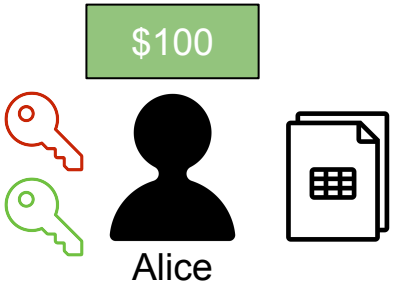
Blockchains: everyone updates on their own asap!

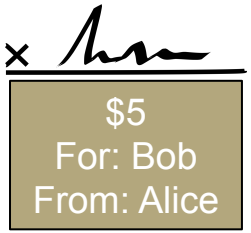


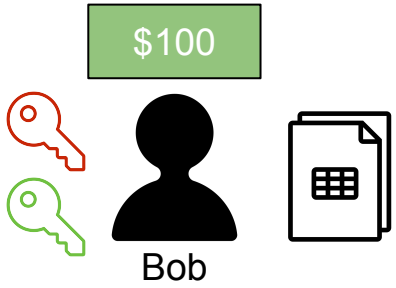
Blockchains

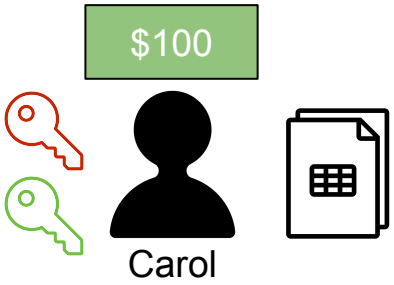


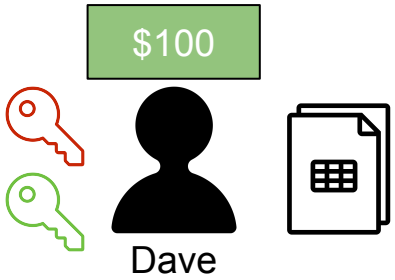
Blockchains: stay in sync with code and NO trust

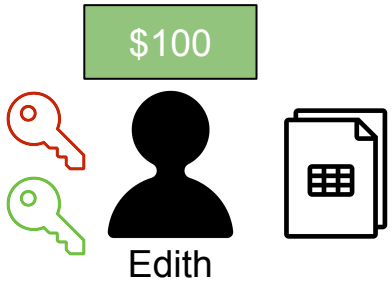




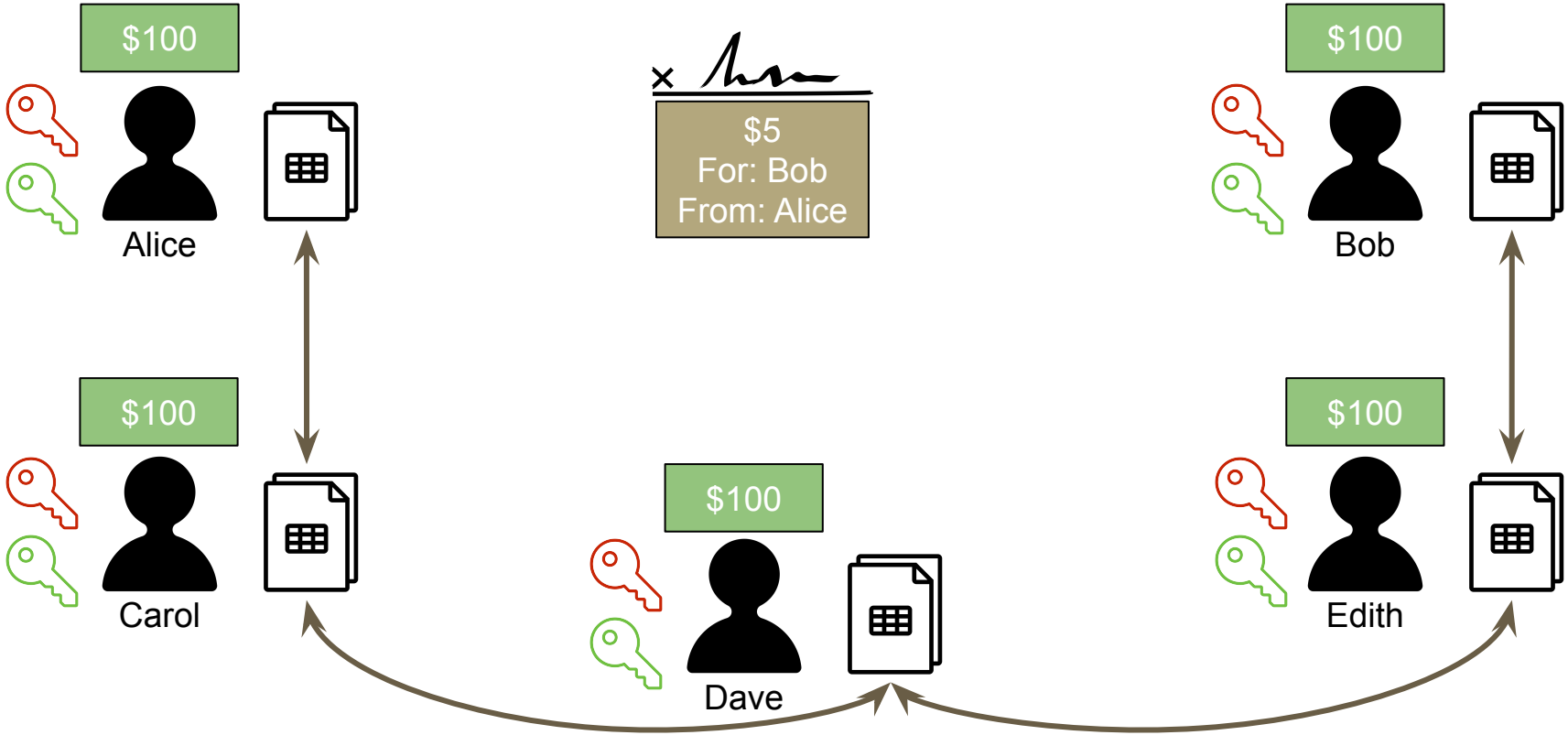








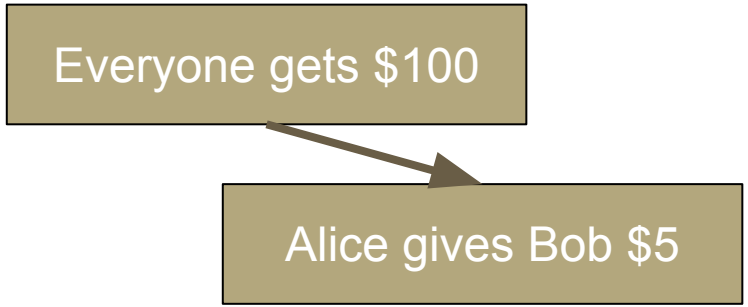
Blockchains: store in blocks chained together



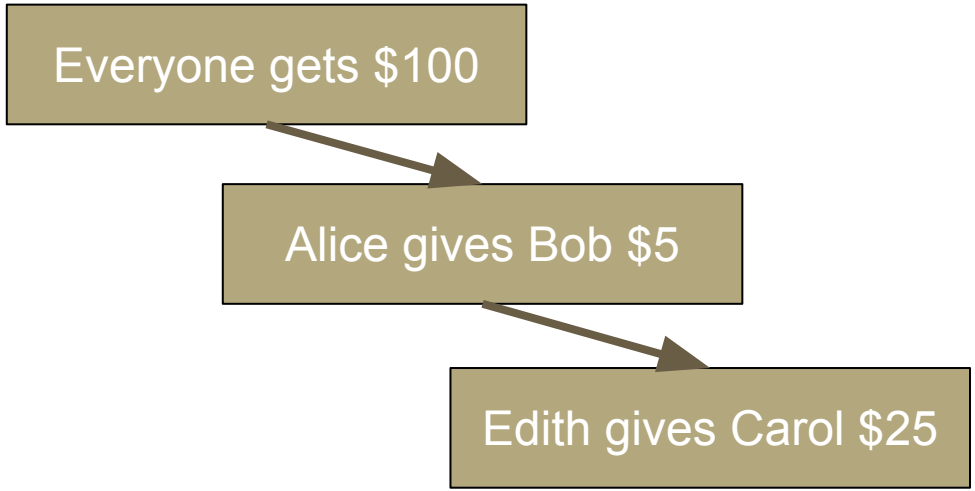
Blockchain: a cryptographically-verifiable Tx chain

Everyone gets $100

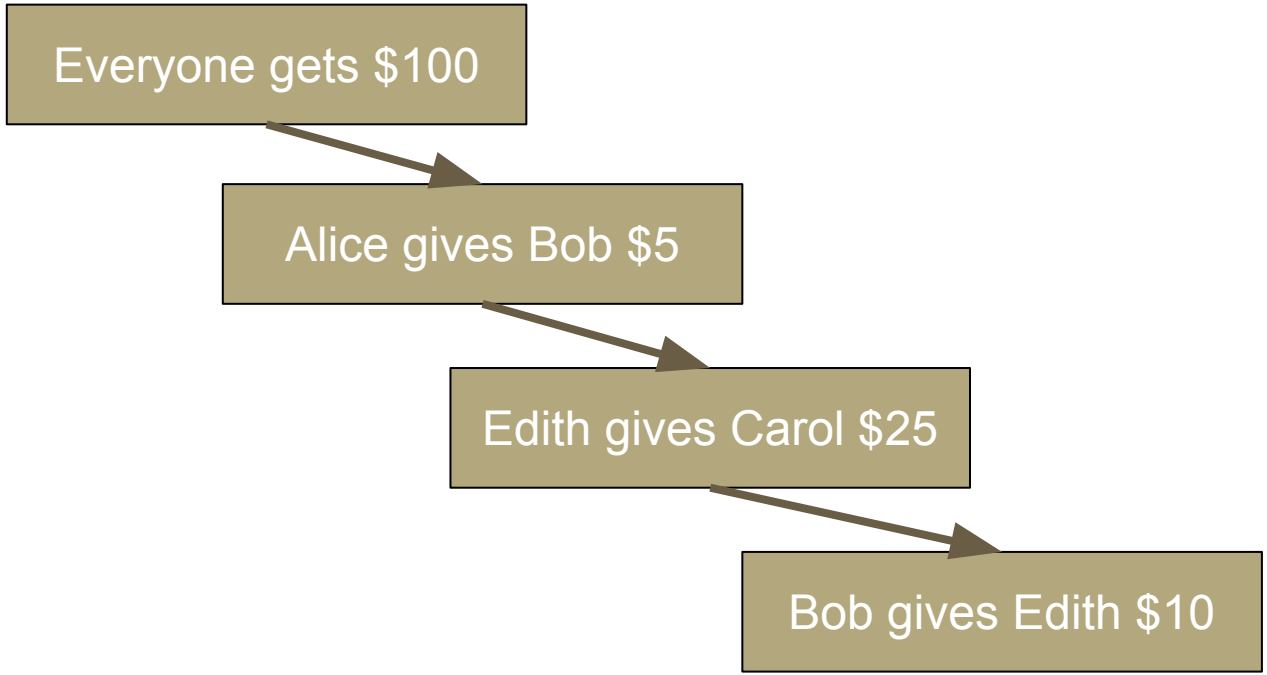
Blockchain: a cryptographically-verifiable Tx chain



Blockchain: a cryptographically-verifiable Tx chain

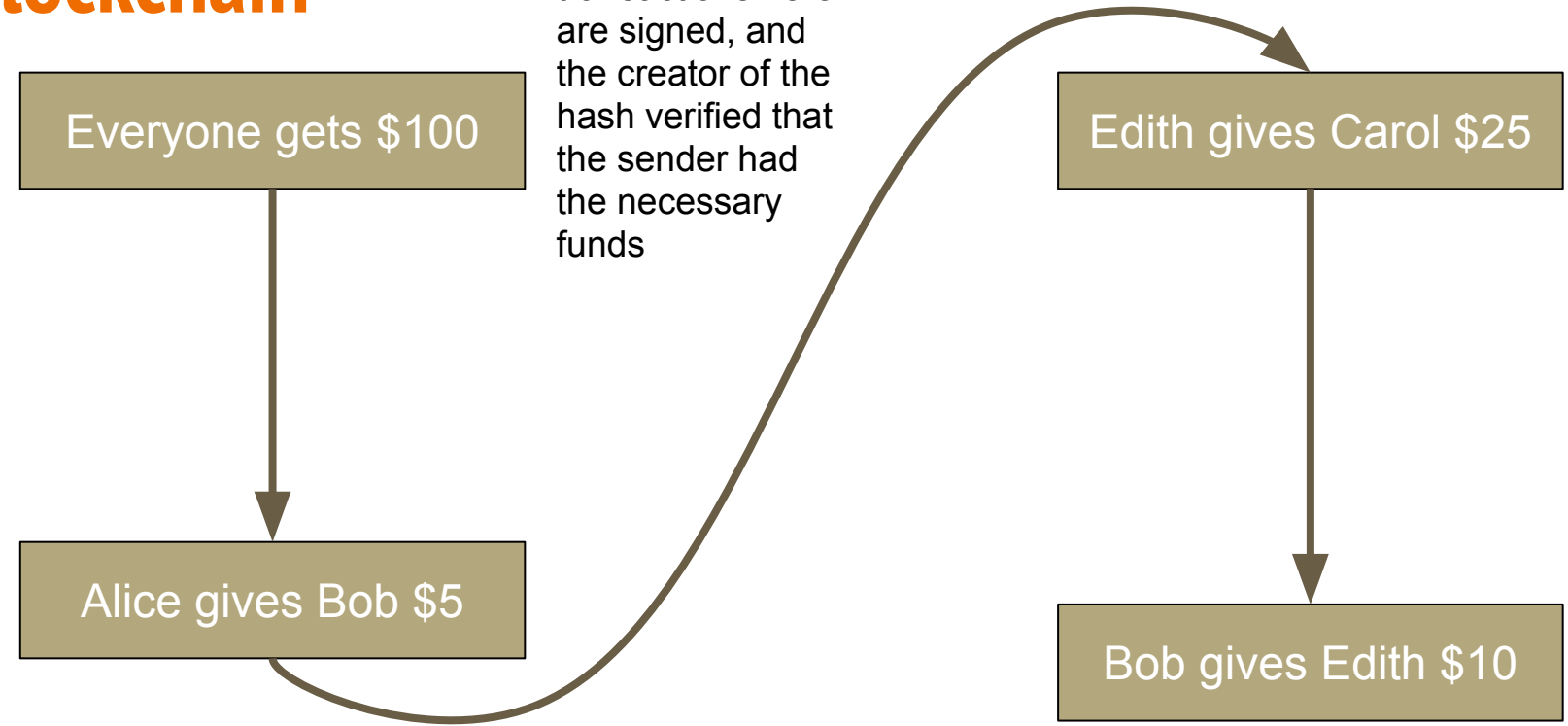


Blockchain: a cryptographically-verifiable Tx chain

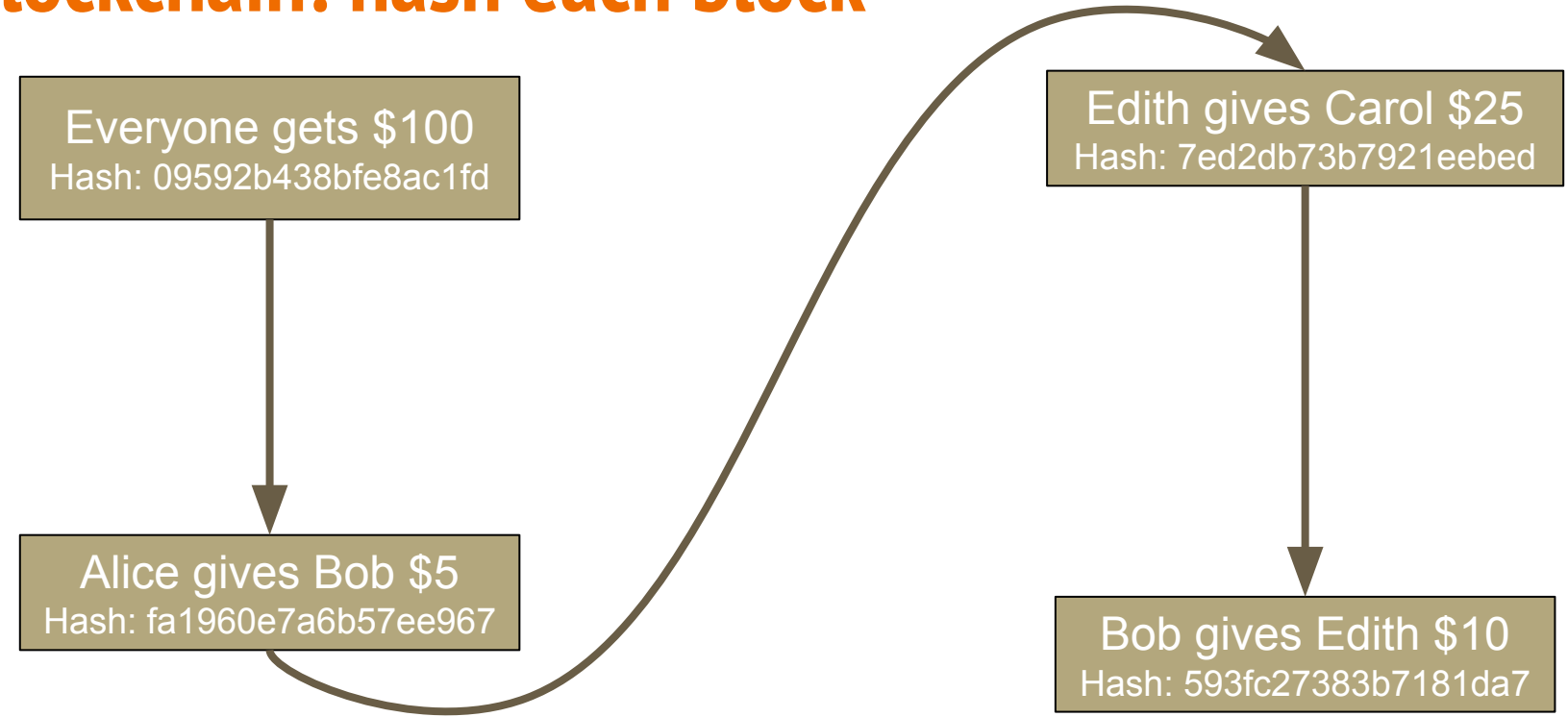


Blockchain

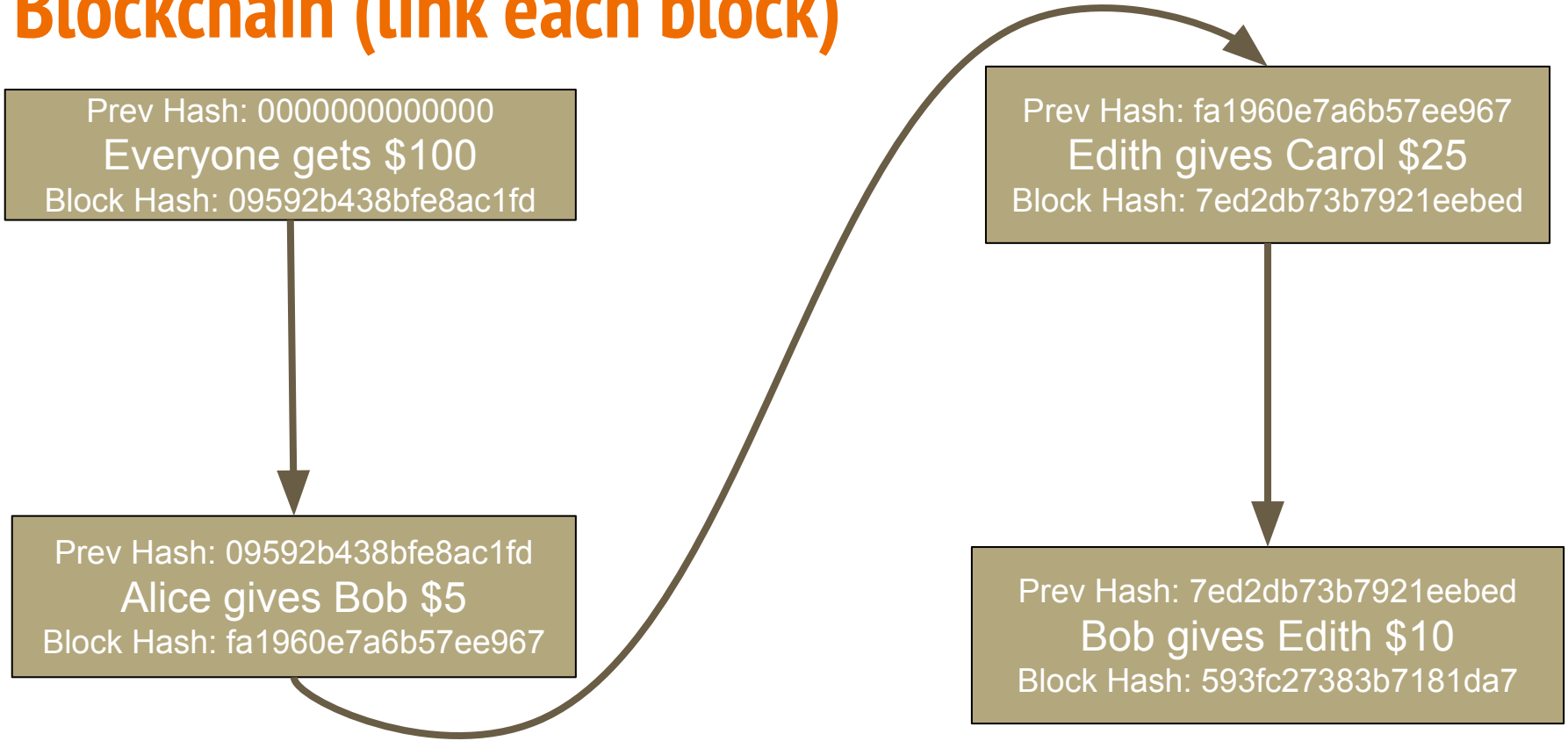
Assume all transactions here are signed, and the creator of the hash verified that the sender had the necessary funds



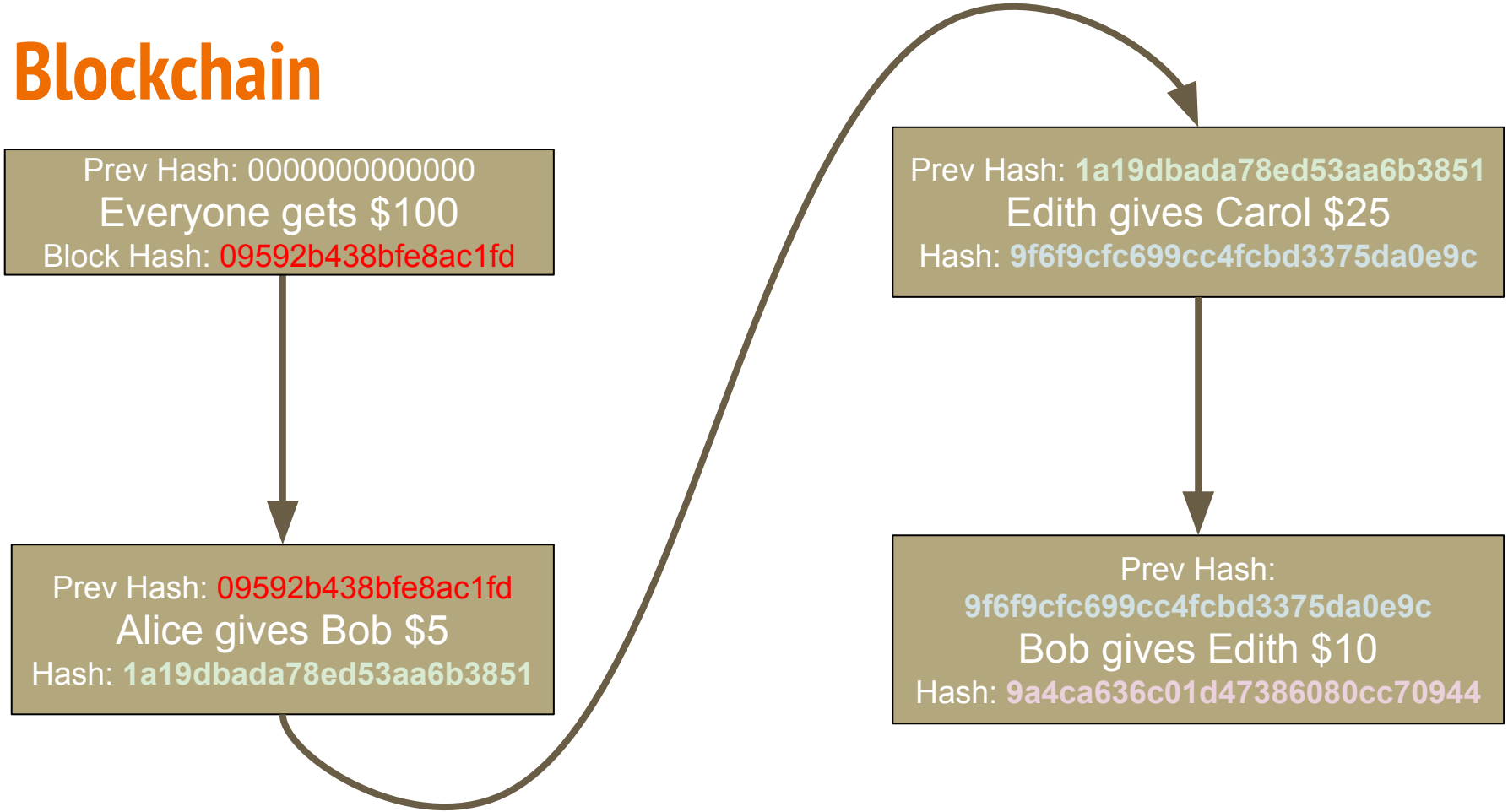
Blockchain: hash each block



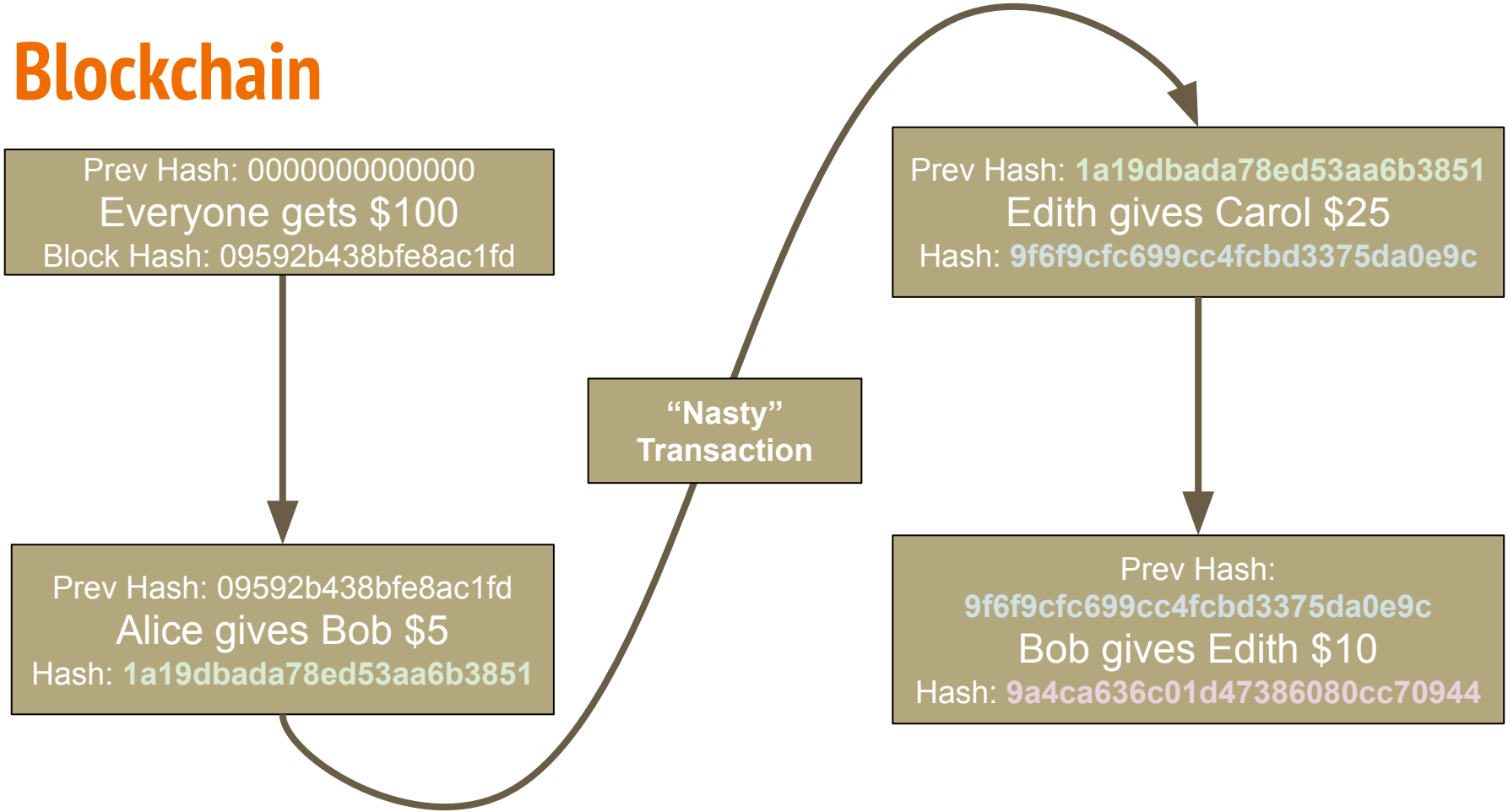
Blockchain (link each block)



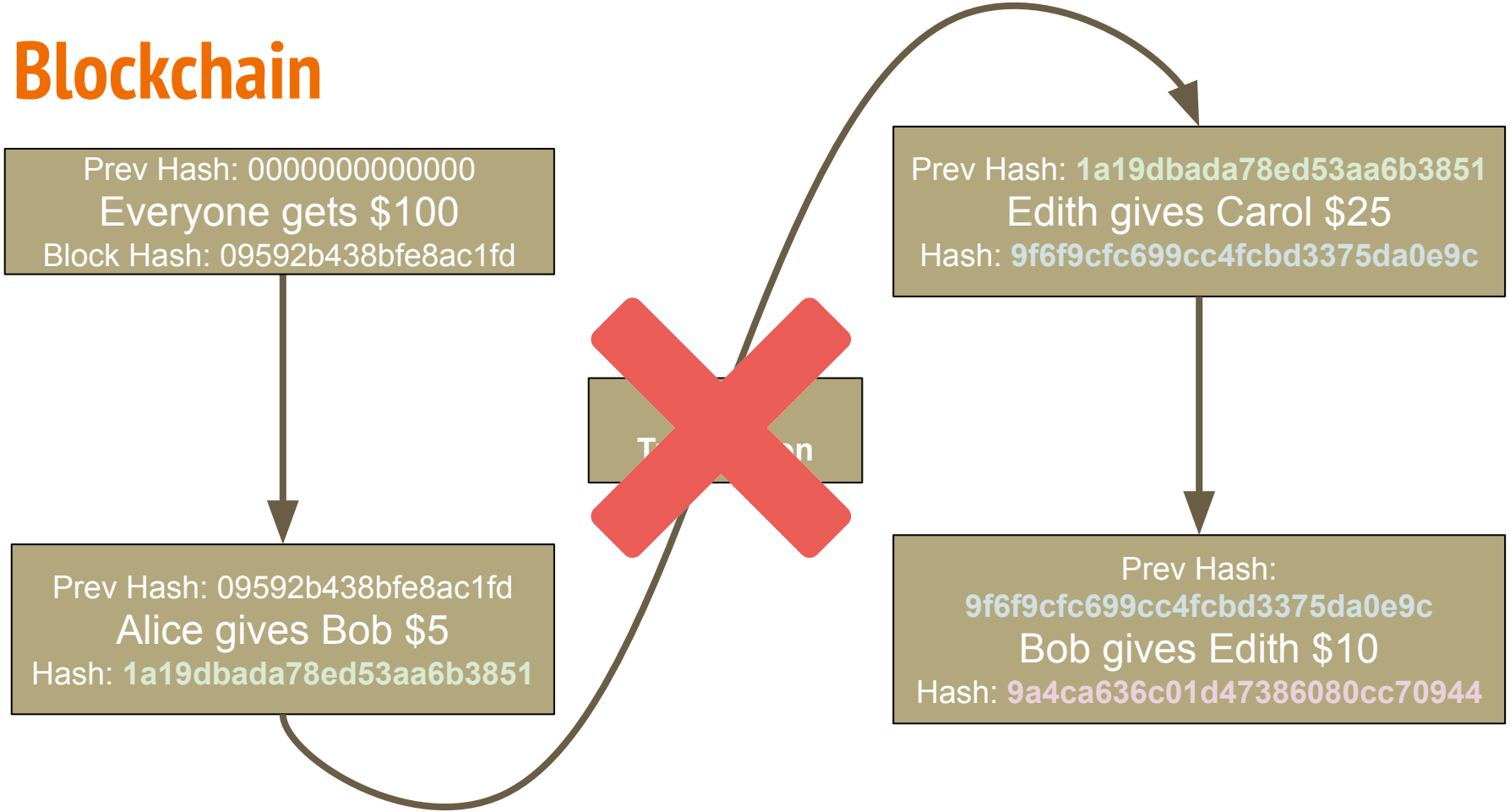
Blockchain


Prev Hash: 0000000000000
Everyone gets $100
Block Hash: 09592b438bfe8ac1fd
Prev Hash: 09592b438bfe8ac1fd
Alice gives Bob $5
Hash: 1a19dbada78ed53aa6b3851
Prev Hash: 1a19dbada78ed53aa6b3851
Edith gives Carol $25
Hash: 9f6f9cfc699cc4fcbd3375da0e9c
Prev Hash:
9f6f9cfc699cc4fcbd3375da0e9c
Bob gives Edith $10
Hash: 9a4ca636c01d47386080cc70944

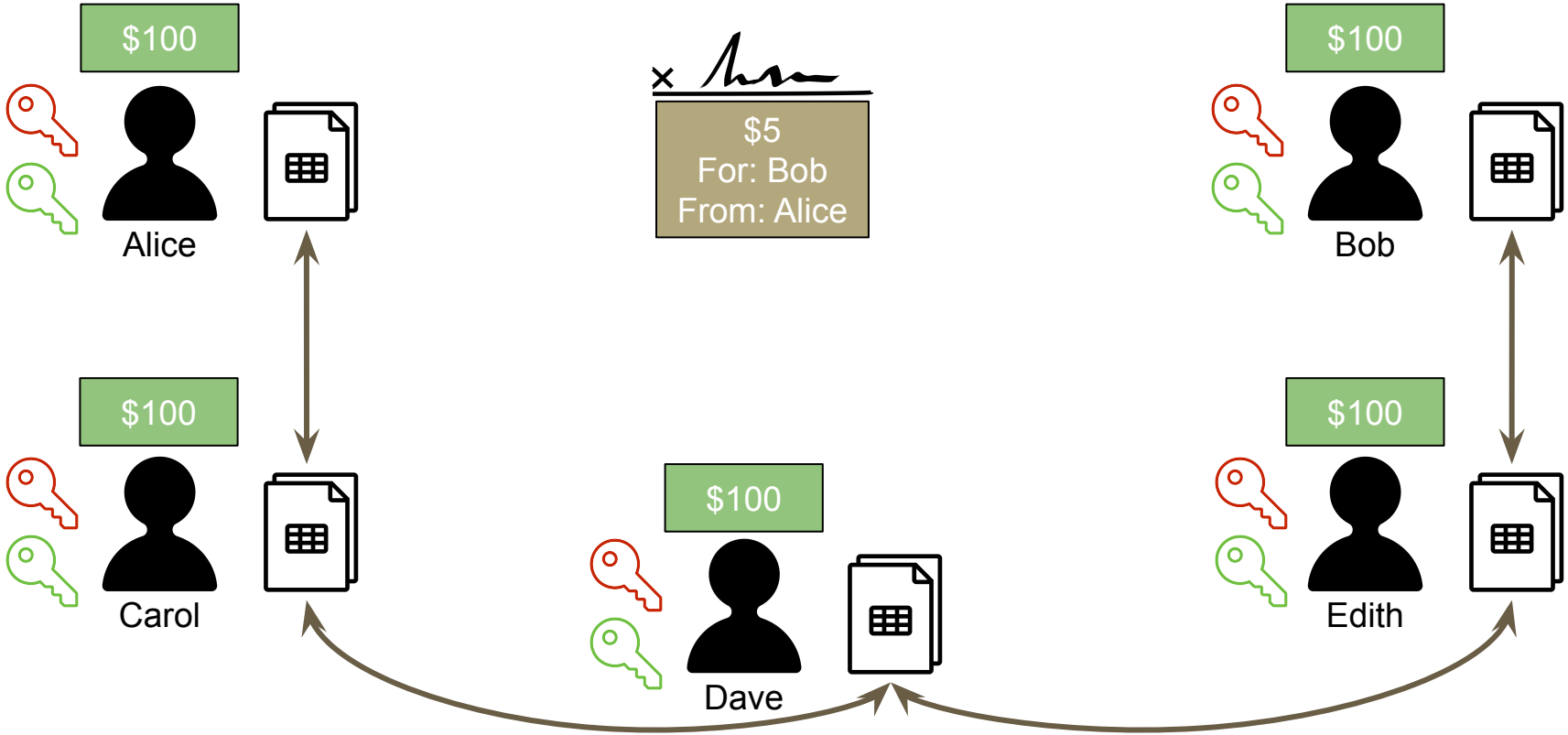
Blockchain


Prev Hash: 0000000000000
Everyone gets $100
Block Hash: 09592b438bfe8ac1fd
Prev Hash: 09592b438bfe8ac1fd
Alice gives Bob $5
Hash: 1a19dbada78ed53aa6b3851
"Nasty" Transaction
Prev Hash: 1a19dbada78ed53aa6b3851
Edith gives Carol $25
Hash: 9f6f9cfc699cc4fcbd3375da0e9c
Prev Hash: 9f6f9cfc699cc4fcbd3375da0e9c
Bob gives Edith $10
Hash: 9a4ca636c01d47386080cc70944

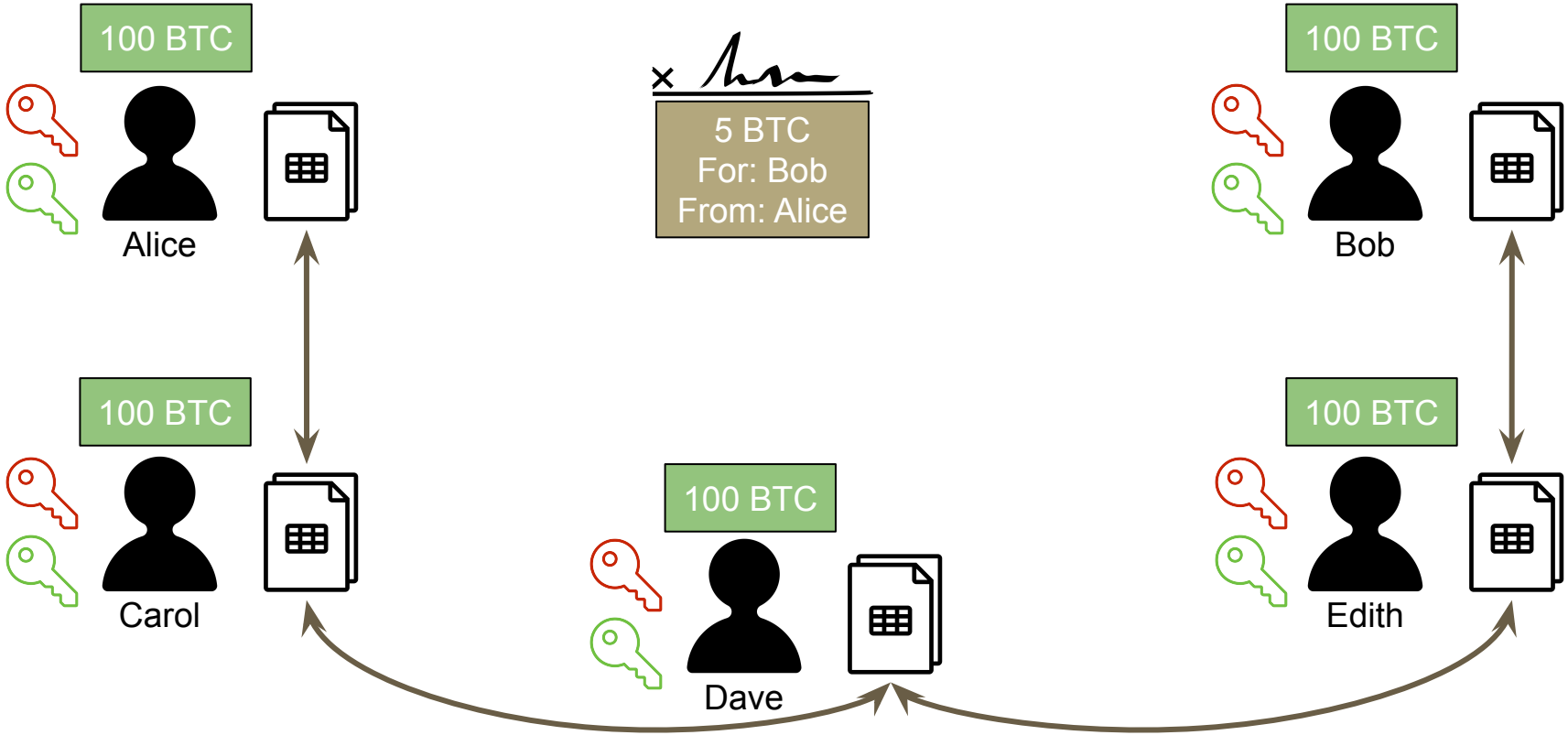
Blockchain


Prev Hash: 0000000000000
Everyone gets $100
Block Hash: 09592b438bfe8ac1fd
Prev Hash: 09592b438bfe8ac1fd
Alice gives Bob $5
Hash: 1a19dbada78ed53aa6b3851
Prev Hash: 1a19dbada78ed53aa6b3851
Edith gives Carol $25
Hash: 9f6f9cfc699cc4fcbd3375da0e9c
Prev Hash:
9f6f9cfc699cc4fcbd3375da0e9c
Bob gives Edith $10
Hash: 9a4ca636c01d47386080cc70944

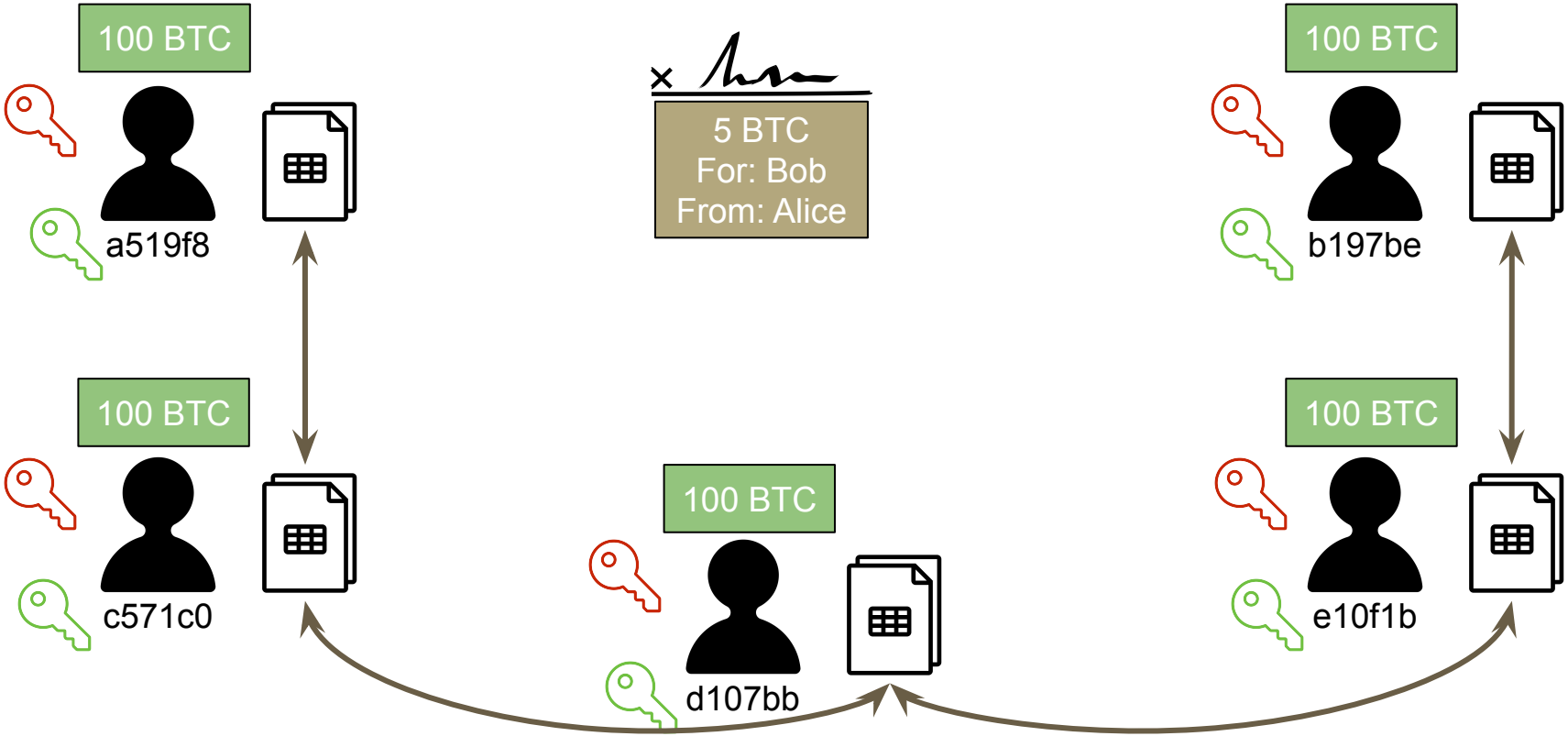
Bitcoin: a shared Blockchain (cooperative)



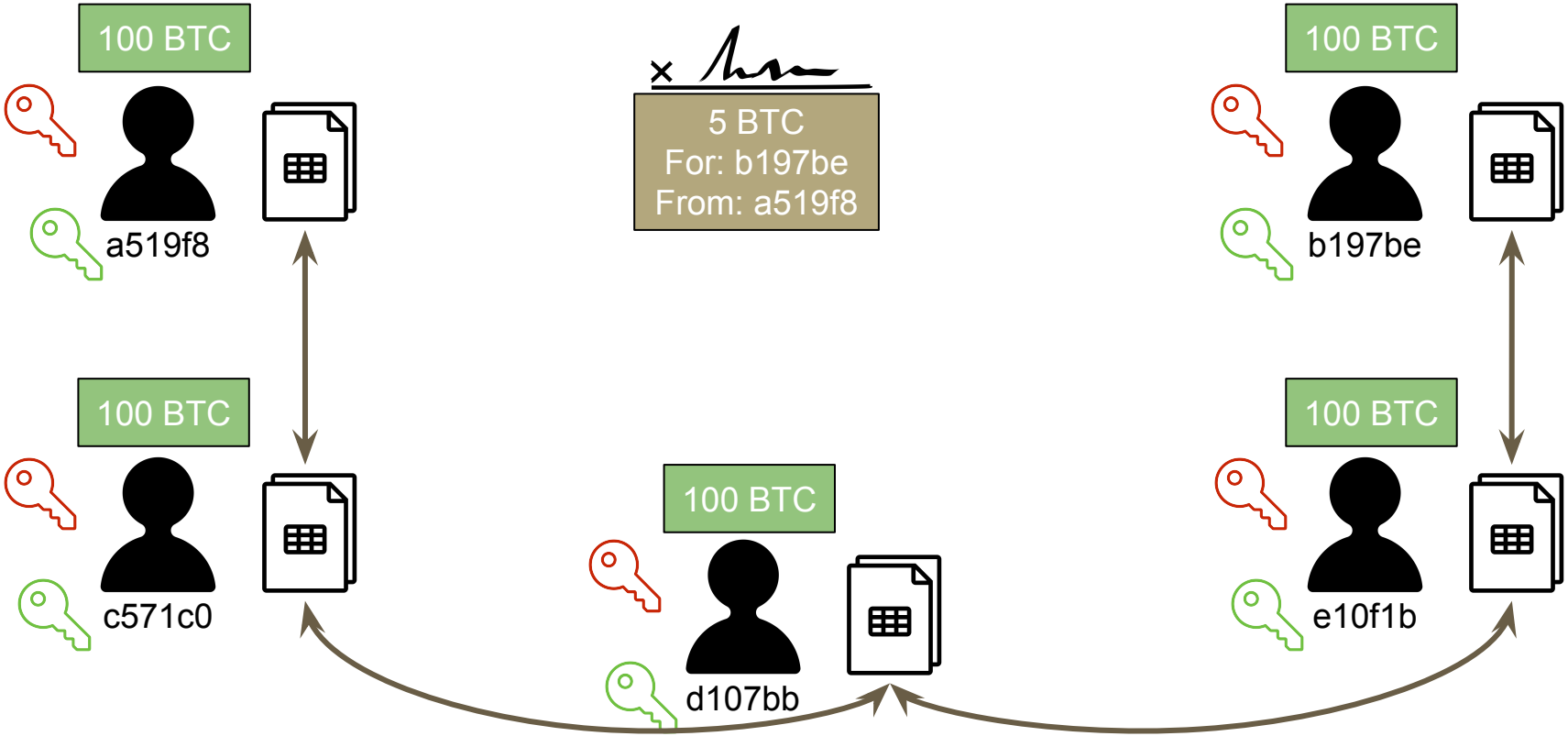
Bitcoin: change USD to Bitcoin



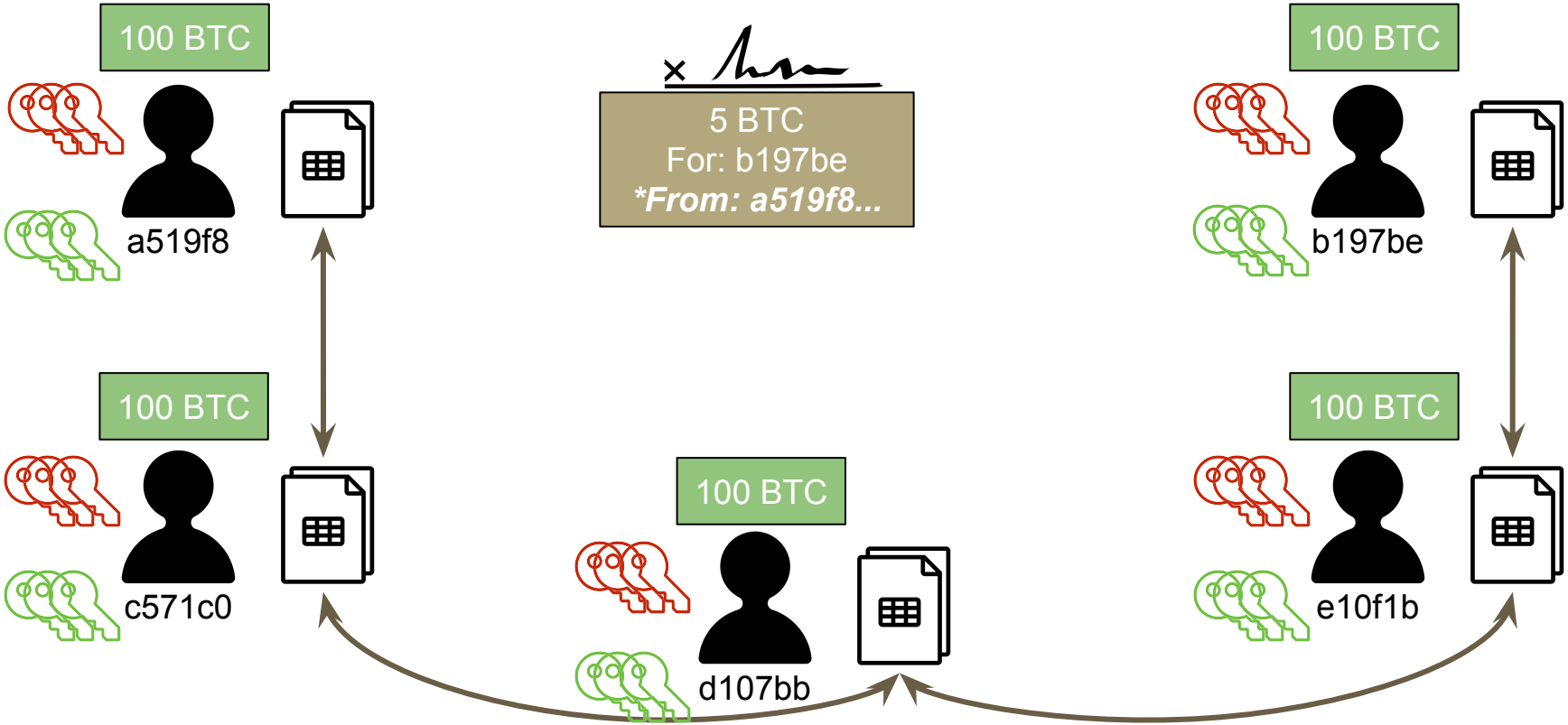
Bitcoin: no names, just (public) keys



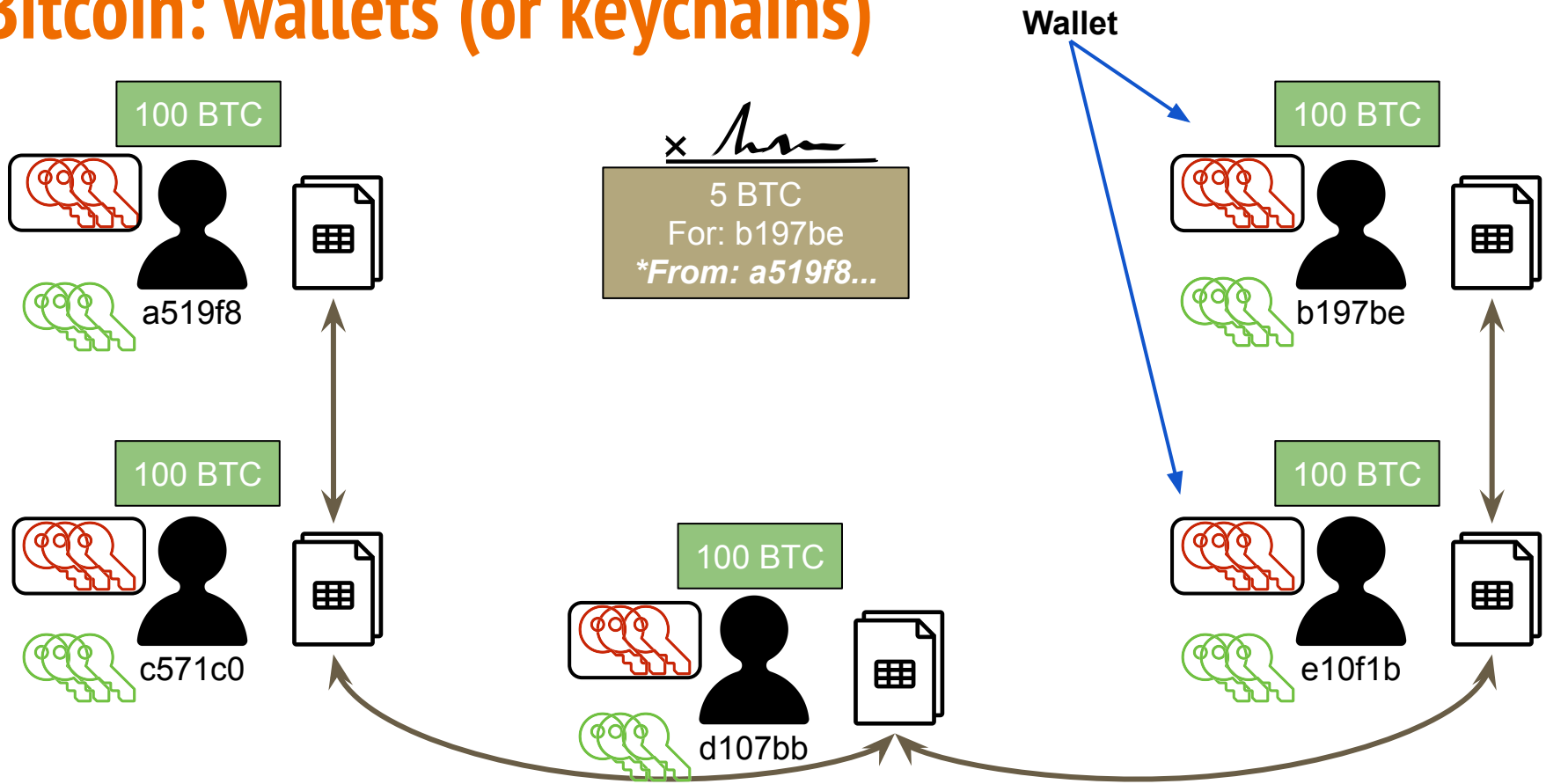
Bitcoin: keys also on the Tx's, no names



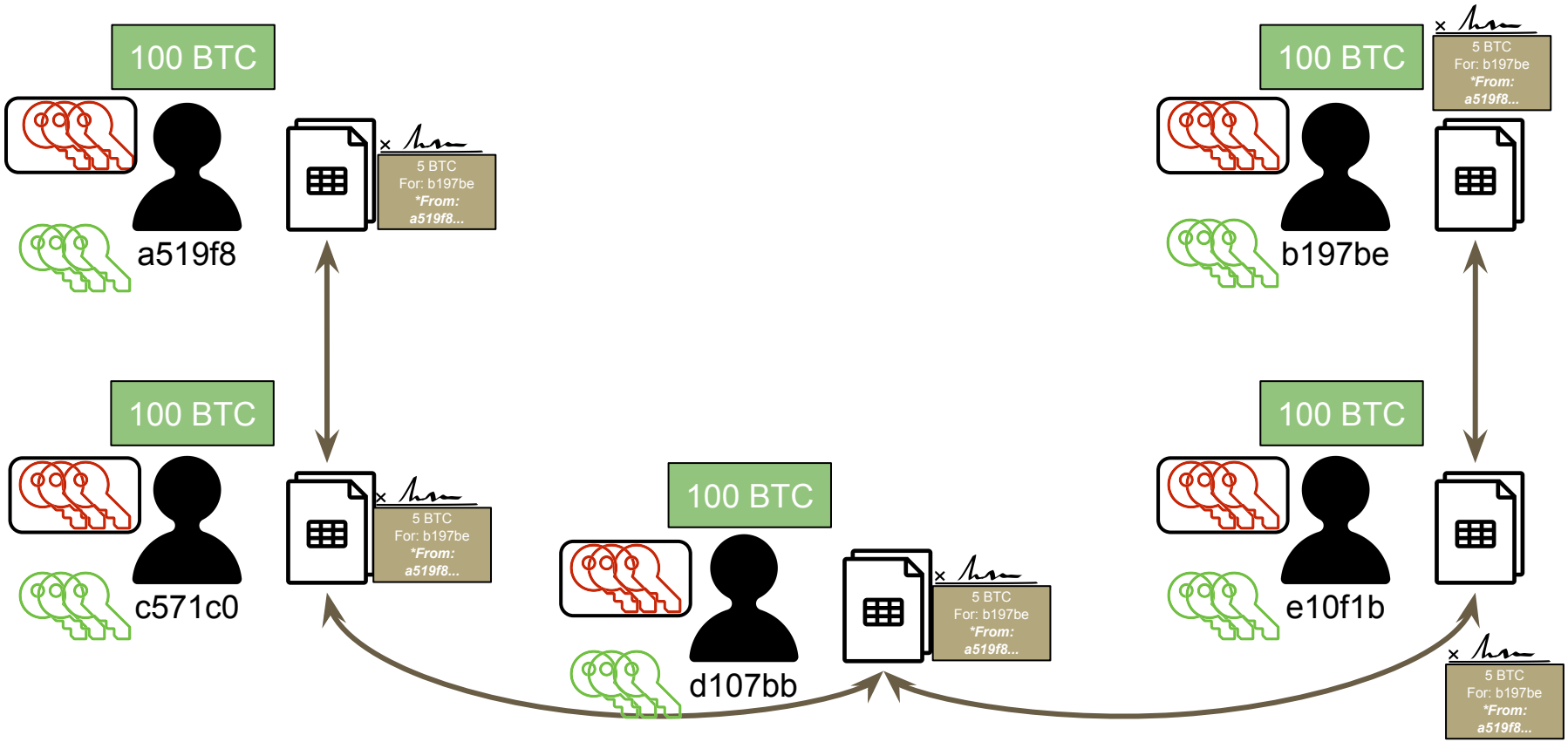
Bitcoin: multiple keys are allowed



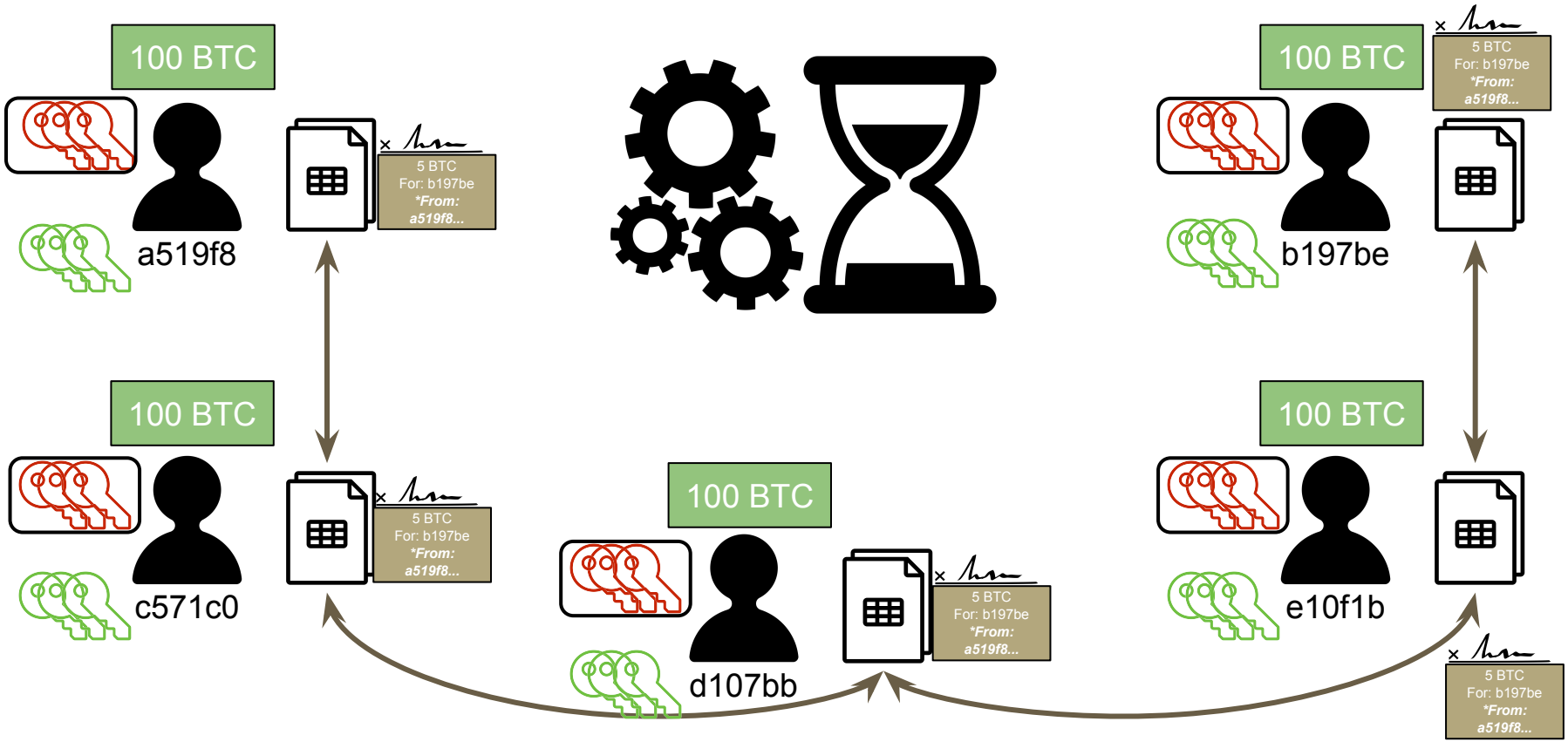
Bitcoin: wallets (or keychains)

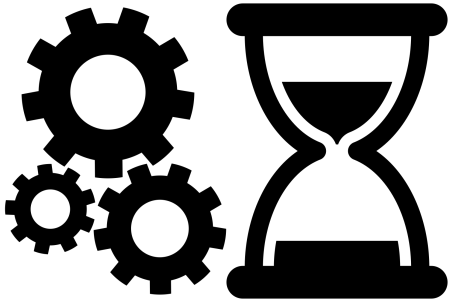


Bitcoin: cryptographic puzzle



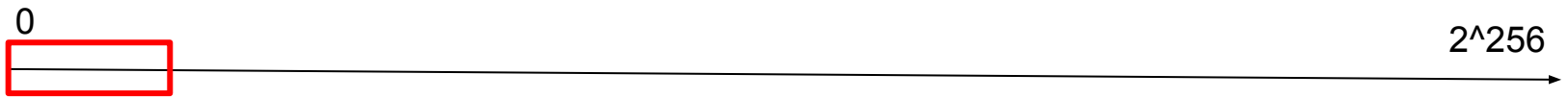
Bitcoin: “computational puzzle”





What is this “computational puzzle” (proof-of-work)?!

SHA-256 Hash



$$\left(\frac{1}{16}\right) \times 2^{256}$$

```
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000001
0000000000000000000000000000000000000000000000000000000000000002
0000000000000000000000000000000000000000000000000000000000000009
000000000000000000000000000000000000000000000000000000000000000a
000000000000000000000000000000000000000000000000000000000000000b
000000000000000000000000000000000000000000000000000000000000000f
0000000000000000000000000000000000000000000000000000000000000010
03b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
1000000000000000000000000000000000000000000000000000000000000000
```

Demo

The Bitcoin “Puzzle”

5 BTC
For: b197be
From: a519f8...

The Bitcoin “Puzzle”

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8...

The Bitcoin “Puzzle”

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…

Hash: ----------

The Bitcoin “Puzzle”

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce:
Nonce Solver:
Hash: ----------

The Bitcoin "Puzzle"

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce:
Nonce Solver:
Hash: ----------

Puzzle Solution

Puzzle Solver (miner)

The Bitcoin "Puzzle"

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce:
Nonce Solver:
Hash: ----------

Puzzle Solution

Puzzle Solver

Must be below certain value, say one leading zero

The Bitcoin "Puzzle": example of how miners mine

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 0
Nonce Solver: a519f8 (Alice)
Hash: a166137346cd32e73e

Puzzle Solution

Puzzle Solver

Must be below certain value

The Bitcoin "Puzzle"

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 1
Nonce Solver: b197be (Bob)
Hash: d59910db074b35fa9d

Puzzle Solution

Puzzle Solver

Must be below certain value

The Bitcoin "Puzzle"

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 2
Nonce Solver: c571c0 (Carol)
Hash: 4c274d79254f259960a

Puzzle Solution

Puzzle Solver

Must be below certain value

The Bitcoin "Puzzle"

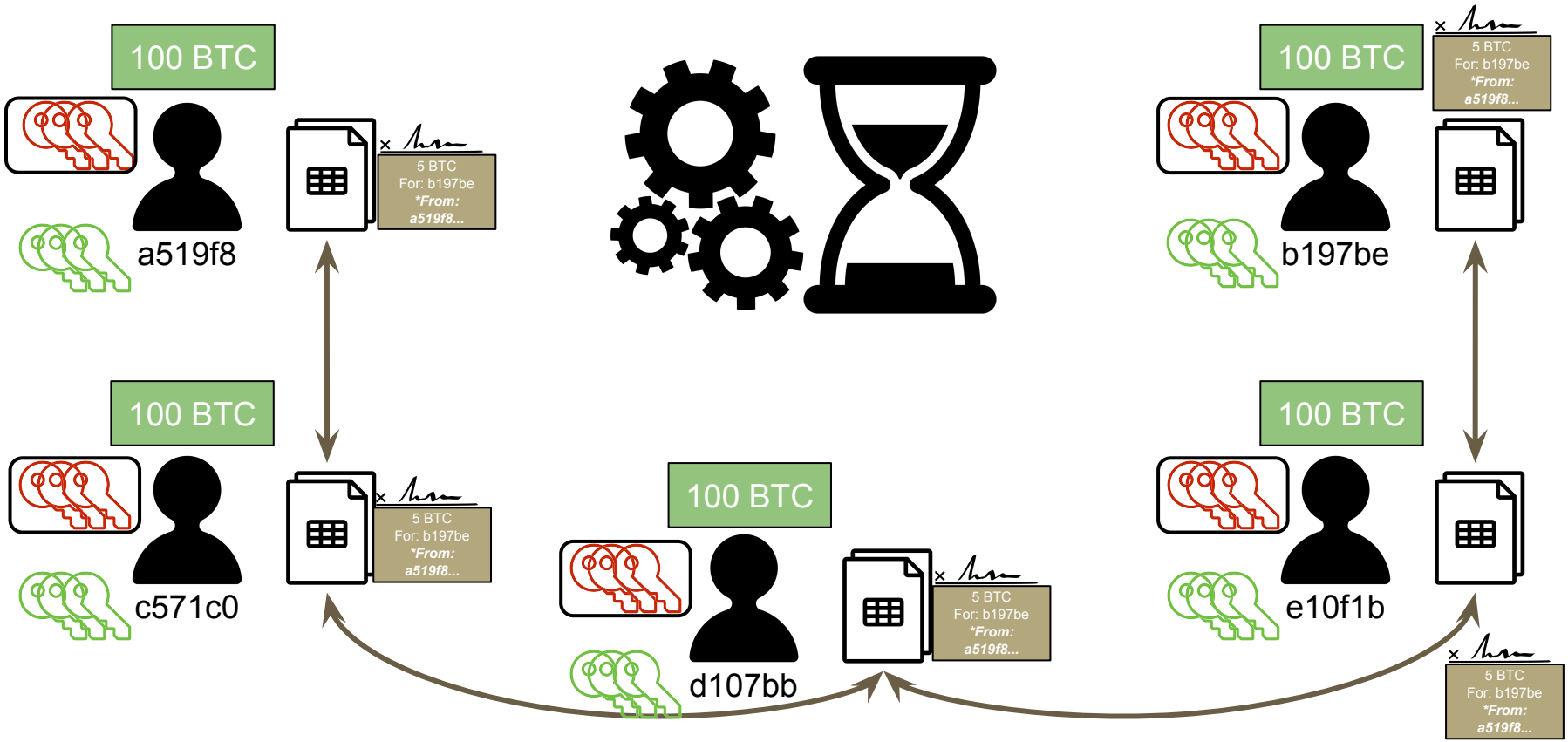
Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: **03a419ef573a846f**

Puzzle Solution

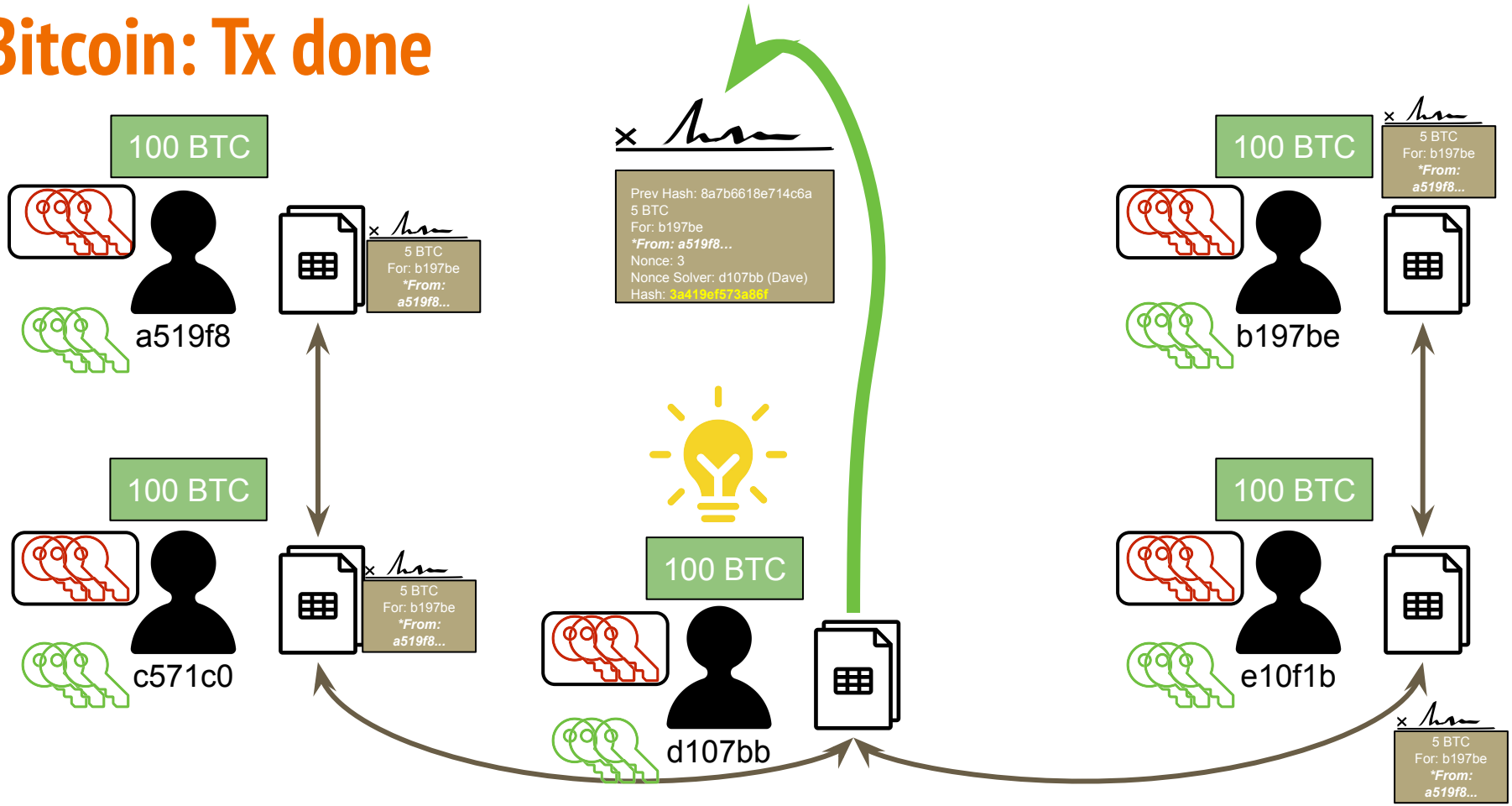
Puzzle Solver

Must be below certain value

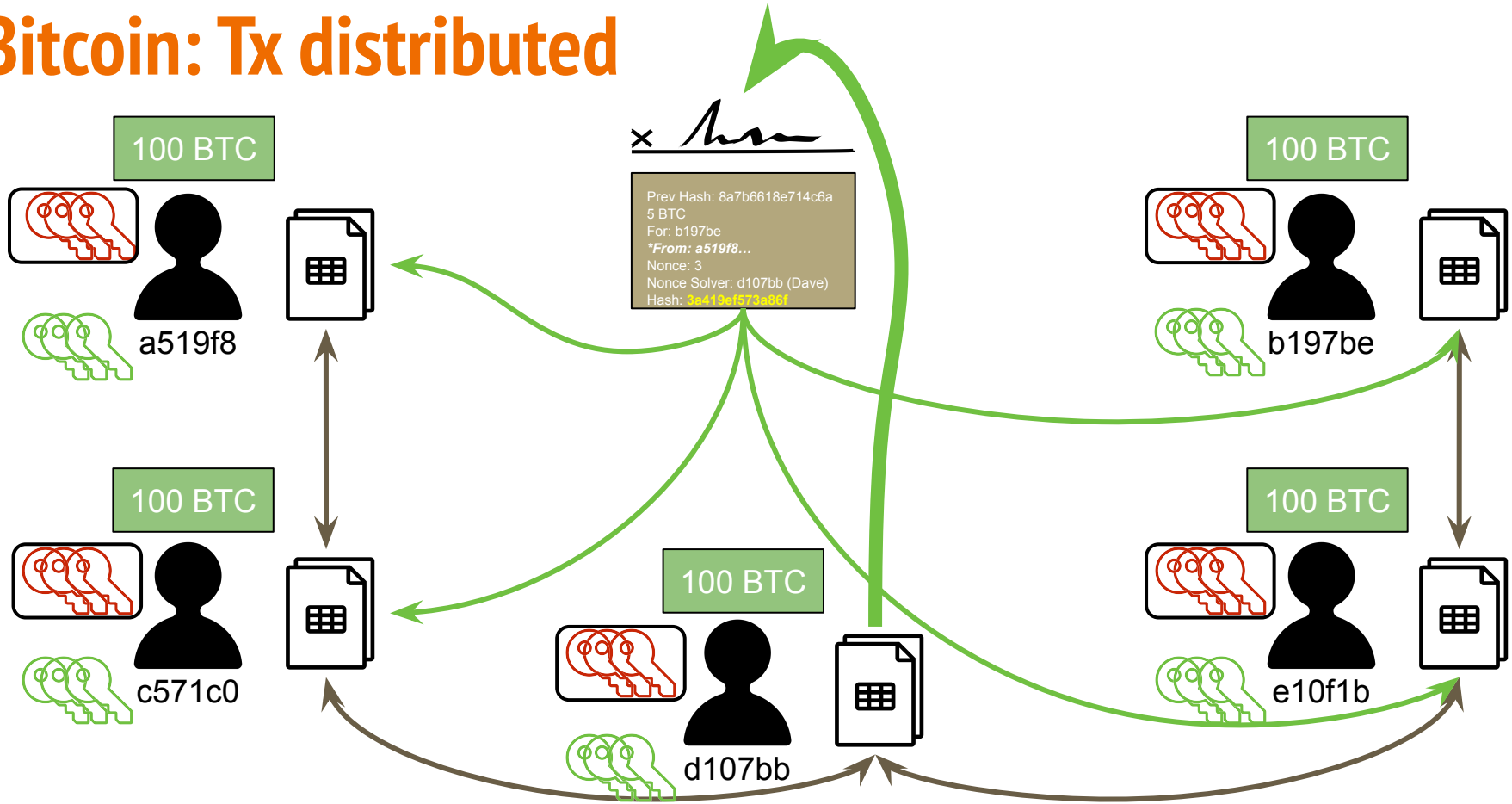
Bitcoin


100 BTC
a519f8
5 BTC
For: b197be
*From:
a519f8...
100 BTC
c571c0
5 BTC
For: b197be
*From:
a519f8...
100 BTC
d107bb
5 BTC
For: b197be
*From:
a519f8...
100 BTC
b197be
5 BTC
For: b197be
*From:
a519f8...
100 BTC
e10f1b
5 BTC
For: b197be
*From:
a519f8...

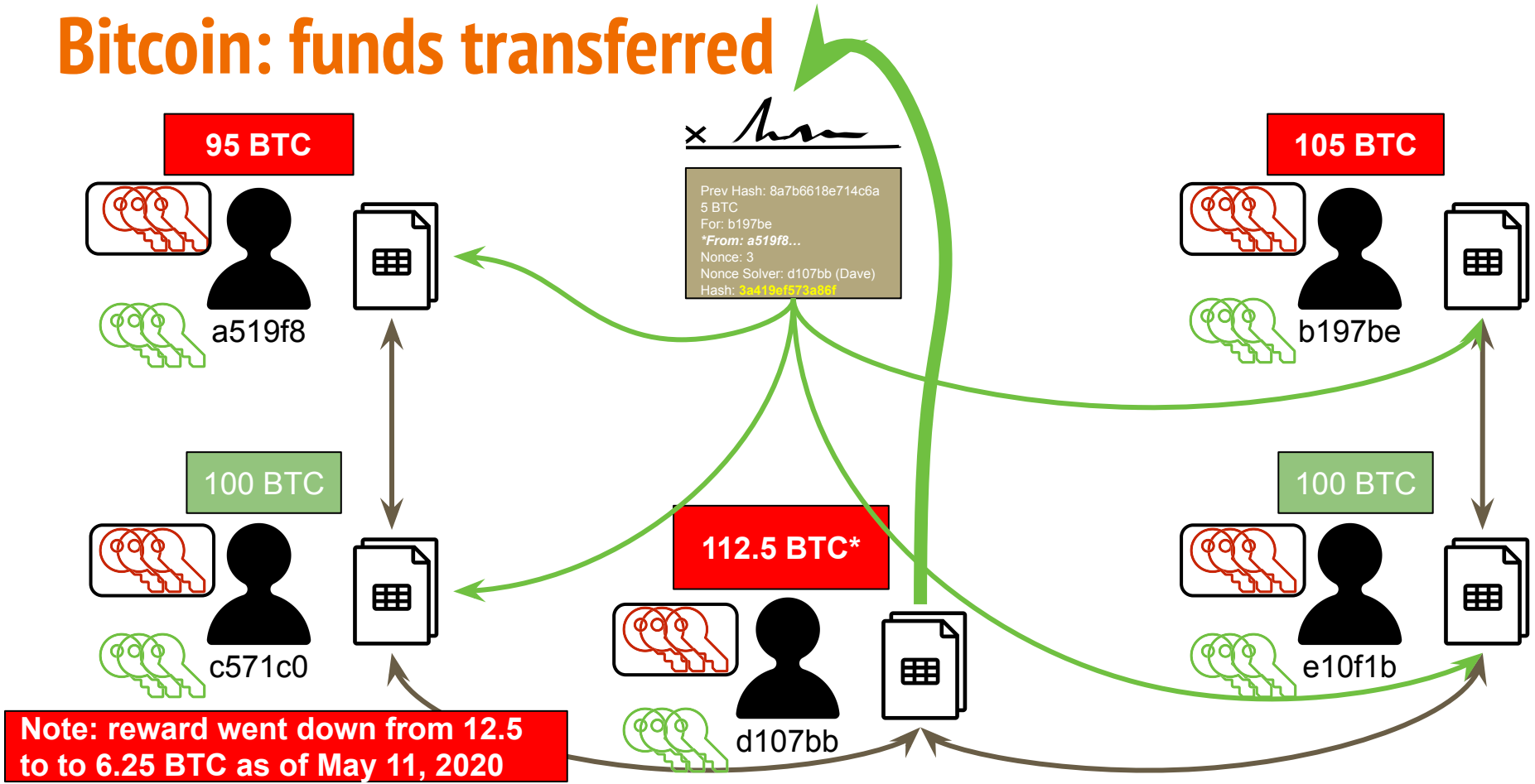
Bitcoin: Tx done



Bitcoin: Tx distributed



Bitcoin: funds transferred



The Bitcoin “Puzzle”: can you steal the nonce?

Puzzle Solution - nonce depends on solver too

Puzzle Solver

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: **03a419ef573a86f**

Must be below certain value

The Bitcoin "Puzzle": nonce is block-specific

Prev Hash: 8a7b6618e714c6a

5 BTC

For: b197be

From: a519f8…

Nonce: 3

Nonce Solver: d107bb (Dave)

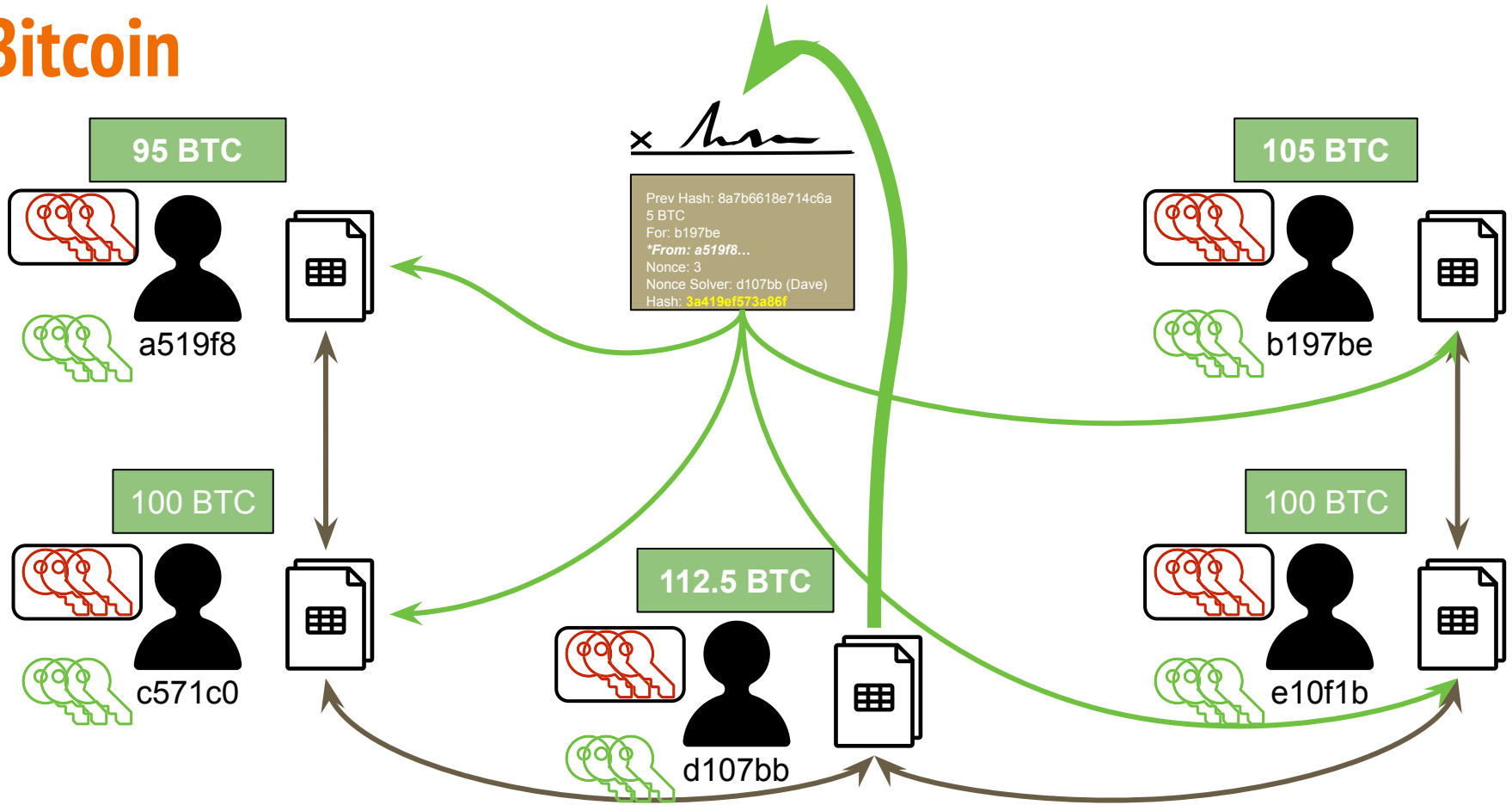
Hash: **03a419ef573a86f**

Puzzle Solution

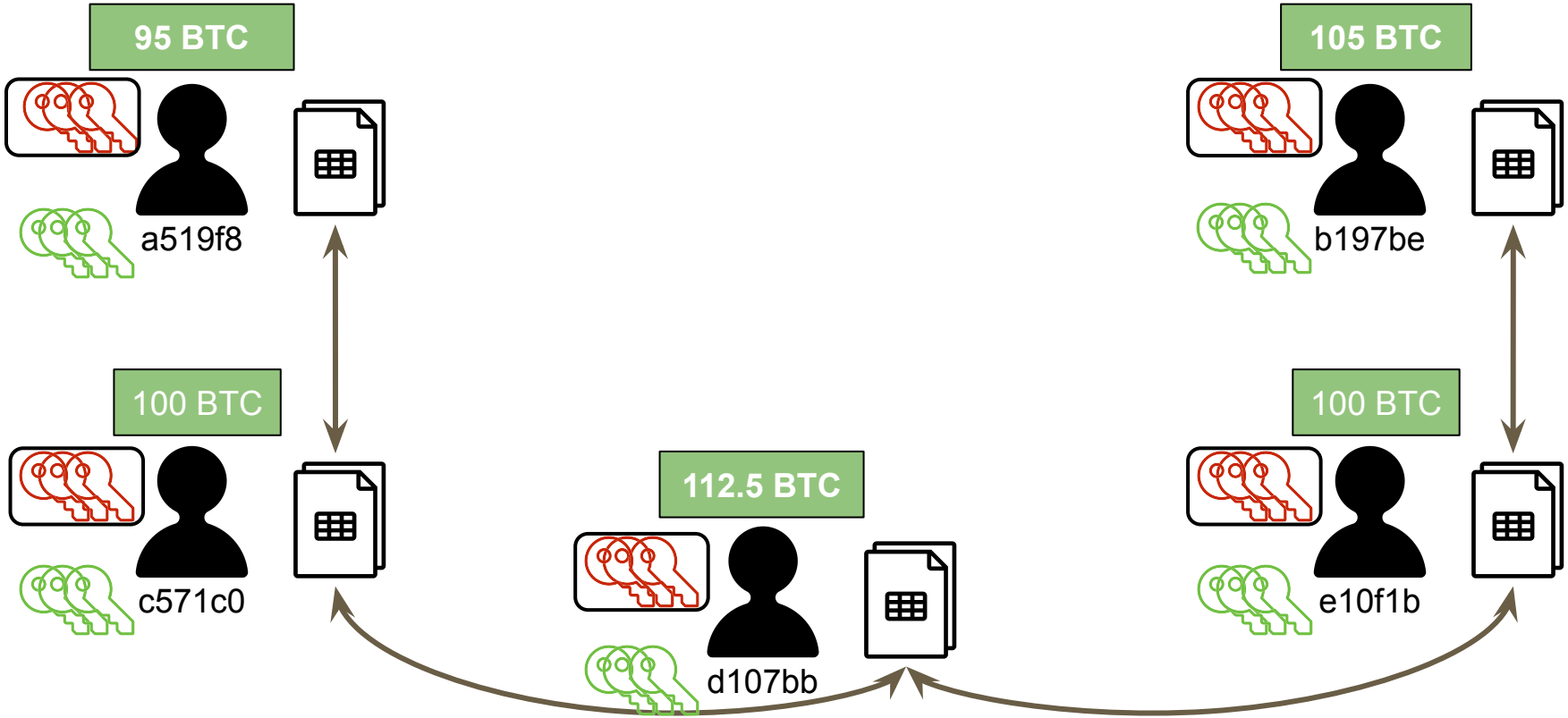
Puzzle Solver

Must be below certain value

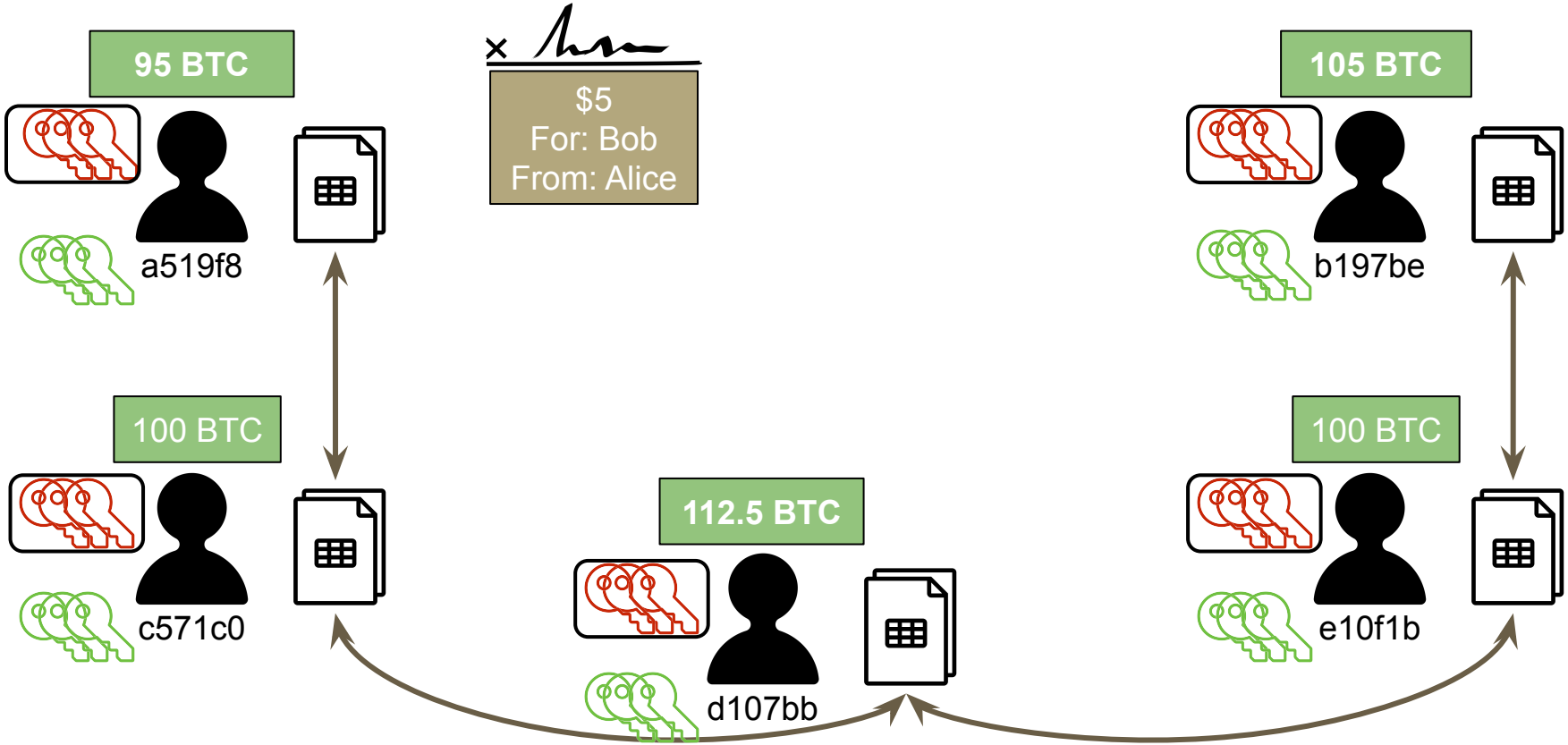
Bitcoin


95 BTC
a519f8
Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
*From: a519f8...
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: 3a419ef573a86f
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

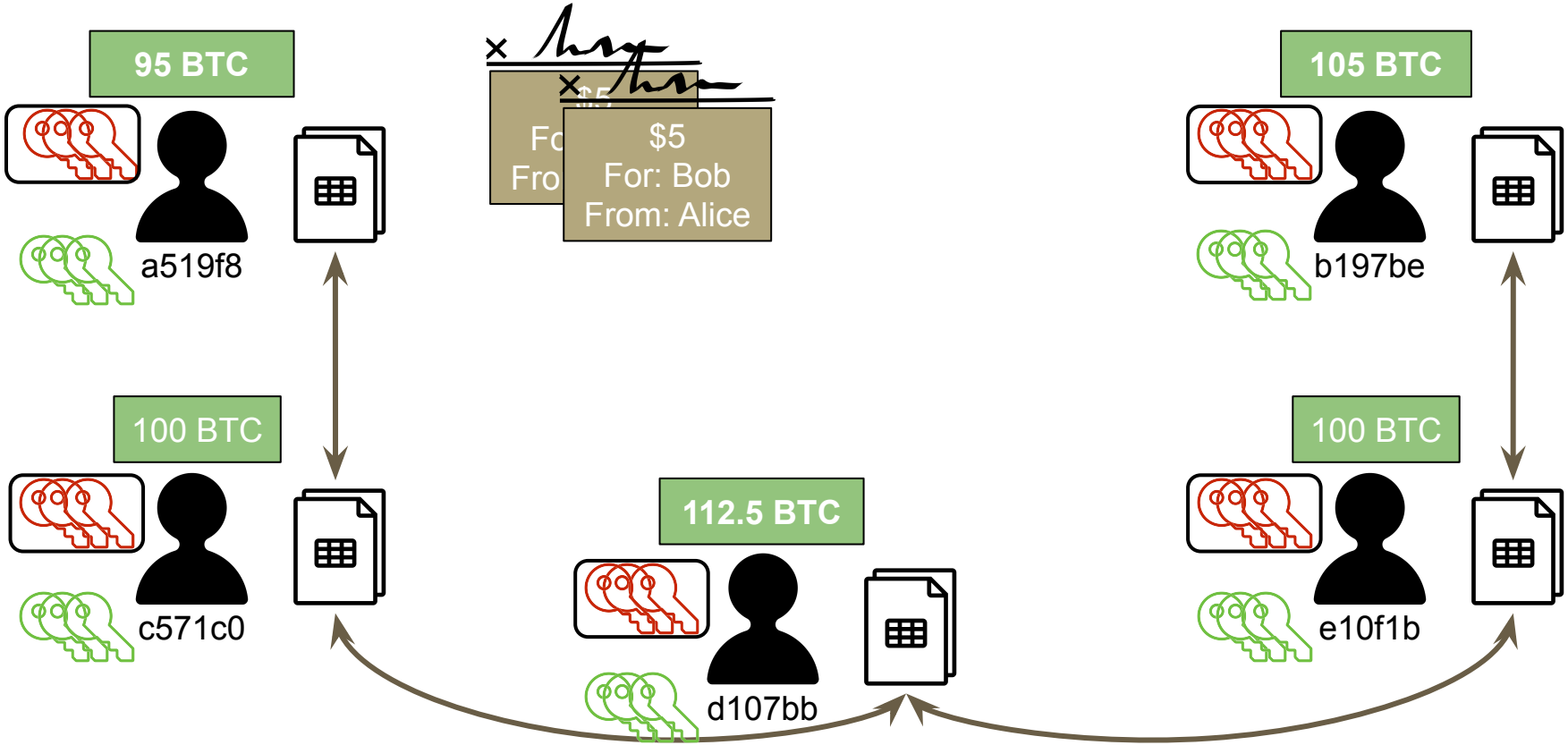
Bitcoin: one Tx per block? Not really!



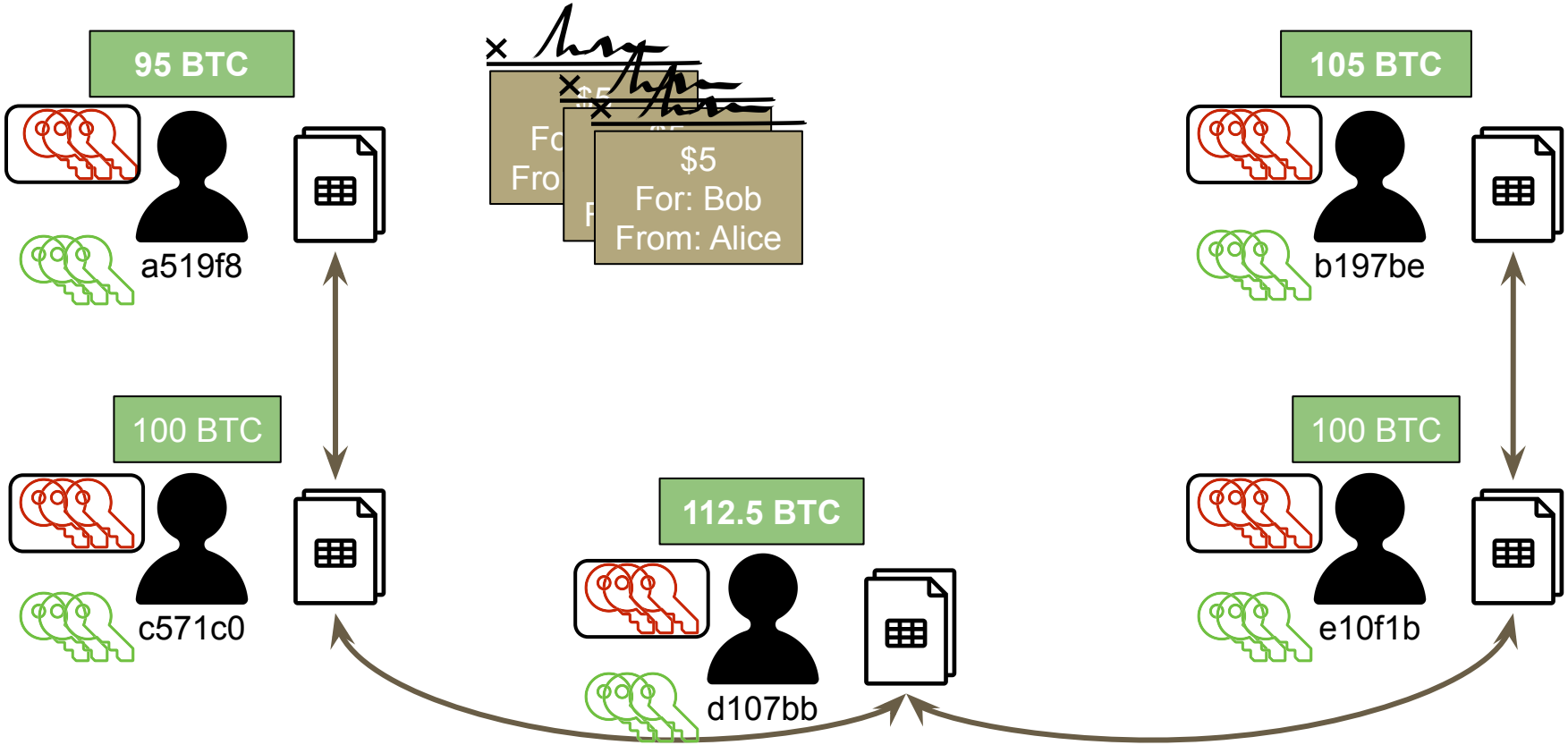
Bitcoin


95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

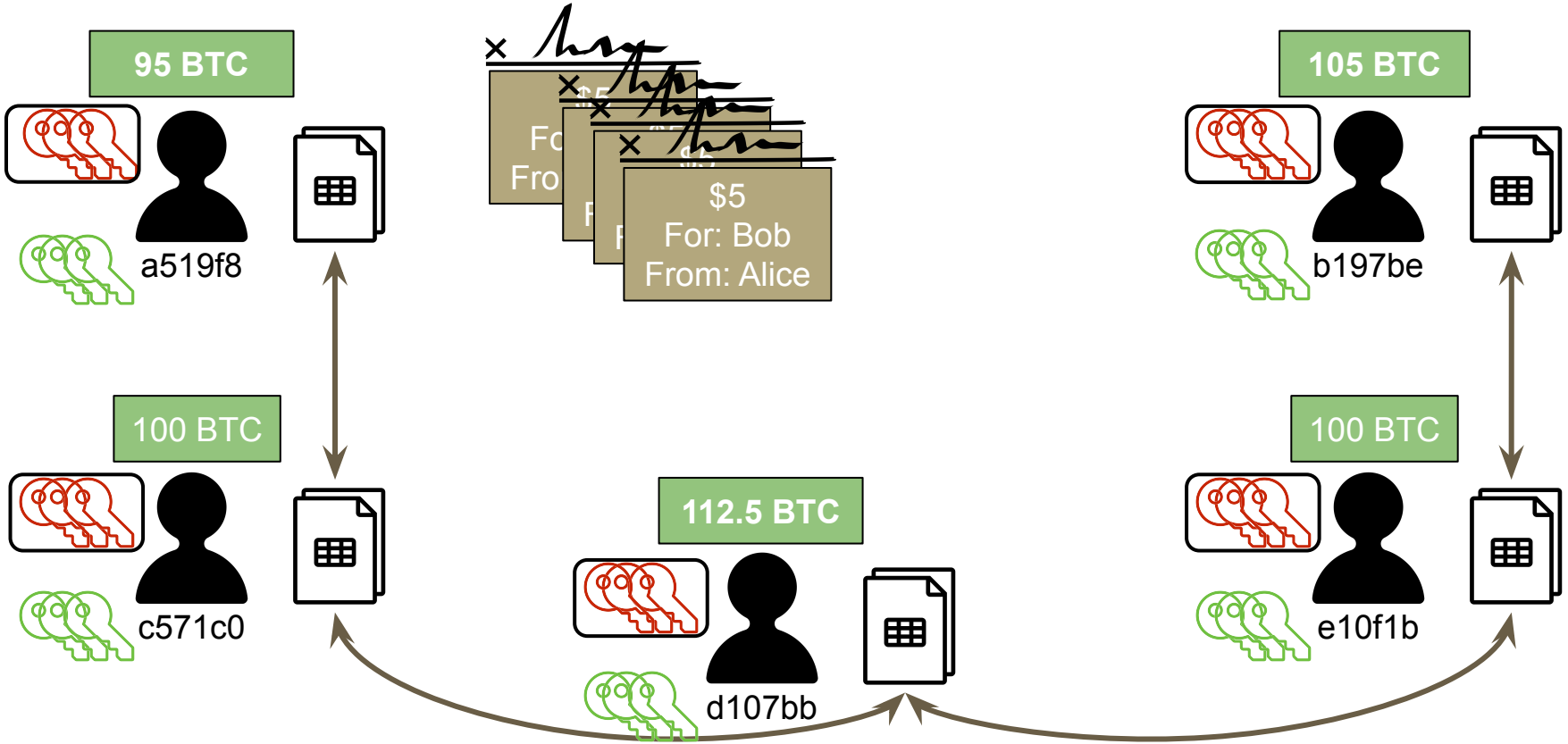
Bitcoin


95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

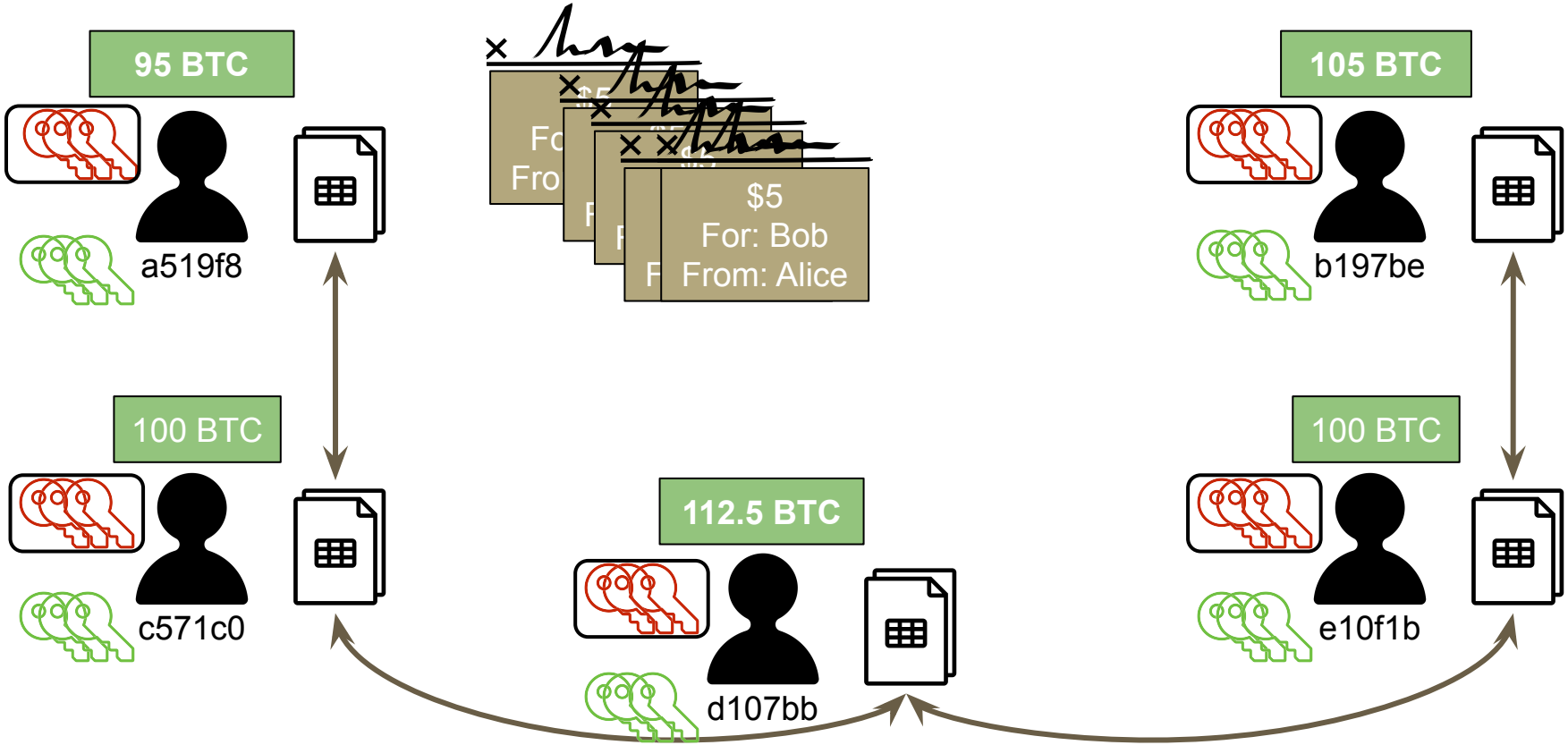
Bitcoin


95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

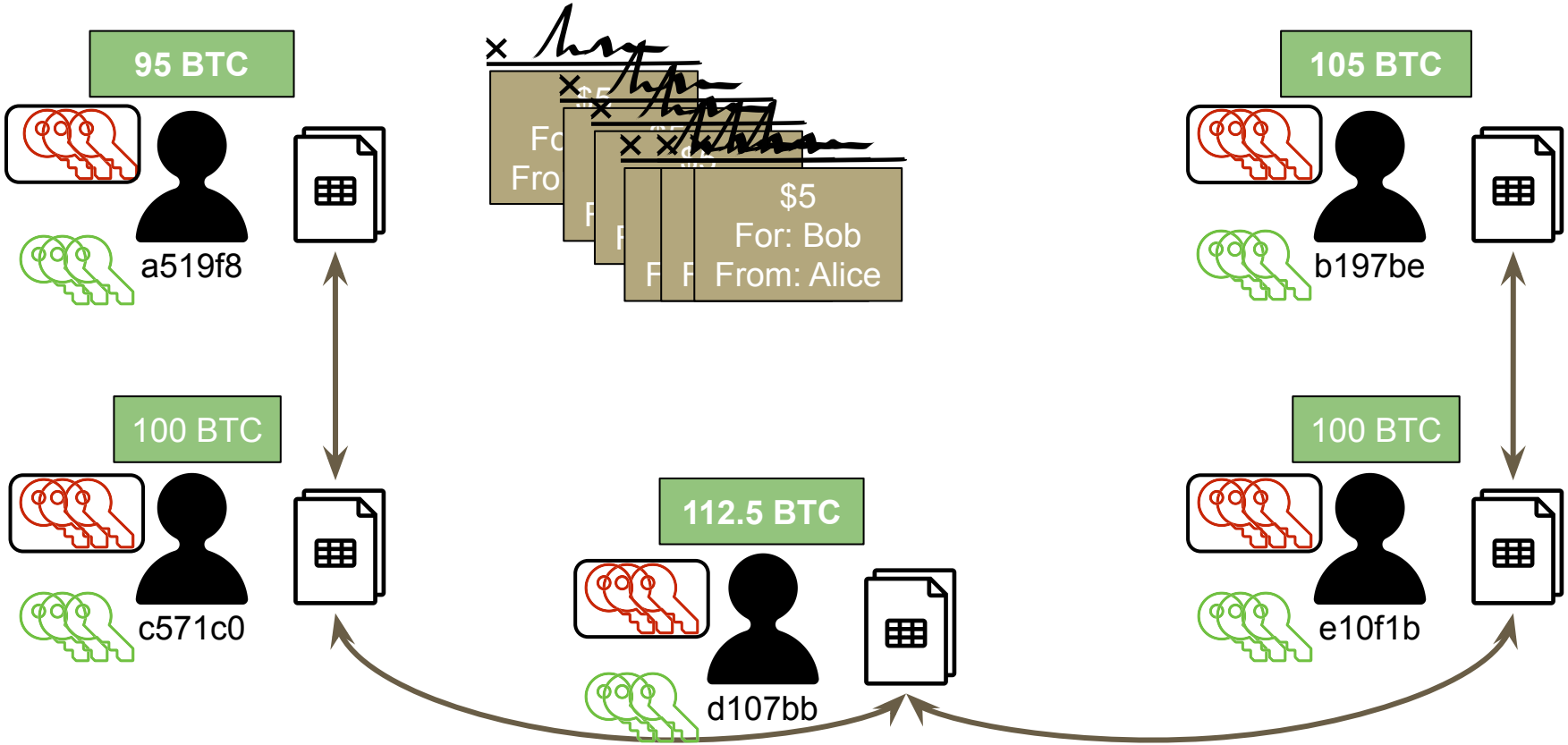
Bitcoin


95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

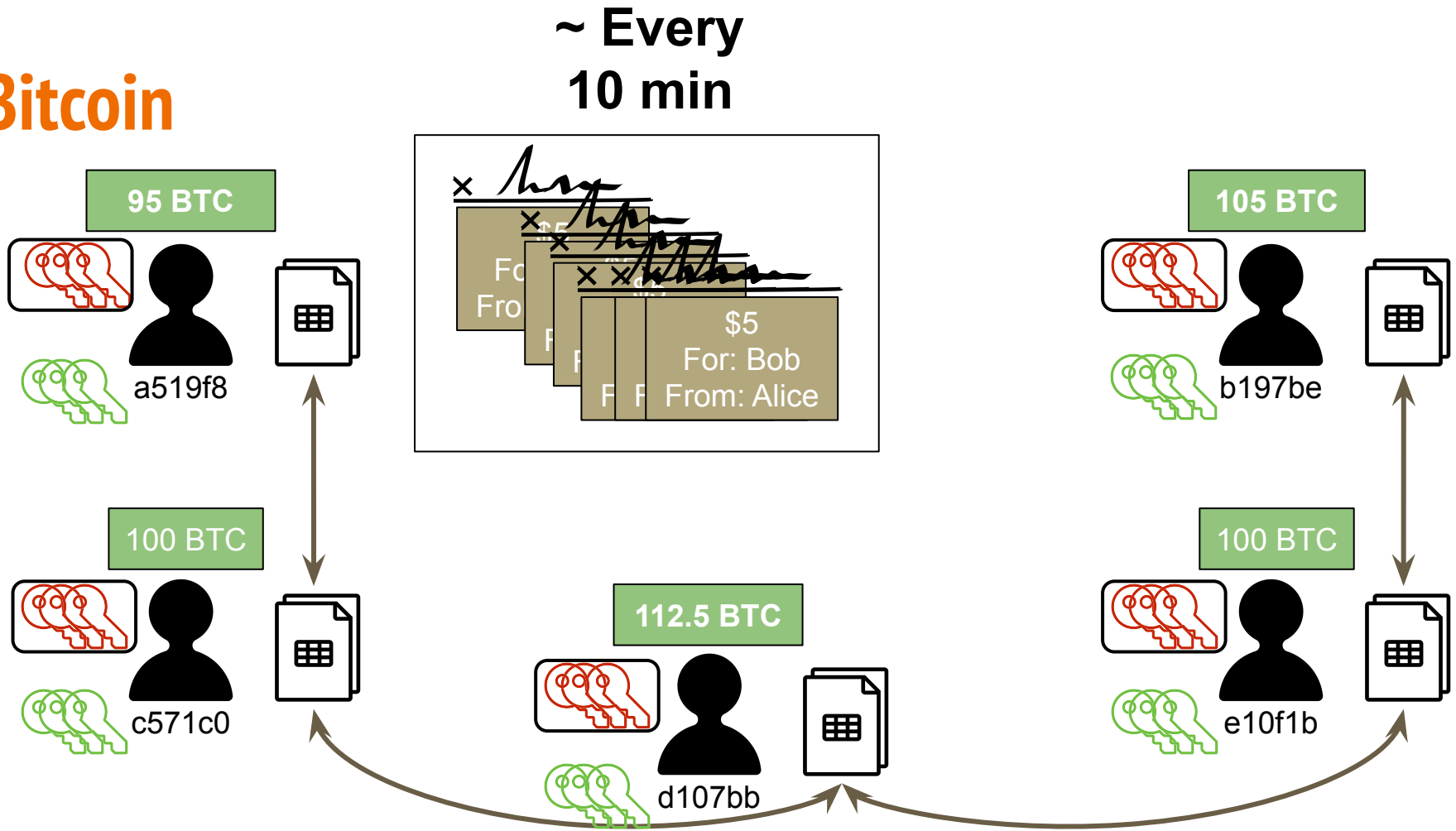
Bitcoin


95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

Bitcoin

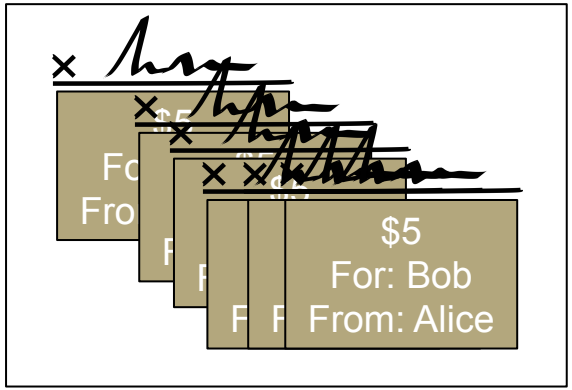

95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

Bitcoin

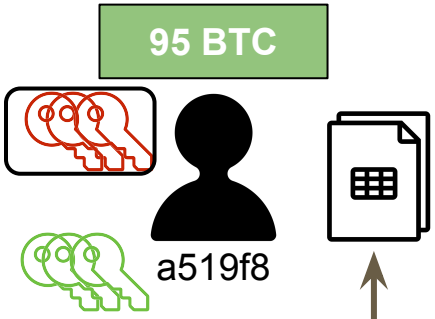

~ Every
10 min
95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
100 BTC
c571c0
112.5 BTC
d107bb
100 BTC
e10f1b

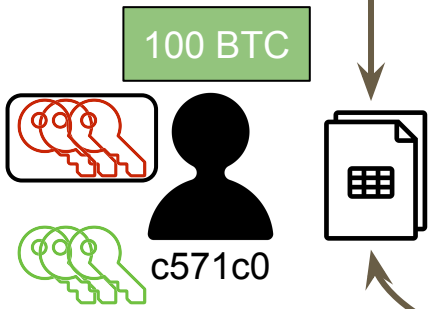
Bitcoin

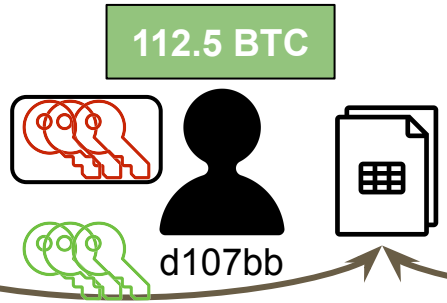
~ Every
10 min

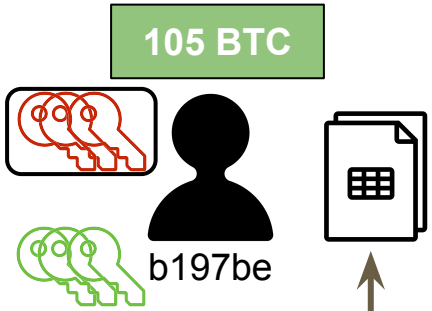


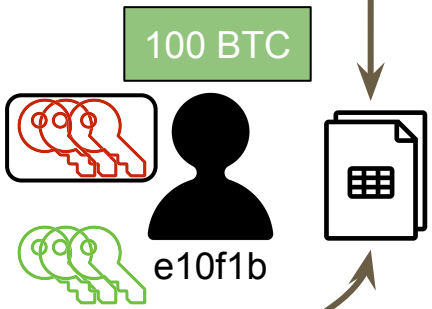
~2,800 avg transactions
(2023 YTD)











Calibrating "Puzzle" (every 2016 blocks; ~2 weeks)

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: **3a419ef573a86f**

Puzzle Solution

Puzzle Solver

Must be below certain value

Calibrating The Bitcoin "Puzzle" w/ Difficulty

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: **3a419ef573a86f**

Puzzle Solution

Puzzle Solver

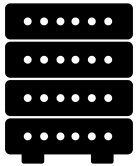
Must be below certain value **(DIFFICULTY)**

Calibrating The Bitcoin "Puzzle" w/ Difficulty

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: **000a419ef573a86f**

Puzzle Solution

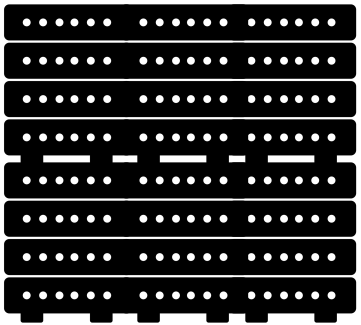
Puzzle Solver



Few computers = low difficulty, i.e. blocks can be solved more easily

Must be below certain value **(DIFFICULTY)**

Calibrating The Bitcoin "Puzzle"...



More computers = high difficulty, i.e. blocks more time-consuming to solve, but balances out because more computers working to solve the problem

Prev Hash: 8a7b6618e714c6a
5 BTC
For: b197be
From: a519f8…
Nonce: 3
Nonce Solver: d107bb (Dave)
Hash: **000000a419ef573a**

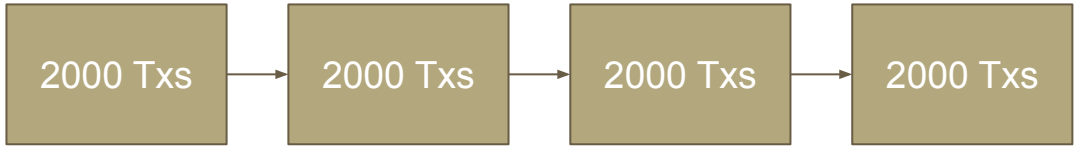
Puzzle Solution

Puzzle Solver

Must be below certain value **(DIFFICULTY)**

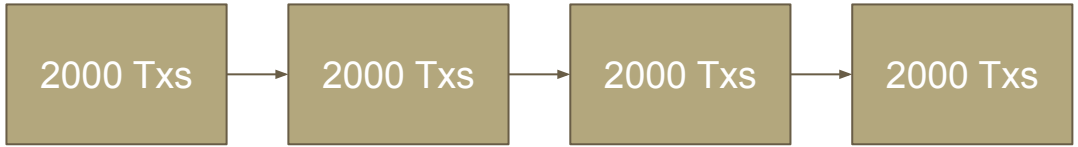
Why the Puzzle?

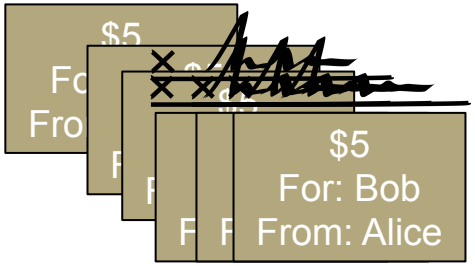
Normal Miner's Blockchain:



Why the Puzzle?

Normal Miner's Blockchain:

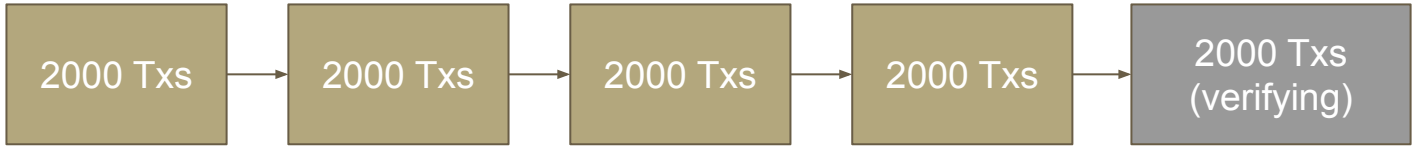


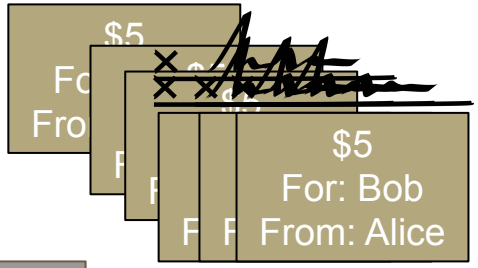


Pending Transactions

Why the Puzzle?

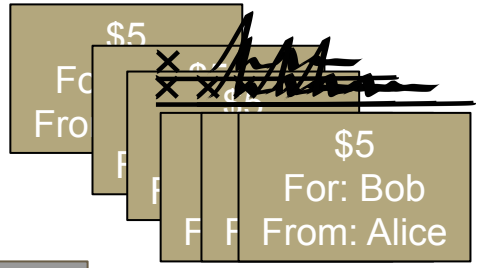
Normal Miner's Blockchain:





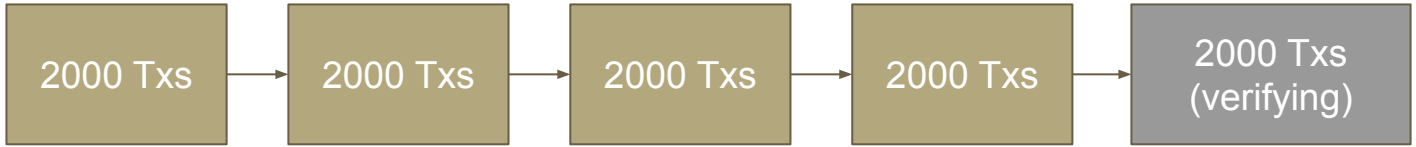
Pending Transactions

Why the Puzzle?

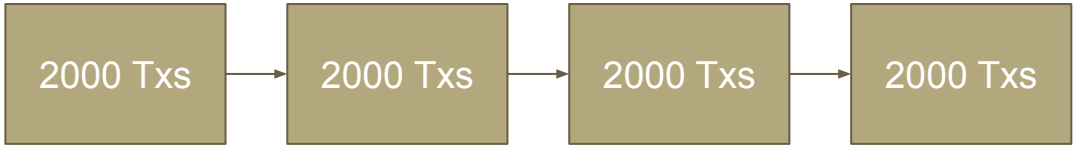


Pending Transactions

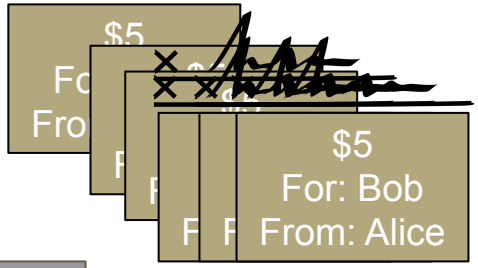
Normal Miner's Blockchain:



Malicious Miner's Blockchain:

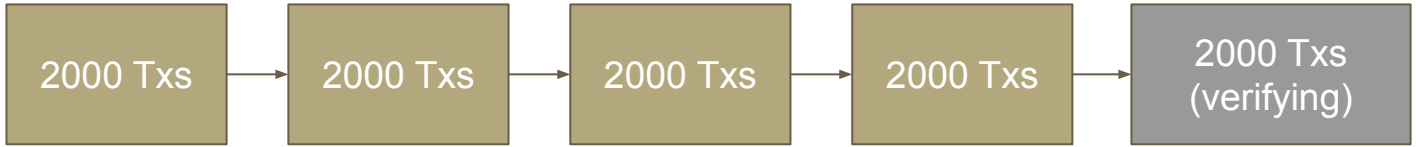


Why the Puzzle? Let's spam!



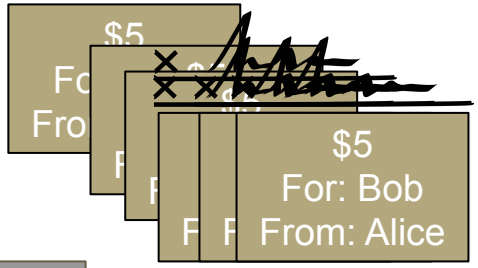
Pending Transactions

Normal Miner's Blockchain:



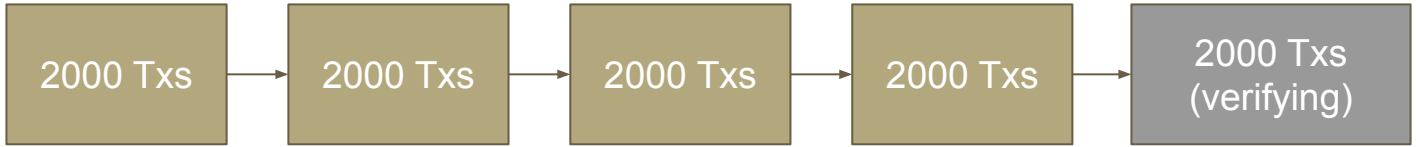
Malicious Miner's Blockchain:

Why the Puzzle?

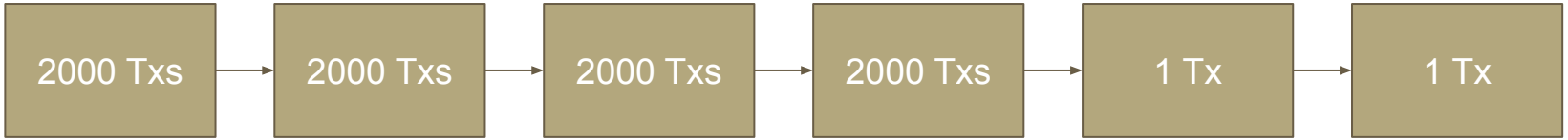


Pending Transactions

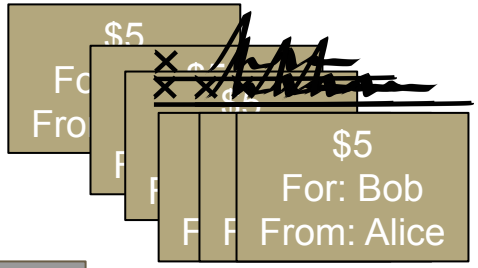
Normal Miner's Blockchain:



Malicious Miner's Blockchain:

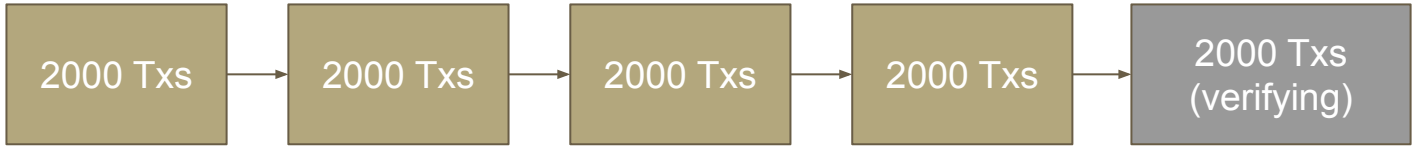


Why the Puzzle?

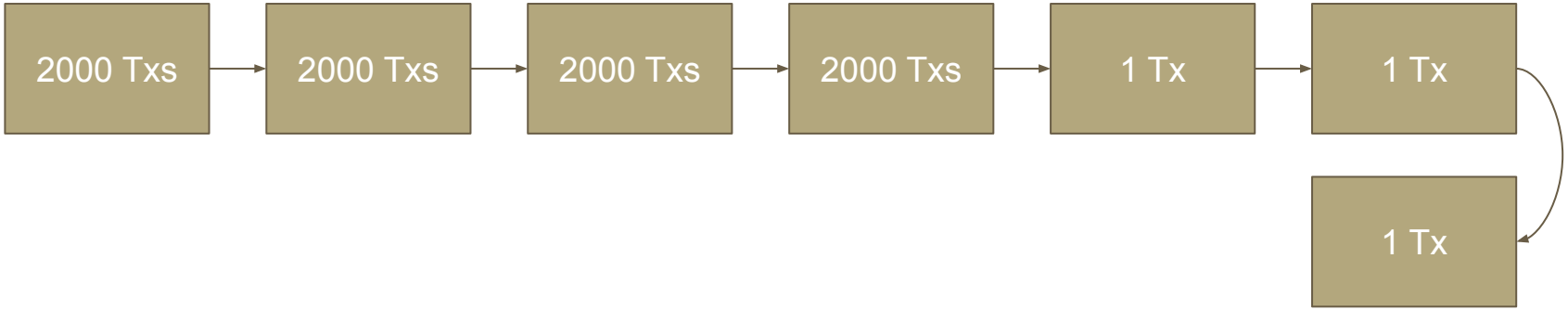


Pending Transactions

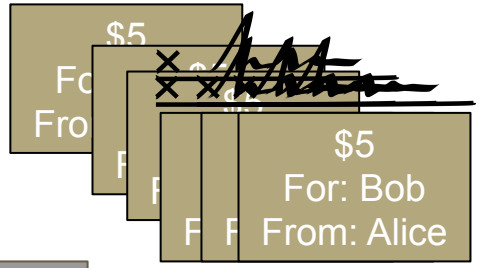
Normal Miner's Blockchain:



Malicious Miner's Blockchain:

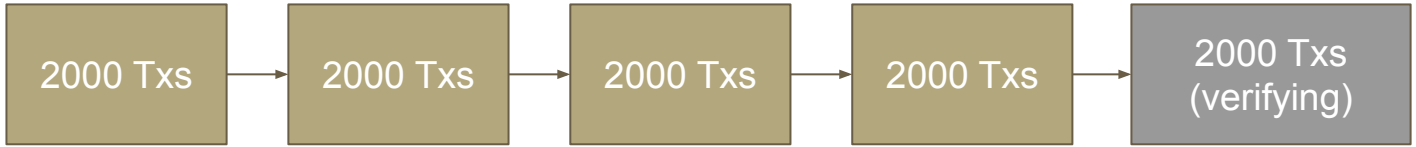


Why the Puzzle?

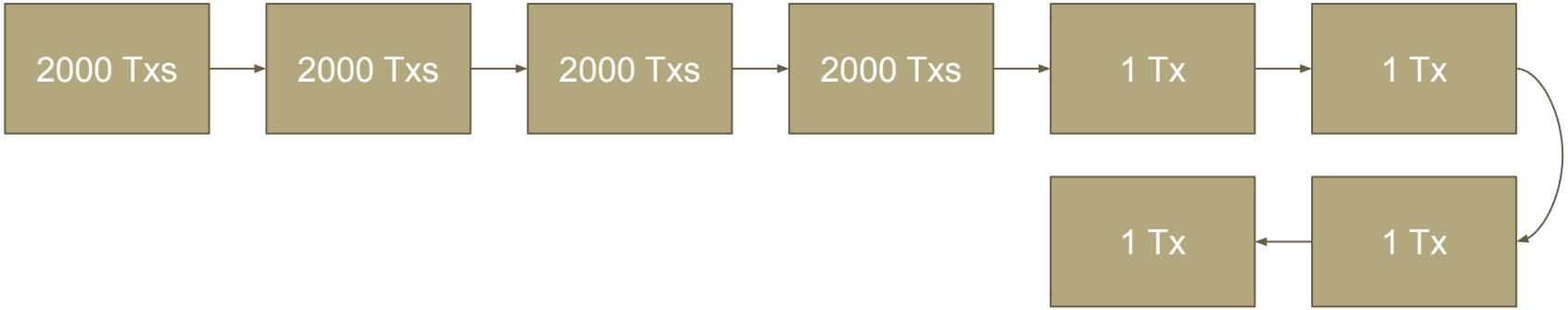


Pending Transactions

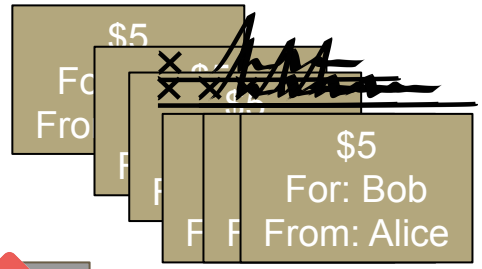
Normal Miner's Blockchain:



Malicious Miner's Blockchain:

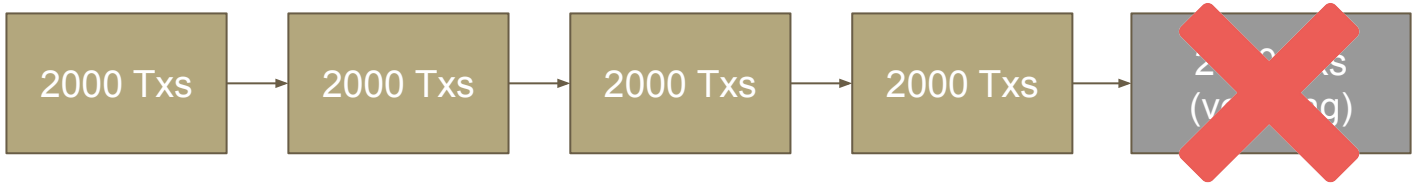


Why the Puzzle?

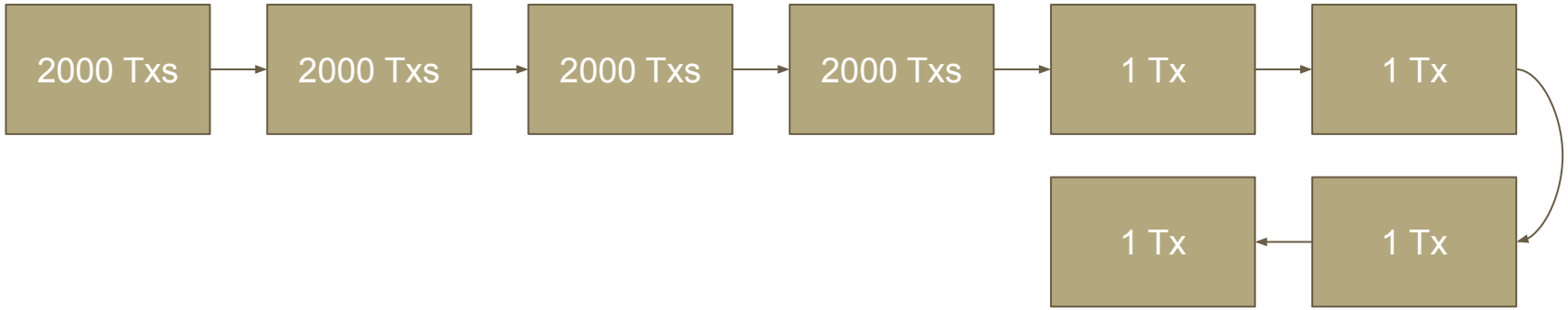


Pending Transactions

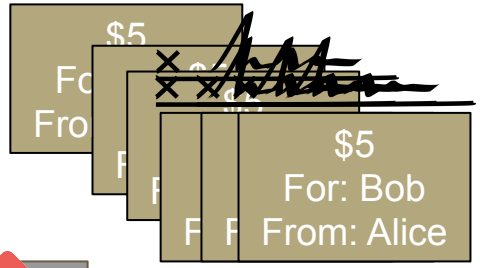
Normal Miner's Blockchain:



Malicious Miner's Blockchain:

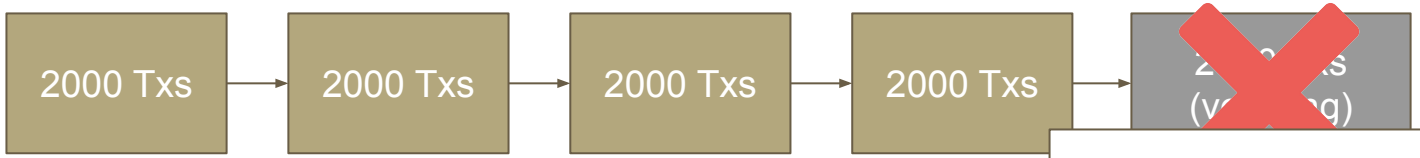


Why the Puzzle?



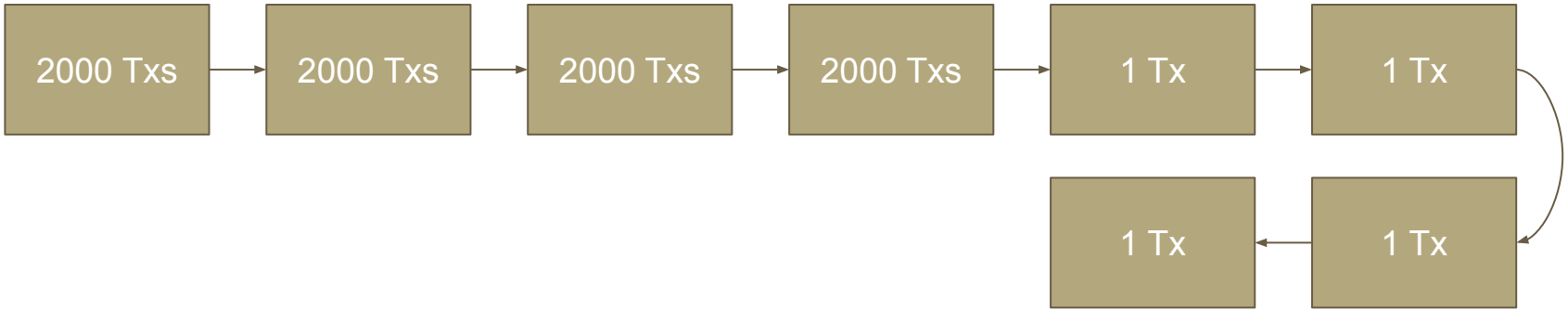
Pending Transactions

Normal Miner's Blockchain:

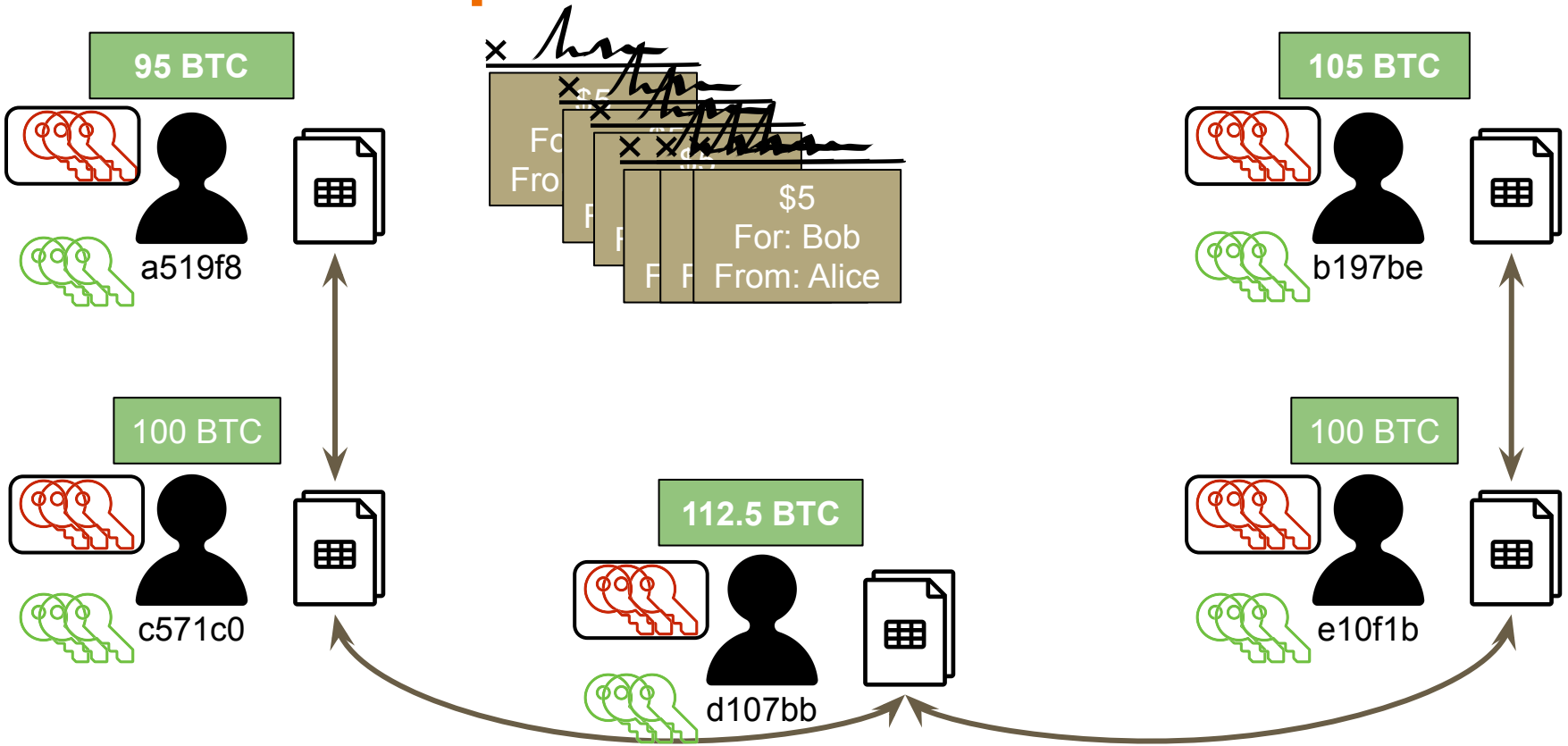


Lost or Possibly Reversed Transactions

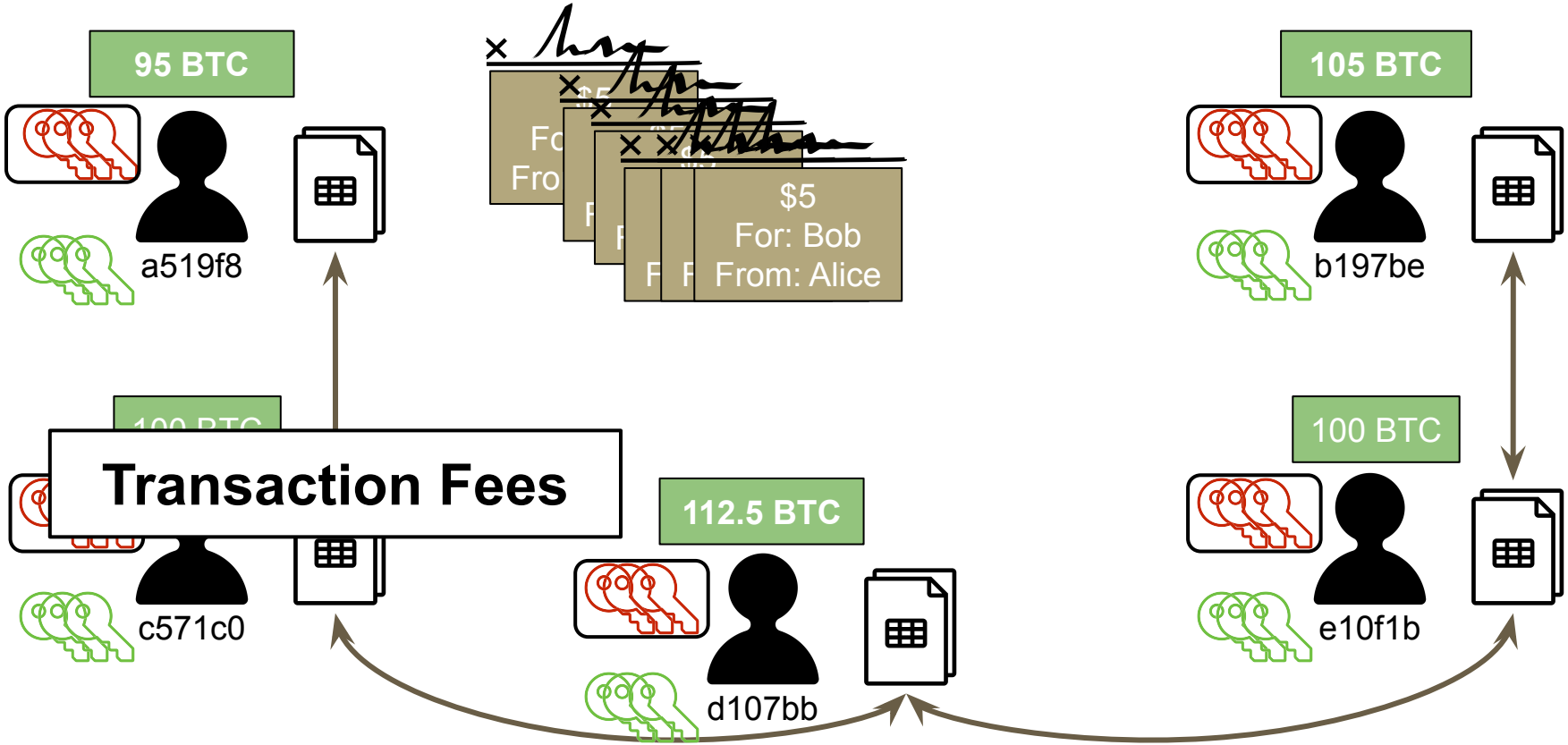
Malicious Miner's Blockchain:



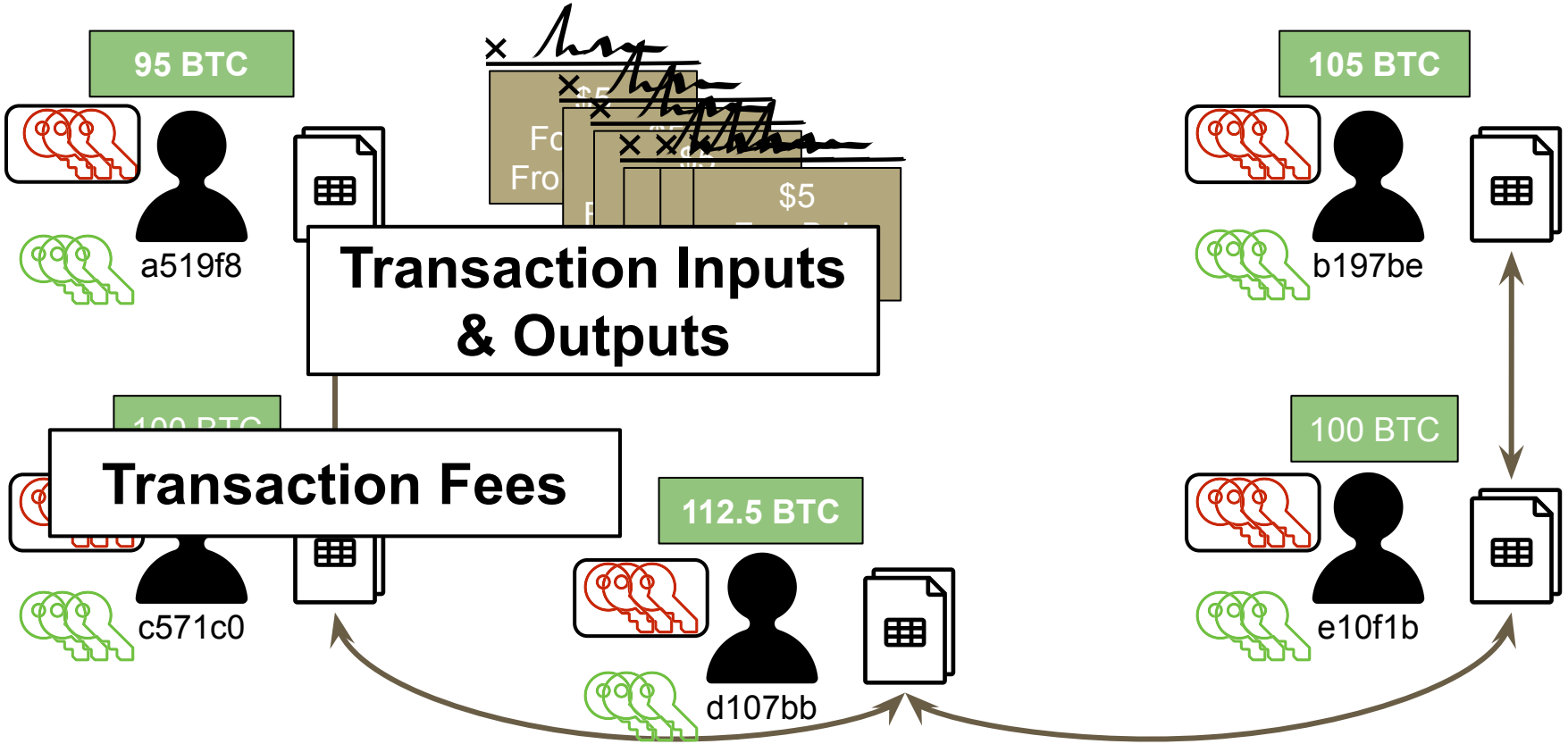
Bitcoin: other topics



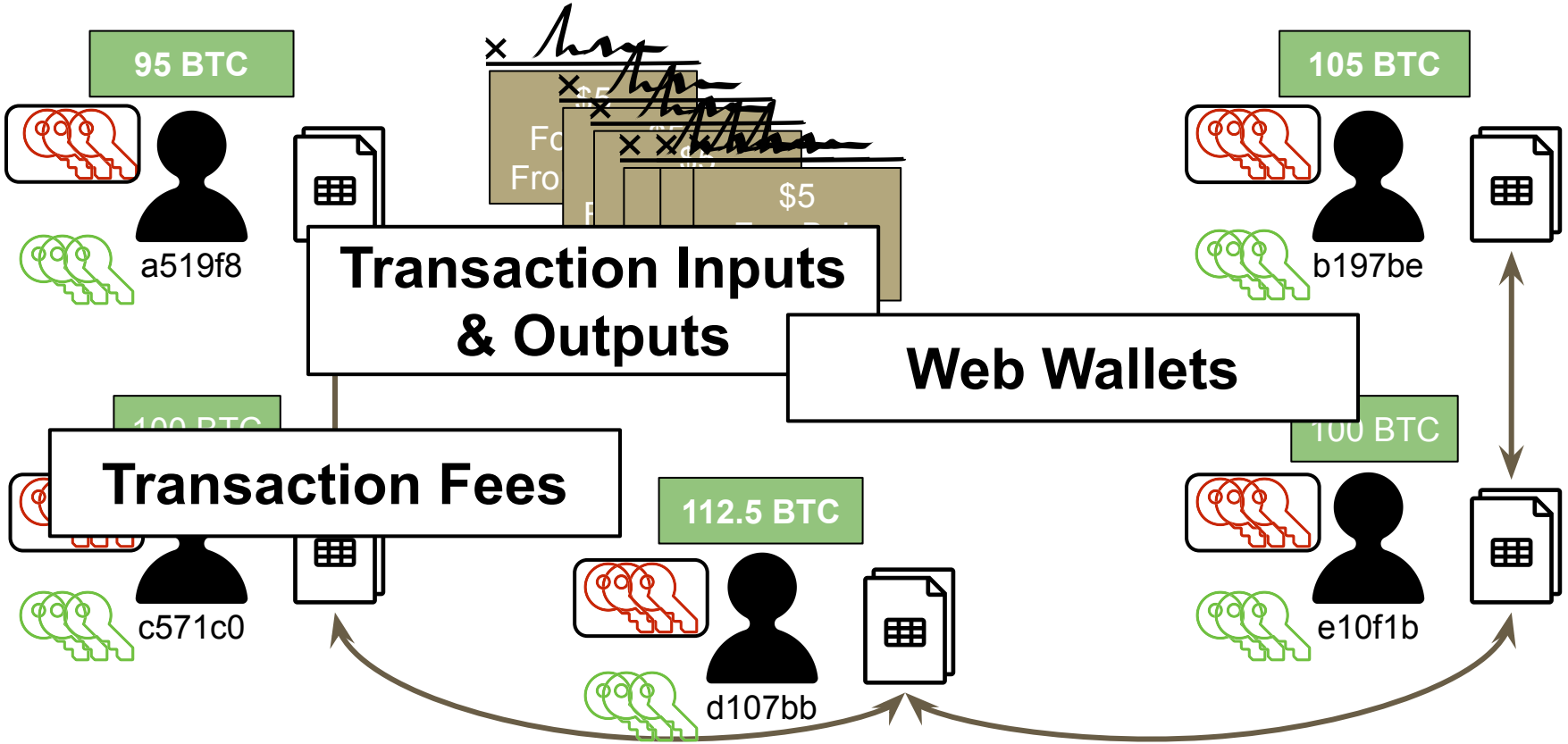
Bitcoin


95 BTC
a519f8
$5
For: Bob
From: Alice
105 BTC
b197be
Transaction Fees
112.5 BTC
d107bb
100 BTC
e10f1b
c571c0

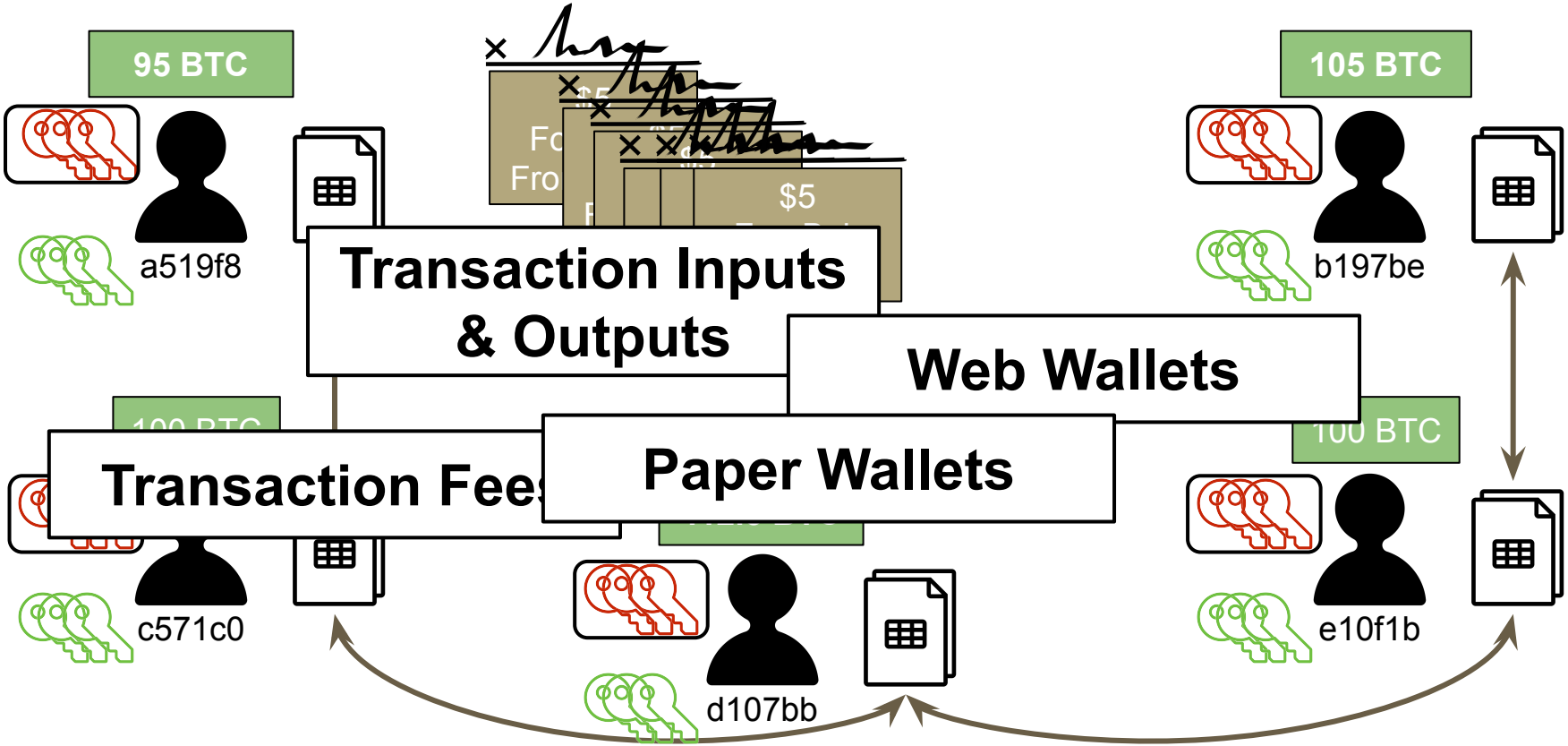
Bitcoin


95 BTC
a519f8
Transaction Inputs & Outputs
Transaction Fees
105 BTC
b197be
100 BTC
e10f1b
112.5 BTC
d107bb
c571c0

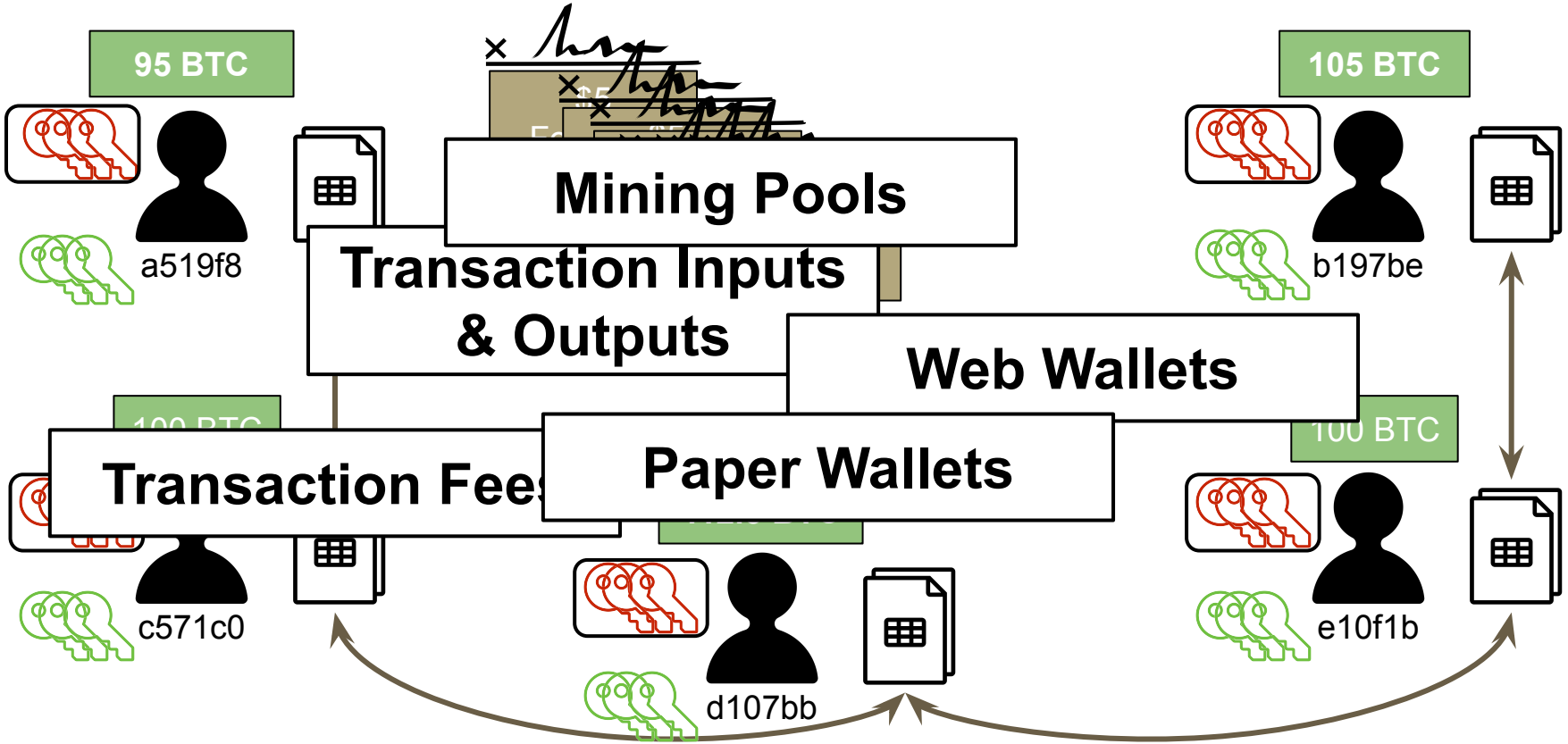
Bitcoin


95 BTC
a519f8
105 BTC
b197be
Transaction Inputs & Outputs
Web Wallets
Transaction Fees
112.5 BTC
d107bb
c571c0
e10f1b

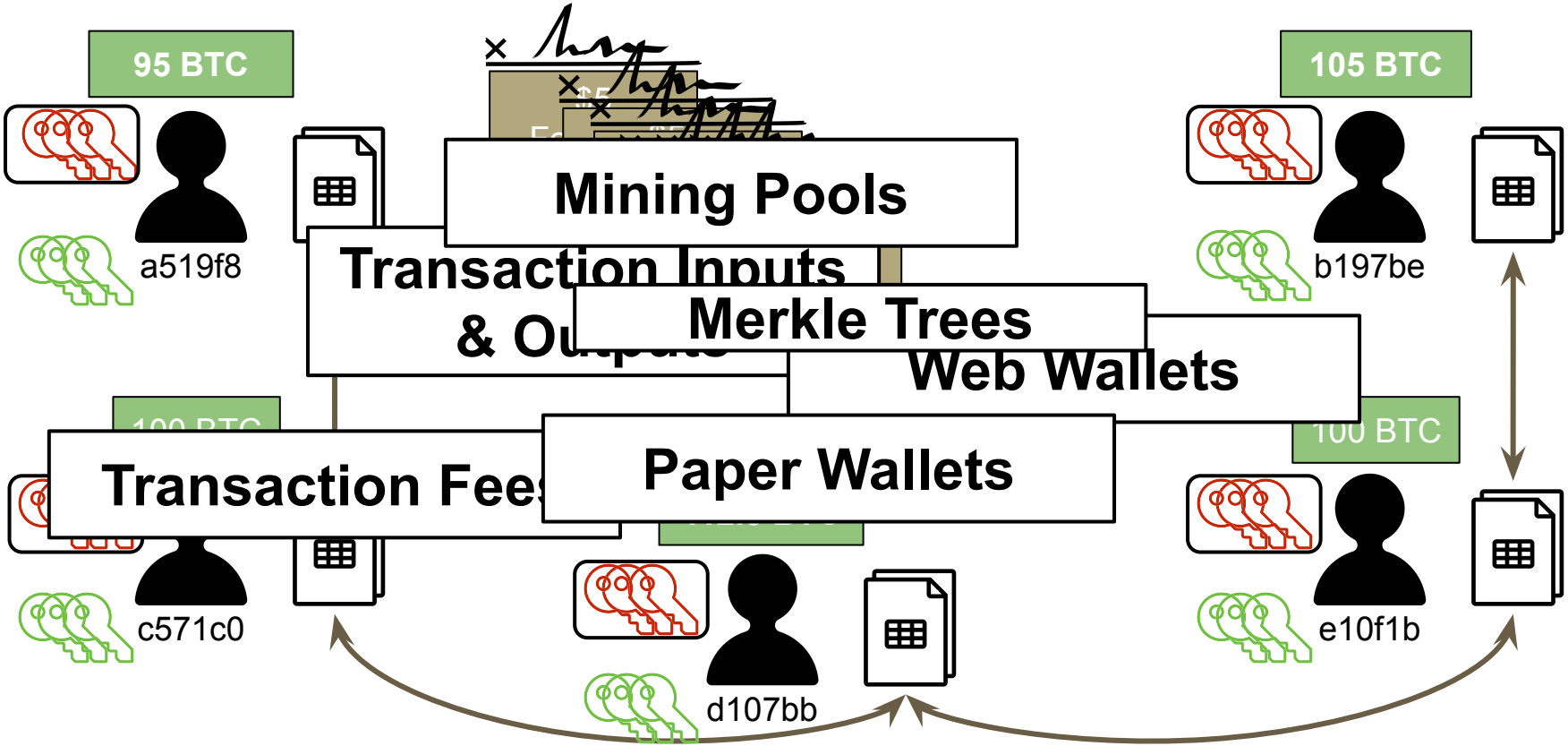
Bitcoin


95 BTC
105 BTC
a519f8
b197be
Transaction Inputs & Outputs
Web Wallets
Transaction Fees
Paper Wallets
100 BTC
c571c0
d107bb
e10f1b

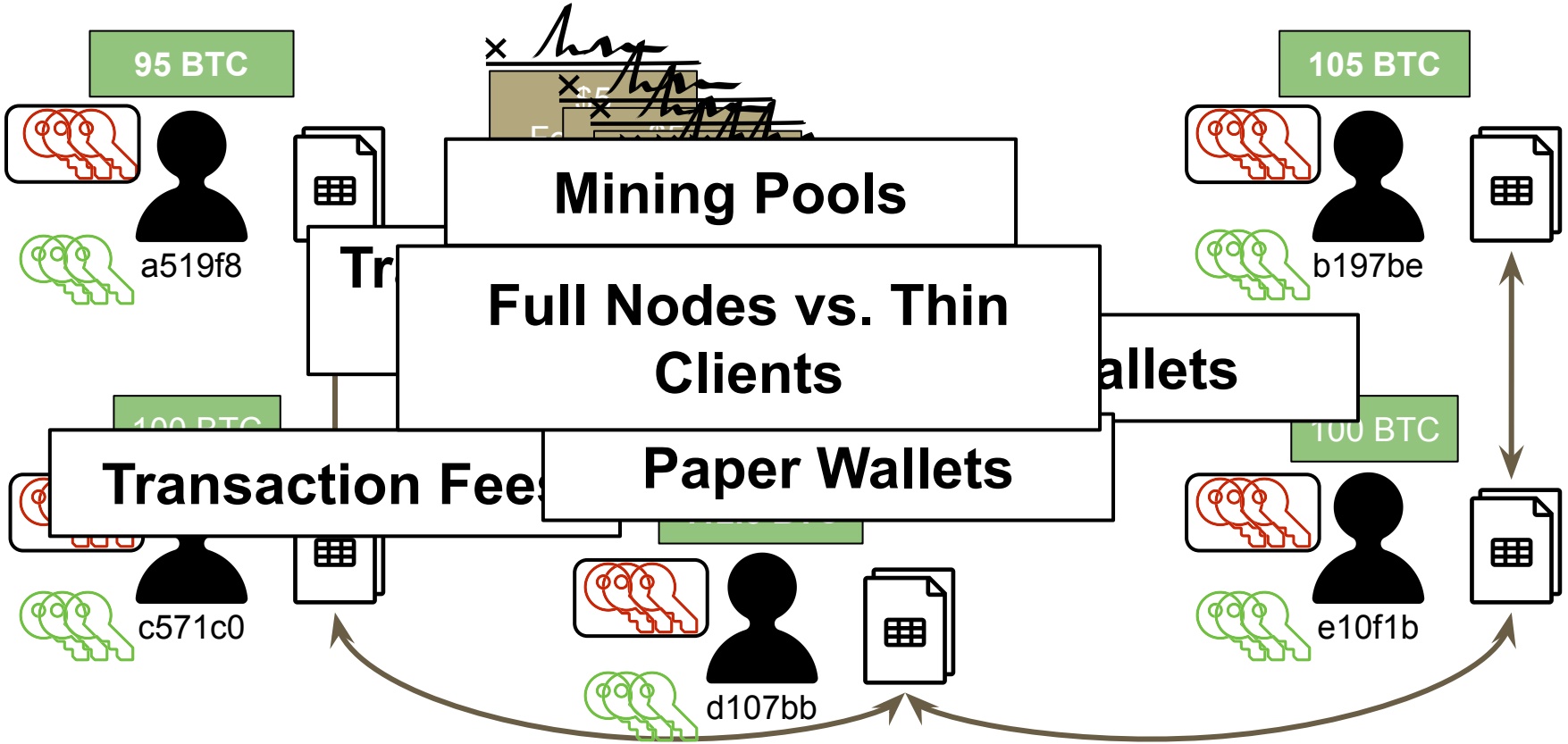
Bitcoin


95 BTC
105 BTC
a519f8
b197be
Mining Pools
Transaction Inputs & Outputs
Web Wallets
Transaction Fees
Paper Wallets
100 BTC
c571c0
d107bb
e10f1b

Bitcoin


95 BTC
105 BTC
a519f8
b197be
Mining Pools
Transaction Inputs
& Outputs
Merkle Trees
Web Wallets
Transaction Fees
Paper Wallets
100 BTC
c571c0
d107bb
e10f1b

Bitcoin


95 BTC
105 BTC
a519f8
b197be
Mining Pools
Full Nodes vs. Thin Clients
Transaction Fees
Paper Wallets
100 BTC
c571c0
d107bb
e10f1b

Funny Story: guard your wallet (Dec 2013)!!

This was just the beginning!
Lot more to learn …

Thank you for your participation.

Visit: fintech.gsb.columbia.edu