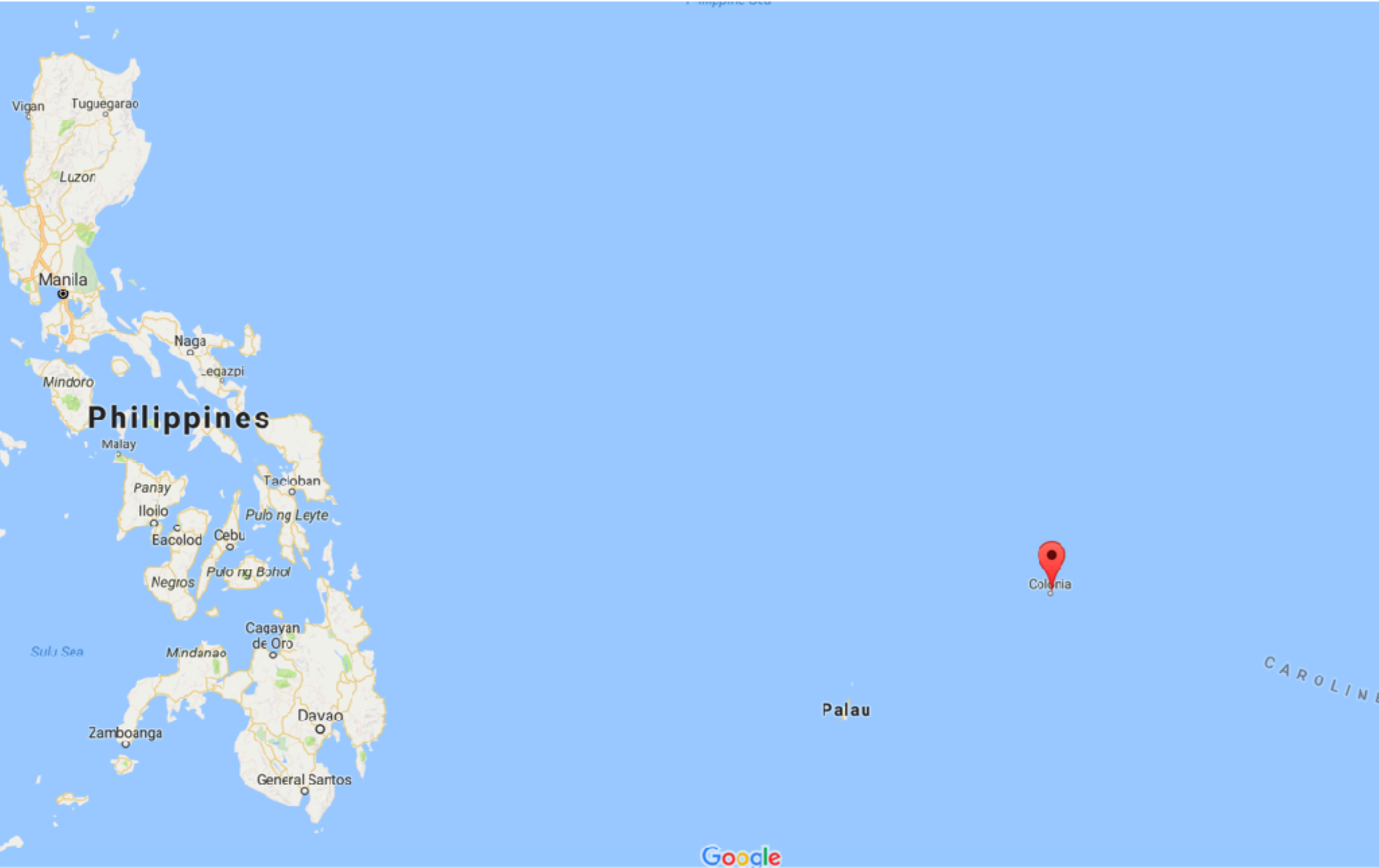


Basic function of money

How does Bitcoin work?

Future of money





China

South Korea

Japan

Sea of Japan

East China Sea

North Pacific Ocean

Myanmar (Burma)

Philippine Sea

HI

Thailand

Vietnam

Philippines

Gulf of Thailand

Malaysia

Indonesia

Papua New Guinea

Banda Sea

Arafura Sea

Australia

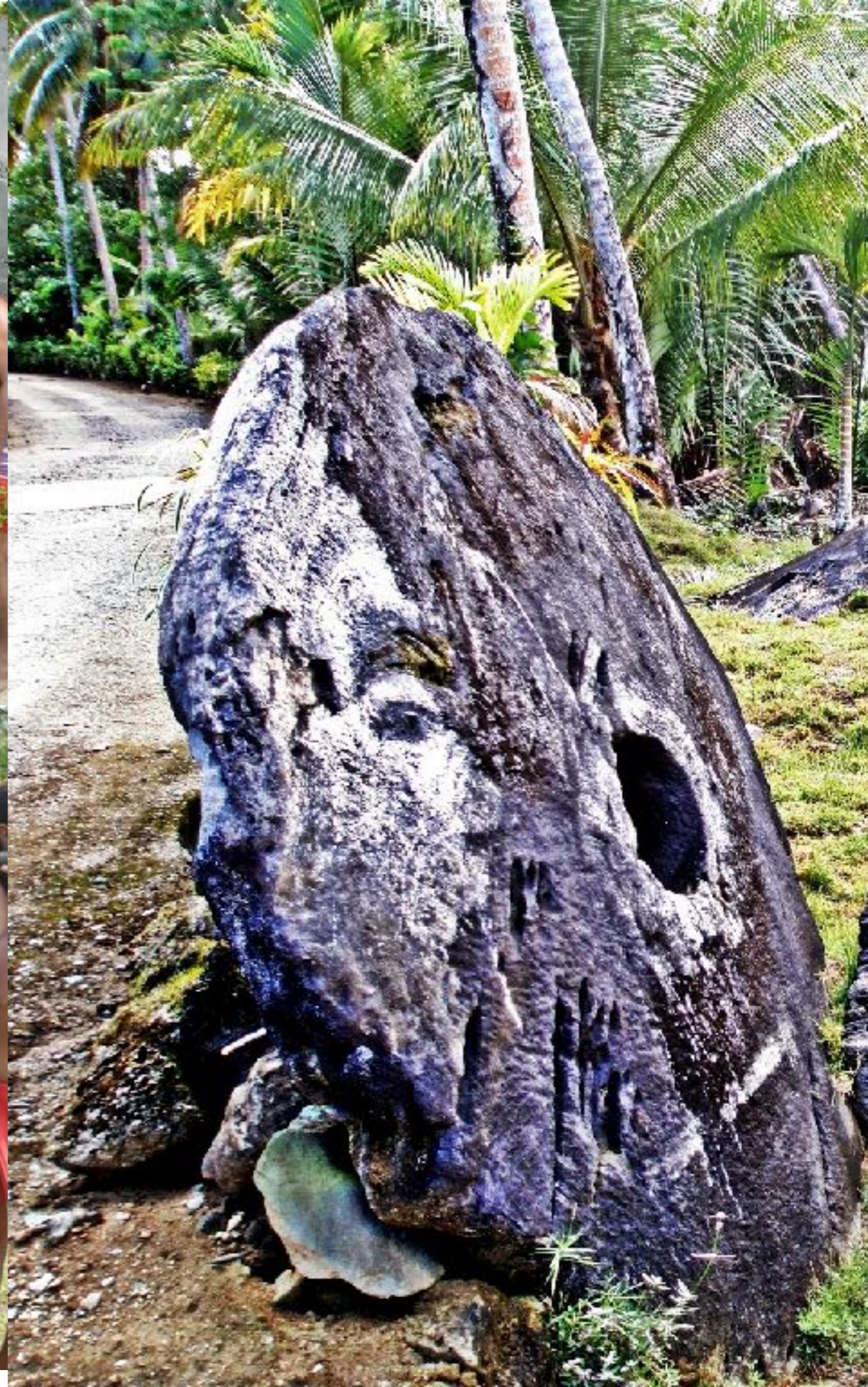
Coral Sea

NT

QLD

WA







WORLD TRADE CENTER

Cortlandt St M

Vesey St M

M Fulton Street Subway

Brooklyn Bridge

2

Zuccotti Park

M Fulton Street

Trinity Pl

Broadway

Pearl St

Trinity Church

33 Liberty Street

New York Stock Exchange

Federal Hall

M Wall Street

ove

of ge

Charging Bull

55 Wall Street

2

Bowling Green

r House

Battery Park

State St

The Dead Rabbit Grocery and Grog

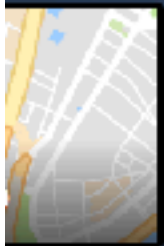
ter St

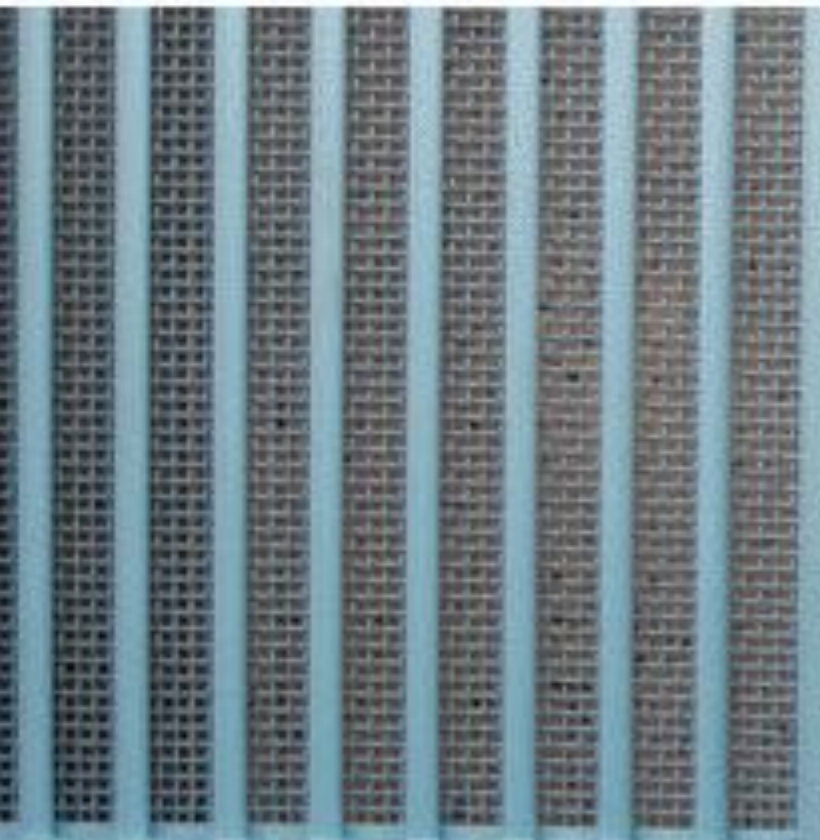
SeaGlass Carousel

M South Ferry

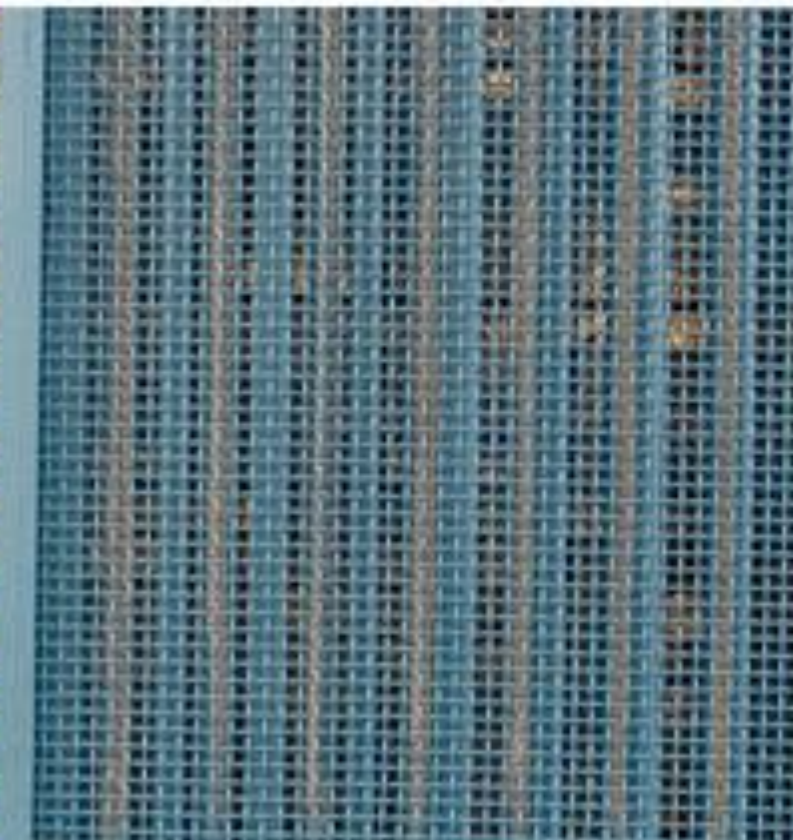
DR Di

Google





31



<http://money.cnn.com/2017/08/23/investing/germany-gold-reserves-new-york-paris/>
Germany's got its gold back.

The country's central bank announced Wednesday it has completed a program to repatriate gold bars worth nearly \$31 billion from storage locations in New York and Paris.

Germany has been bringing gold home to Frankfurt from the two cities since 2013. The final 100 tons were moved from Paris earlier this year, the central bank said.

In total, 743 tons have been transferred. The project was completed three years ahead of schedule.

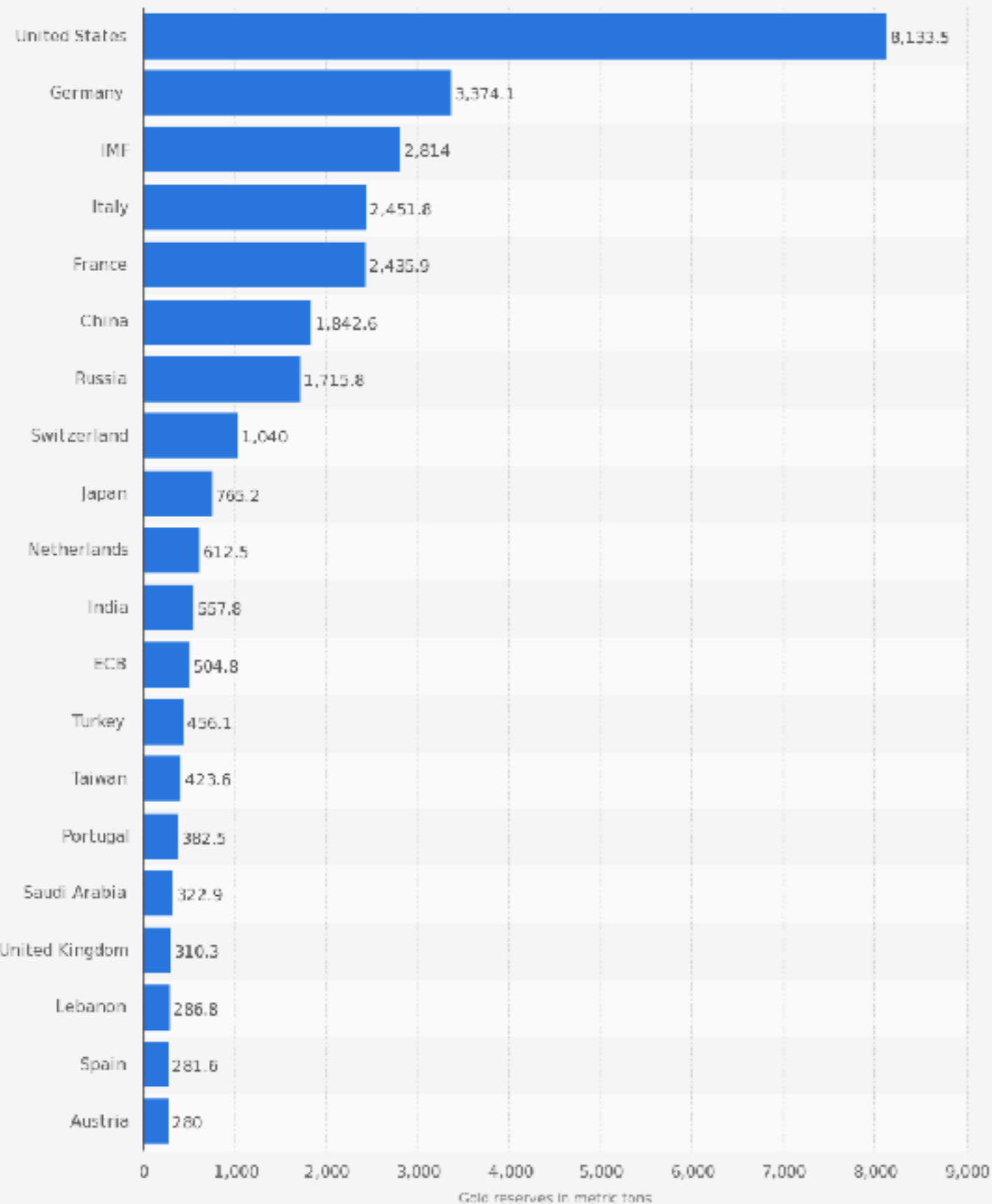
The central bank previously said it was bringing the gold home to help build public "trust and confidence."

But it's also a recognition that times have changed: Germans are no longer worried about preventing their gold reserves from falling under Soviet control -- a real fear during the Cold War.

And the central bank no longer needs to keep gold in Paris as a protective measure that would allow it to quickly exchange international currency in an emergency. Both countries use the euro.



Gold reserves of largest gold holding countries worldwide as of June 2017 (in metric tons)



Source:
IMF; World Gold Council
© Statista 2017

Additional Information:
Worldwide; IMF; World Gold Council; June 2017

Live Metal Spot Prices (24 hours)

GOLD SPOT PRICES	GOLD PRICE TODAY	SPOT CHANGE
Gold Price Per Ounce	\$1,342.00	▲ \$0.00

...
 ...
 ...
 ...
 ...
 fatto sacrodo ————— 120 ————— 120 —————

Castro

- Antonio de pace vo colle roc
 maio licu ventingui ————— 5 8
- Proppi dimighele d'istata fornaco
 10 licu quareo ————— 4 8
- Antonio de pace fornaco a
 fontanaria mprata licu patto
 chq ————— 1 4 8
- Matto Antonio muntano licu
 quingq ————— 1 5 8
- Domenico d'locingo oculo laia
 porta asammato licu ostanta — 8 0 8
- Giovanni vo p'dato d'muntano
 10 acouzzano licu cinque — 5 8
- Luca d'marcho c'chopantom fo
 enacq asampuro aponto licu 80q — 1 0 8

Inchiarichi

- franc' detto ————— anny 30 ————— 1200
- Isabella sua donna ————— anny 21 ————— 1200
- Corouonluoz suo fidoquolo anny — 3 ————— 1200
- Antonia sua fidoquola — anny — 2 ————— 1200
- Lisa sua fidoquola abalia anny — 1 ————— 1200

La casa dove abita detto franc' tunc appi
 Eione sacrodo...

BLOCK SUMMARY

Blocks Mined	184
Time Between Blocks	7.32 minutes
Bitcoins Mined	2,300.00000000 BTC

MARKET SUMMARY

Market Price	\$4,620.57	View Chart
Trade Volume	\$403,033,919.15	
Trade Volume	87,225.94000000 BTC	

TRANSACTION SUMMARY

Total Transaction Fees (BTC)	267.62941481 BTC	View Chart
Number of Transactions	277,764	View Chart
Total Output Volume (BTC)	3,320,109.59443188 BTC	View Chart
Estimated Transaction Volume (BTC)	326,224.71025038 BTC	View Chart
Estimated Transaction Volume (USD)	\$1,507,345,420.86	View Chart

MINING COST

Total Miners Revenue (USD)	\$11,863,921.76	View Chart
% Earned From Transaction Fees	10.42%	
% Of Transaction Volume	0.79%	View Chart
Cost per Transaction (USD)	\$42.71	View Chart

HASH RATE AND ELECTRICITY CONSUMPTION

Money L2

Early History of Money

Functions of money

WE have seen that three inconveniences attach to the practice of simple barter, namely, the improbability of coincidence between persons wanting and persons possessing; the complexity of exchanges, which are not made in terms of one single substance; and the need of some means of dividing and distributing valuable articles. Money remedies these inconveniences, and thereby performs two distinct functions of high importance, acting as—

(1) A medium of exchange.

(2) A common measure of value.

In its first form money is simply any commodity esteemed by all persons, any article of food, clothing, or ornament which any person will readily receive, and which, therefore, every person desires to have by

A Standard of Value.

A third function of money soon develops itself. Commerce cannot advance far before people begin to borrow and lend, and debts of various origin are contracted. It is in some cases usual, indeed, to restore the very same article which was borrowed, and in almost every case it would be possible to pay back in the same kind of commodity. If corn be borrowed, corn might be paid back, with interest in corn; but the lender will often not wish to have things returned to him at an uncertain time, when he does not much need them, or when their value is unusually low. A borrower, too, may need several

A Store of Value.

It is worthy of inquiry whether money does not also serve a fourth distinct purpose—that of embodying value in a convenient form for conveyance to distant places. Money, when acting as a medium of exchange, circulates backwards and forwards near the same spot, and may sometimes return to the same hands again and again. It subdivides and distributes property, and *lubricates* the action of exchange. **But at times a person needs to condense his property into the smallest compass, so that he may hoard it away for a time, or carry it with him on a long journey, or transmit it to a friend in a distant**

Early history of money

but it is otherwise with the skins, which, being preserved and valued for clothing, became one of the earliest materials of currency. Accordingly, there is abundant evidence that **furs or skins** were employed as money in many ancient nations. They serve this purpose to the present day in some parts of the world.

In the book of Job (ii. 4) we read, "Skin for skin, yea, all that a man hath will he give for his life;" a statement clearly implying that skins were taken as the representative of value among the ancient Oriental nations. Etymological research shows that the same may be said of the northern nations from the earliest

Articles of Ornament as Currency.

A passion for personal adornment is one of the most primitive and powerful instincts of the human race, and as articles used for such purposes would be durable, universally esteemed, and easily transferable, it is natural that they should be circulated as money. The wampumpeag of the North American Indians is a case in point, as it certainly served as jewellery. It consisted of beads made of the ends of black and white shells, rubbed down and polished, and then strung into belts or necklaces, which were valued according to their length, and also according to their colour and lustre, a foot of black peag being worth two feet of white peag. It was so well established as currency among the natives that the Court of Massachusetts ordered, in 1649, that it should be received in the payment of debts among settlers to the amount of forty shillings. It is curious to learn, too,

Currency in the Pastoral State.

In the next higher stage of civilization, the pastoral state, **sheep and cattle** naturally form the most valuable and negotiable kind of property. They are easily transferable, convey themselves about, and can be kept for many years, so that they readily perform some of the functions of money.

We have abundance of evidence, traditional, written, and etymological, to show this. In the Homeric poems oxen are distinctly and repeatedly mentioned as the commodity in terms of which other objects are valued. The arms of Diomed are stated to be worth nine oxen, and are compared with those of Glaucos, worth one hundred. **The tripod, the first prize for wrestlers in the 23rd Iliad, was valued at twelve oxen, and a woman captive, skilled in industry, at four.†** It is peculiarly

* "Travels in Alaska, etc.," by F. Whymper, p. 225.

† Gladstone, "Juventus Mundi," p. 534.

amount of forty shillings. It is curious to learn, too, that just as European misers hoard up gold and silver coins, the richer Indian chiefs secrete piles of wampum beads, having no better means of investing their superfluous wealth.

Exactly analogous to this North American currency, is that of the cowry shells, which, under one name or another—chamgos, zimbis, bouges, porcelanes, etc.—have long been used in the East Indies as small money. In British India, Siam, the West Coast of Africa, and else-

women as wives for the settlers, the price per head was one hundred pounds of tobacco, subsequently raised to one hundred and fifty. As late as 1732, the legislature of Maryland made tobacco and Indian corn legal tenders; and in 1641 there were similar laws concerning corn in Massachusetts. The governments of some of the West India Islands seem to have made attempts to imitate these peculiar currency laws, and it was provided that the successful plaintiff in a lawsuit should be obliged to accept various kinds of raw produce, such as sugar, rum, molasses, ginger, indigo, or tobacco.* Such endeavours to establish a kind of multiple currency will be found to possess considerable interest for us in a later chapter.

.....

of exchange.

Salt has been circulated not only in Abyssinia, but in Sumatra, Mexico, and elsewhere. Cubes of benzoin gum or beeswax in Sumatra, red feathers in the Islands of the Pacific Ocean, cubes of tea in Tartary, iron shovels or hoes among the Malagasy, are other peculiar forms of currency. The remarks of Adam Smith concerning the use of **hand-made nails as money** in some Scotch villages will be remembered by many readers, and need not be repeated. M. Chevalier has adduced an exactly corresponding case from one of the French coalfields.

Were space available it would be interesting to discuss the not improbable suggestion of Boucher de Perthes,

is the failure to observe that money requires different properties as regards different functions. To decide upon the best material for money is thus a problem of great complexity, because we must take into account at once the **relative importance of the several functions of money**, the degree in which money is employed for each function, and the importance of each of the physical qualities of the substance with respect to each function. In a simple state of industry money is chiefly required to pass about between buyers and sellers. It should, then, be conveniently **portable, divisible** into pieces of various size, so that any sum may readily be made up, and easily **distinguishable** by its appearance, or by the design impressed upon it. When money however comes to serve

complex questions, we must proceed to a preliminary discussion of the properties in question, which may thus perhaps be enumerated in the order of their importance:—

- | | |
|-----------------------|------------------------|
| 1. Utility and value. | 5. Divisibility. |
| 2. Portability. | 6. Stability of value. |
| 3. Indestructibility. | 7. Cognizability. |
| 4. Homogeneity. | |

Since money has to be exchanged for valuable goods, it should itself possess value, and it must therefore have utility as the basis of value. Money, when once in full currency, is only received in order to be passed on, so that if all people could be induced to take worthless bits of material at a fixed rate of valuation, it might seem that money does not really require to have substantial value. Something like this does frequently happen in the history of currencies, and apparently valueless shells, bits of leather, or scraps of paper, are actually received in exchange for costly commodities. This strange phenomenon is, however, in most cases capable of easy explanation, and if we were acquainted with the history of every kind of money the like explanation would no doubt be possible in other cases. The essential point is that people should be induced to receive money, and pass it on freely at steady ratios of exchange for other objects; but there must always be some sufficient reason first inducing people to accept the money. The force of habit, convention, or legal enactment may do much to maintain money in circulation when once it is afloat, but it is doubtful whether the most powerful government could oblige its subjects to accept and circulate as money a worthless substance which they had no other motive for receiving.

Coast of Africa, and were in all probability employed as ornaments before they were employed as money. All the other articles mentioned in Chapter IV., such as oxen, corn, skins, tobacco, salt, cacao nuts, etc., which have performed the functions of money in one place or other, possessed independent utility and value. If there are any apparent exceptions at all to this rule, they would doubtless admit of explanation by fuller knowledge. We may, therefore, agree with Storch when he says:—“It is impossible that a substance which has no direct value should be introduced as money, however suitable it may be in other respects for this use.”

When once a substance is widely employed as money,

There is, however, no reason to suppose that the value of gold and silver is at present due solely to their conventional use as money. These metals are endowed with such singularly useful properties that, if we could only get them in sufficient abundance, they would supplant all the other metals in the manufacture of household utensils, ornaments, fittings of all kinds, and an infinite multitude of small articles, which are now made of brass, copper, bronze, pewter, German silver, or other inferior metals and alloys.

intolerably bulky, and troublesome to transfer.

The portability of money is an important quality not merely because it enables the owner to carry small sums in the pocket without trouble, but because large sums can be transferred from place to place, or from continent to continent, at little cost. The result is to secure an approximate uniformity in the value of money in all parts of the world. A substance which is very heavy and bulky in proportion to value, like corn or coal, may be very scarce in one place and over abundant in another; yet the supply and demand cannot be

5. *Divisibility.*

Closely connected with the last property is that of divisibility. Every material is, indeed, mechanically divisible, almost without limit. The hardest gems can be broken, and steel can be cut by harder steel. But the material of money should be not merely capable of division, **but the aggregate value of the mass after division should be almost exactly the same as before division.** If we cut up a skin or fur the pieces will, as a general rule, be far less valuable than the whole skin or fur, except for a special intended purpose; and the same is the case with timber, stone, and most other materials in which reunion is impossible. But portions

prices were altered in like proportion as soon as money varied in value, no one would lose or gain, except as regards the coin which he happened to have in his pocket, safe, or bank balance. But, practically speaking, as we have seen, people do employ money as a standard of value for long contracts, and they often maintain payments at the same invariable rate, by custom or law, even when the real value of the payment is much altered. Hence every change in the value of money does some injury to society.

It might be plausibly said, indeed, that the debtor

at ninety pounds than it is at one hundred and ten. On the same principle, all gaming, betting, pure speculation, or other **accidental modes of transferring property involve**, on the average, a dead loss of utility. The whole incitement to industry and commerce and the accumulation of capital depends upon the expectation of enjoyment thence arising, and every variation of the currency tends in some degree to frustrate such expectation and to lessen the motives for exertion.

OF THE UNITED STATES GOVERNMENT

Under **cognizability** we may properly include what has been aptly called *impressibility*, namely, the capability of a substance to receive such an impression, seal, or design, as shall establish its character as current money of certain value. We might more simply say, that the material of money should be *coinable*, so that a portion, being once issued according to proper regulations with the impress of the state, may be known to all as good and legal currency, equal in weight, size, and value to all similarly marked currency. We shall afterwards consider more minutely what is involved in the manufacture of a good coin.

ANOTHER EXAMPLE.

Monarchs or states in difficulty have often coined the metal which they could most easily obtain. The Irish money issued by James II. was said to have been coined from a mixture of old guns, broken bells, waste copper, brass, and pewter, old kitchen furniture, and in fact any refuse metal which his officers could lay their hands upon. He attempted to make pewter crowns circulate for the value of silver ones.

has tampered with it. Even the amount of ordinary wear and tear, which the coin has suffered, may be rudely inferred from the sharpness or partial effacement of the designs, and the roundness of the edges. "Pieces of money," says M. Chevalier, "are ingots of which the weight and the fineness are certified." There is nothing in this definition to distinguish coins from Sycee silver, or from the ordinary stamped bars and ingots of bullion. I should prefer, therefore, to say, *coins are ingots of which the weight and fineness are certified by the integrity of designs impressed upon the surfaces of the metal.*

M. Chevalier and some other continental economists have argued elaborately in favour of a universal standard unit of value, coinciding with the metric system of weights. They wish the unit of value to be ten grams of gold exactly, and seem to think that there is some magical efficacy in the correspondence of money and weights. This correspondence might perhaps be a slight convenience to those bullion dealers who have to calculate the metallic value of coins before melting or exporting them, or to those mint officials who have to adjust and test the weights of coins; to all other persons it would be a matter of complete indifference. Those who use coins in ordinary business need never inquire how much metal they contain. Probably not one person in ten thousand in this kingdom knows, or need know, that a sovereign should contain 123·27447 grains of standard gold. Besides, if we agree to accept a precise metrical quantity of one metal as our standard, the weights of

The *money of account*, as it is called, may differ both from the current money and the standard money. This is well illustrated in the Anglo-Saxon system of currency. The unit of value was the Saxon pound of standard silver, which was far too large to be coined. The only coins issued in any considerable quantity by the Anglo-Saxon kings, were silver pennies and a few halfpennies; yet the usual money of account was the

Digitized by Google

shilling, which, after varying from four to five pence, was fixed by William I. at twelve pence, as it has ever since continued. No coin called a shilling was issued before the reign of Henry VII. Though the shilling

Standard and Token Money.

We must distinguish between coins according as they serve for *standard money* or for *token money*. **A standard coin is one of which the value in exchange depends solely upon the value of the material contained in it.** The stamp serves as a mere indication and guarantee of the quantity of fine metal. We may treat such coins as bullion, and melt them up or export them to countries where they are not legally current; yet the value of the metal being independent of legislation will everywhere be recognised.

Token coins, on the contrary, are defined in value by the fact that they can, by force of law or custom, be exchanged in a certain fixed ratio for standard coins. The metal contained in a token coin has of course a certain value; but it may be less than the legal value in almost any degree. In our English silver coinage the difference is from 9 to 12 per cent., according to the market price of silver; in our bronze coinage the difference is 75 per cent. The metal contained in the French bronze coins is in like manner equal in value to little

Legal Tender.

Money must further be distinguished, according as it is or is not *legal tender*, or has or has not what the French call *cours forcé*. By legal tender is denoted such money as a creditor is obliged to receive in requital of a debt expressed in terms of money of the realm. One great object of legislation is to prevent uncertainty in the interpretation of contracts, and accordingly the Coinage Act defines precisely what will constitute a legal offer of payment on the part of a debtor, as regards a money debt. If a debtor tender to his creditor the amount of a debt due in legal tender money, and it be refused, the creditor may indeed apply for it, or sue for

The Force of Habit in the Circulation of Money.

No one can possibly understand many social phenomena unless he constantly bears in mind the force of habit and social convention. This is strikingly true in our subject of money. Over and over again in the course of history, powerful rulers have endeavoured to put new coins into circulation or to withdraw old ones; but **the instincts of self-interest or habit in the people have been too strong for laws and penalties.** Though in particular instances it may be difficult to explain occurrences which happen in the circulation of coins, yet a close analysis of the character of those who handle money, and their motives for holding or paying it away, will throw much light upon the subject.

to restore the standard of the currency. A curious instance of successive attempts to beguile a people are found in certain Roman denarii of the Consular times. False coiners having issued plated denarii among the subject Germans, the people appeared to have notched them with files to test their genuineness. The Germans having thus become accustomed to see genuine *notched* coins, the Roman government found it desirable to issue new coins notched in a similar manner. But the forgers were not to be beaten. They issued plated denarii with the notches all complete, apparently displaying good metal within; and notched false coins of this kind exist to the present day in numismatic cabinets.

frequently *uncoin* money, either by melting it, or by exporting it to countries where it is sooner or later melted. Some coins are sunk in the sea or lost, and some are carried abroad by emigrants and travellers who do not look closely to the metallic value of the money. But by far the greatest part of the standard coinage is removed from circulation by people who know that they shall gain by choosing for this purpose the new heavy coins most recently issued from the mint. Hence arises the practice, extensively carried on in the present day in England, of *picking and culling*, or, as another technical expression is, *garbling* the coinage, devoting the good new coins to the melting-pot, and passing the old worn coins into circulation again on every suitable opportunity.

appropriately named the Law or Theorem of Gresham, after Sir Thomas Gresham, who clearly perceived its truth three centuries ago. This law, briefly expressed, is that *bad money drives out good money, but that good money cannot drive out bad money.* At first sight there may seem to be something paradoxical in the fact, that when beautiful new coins of full weight are issued from the mint, the people still continue to circulate, in preference, the old depreciated ones. Many well-intentioned efforts to reform a currency have thus been frustrated, to the great cost of states, and the perplexity of statesmen who had not studied the principles of monetary science.

Gresham's law alone furnishes a sufficient refutation of Mr. Herbert Spencer's doctrine, already noticed (p. 64) that money ought to be provided by private manufacturers. People who want furniture, or books, or clothes, may be trusted to select the best which they can afford, because they are going to keep and use these articles; but with money it is just the opposite. Money is made to go. They want coin, not to keep it in their own pockets, but to pass it off into their neighbours' pockets; and the worse the money which they can get their neighbours to accept, the greater the profit to themselves. Thus there is a natural tendency to the depreciation of the metallic currency, which can only be prevented by the constant supervision of the state.

the bullion-broker and exporter. In the second place, adequate measures must be taken for withdrawing from circulation all coins which are worn below the least legal weight, otherwise they will continue to circulate as token coins for an indefinite length of time. All commerce consists in the exchange of commodities of equal value, and the principal money should consist of pieces of metal so nearly equal in metallic contents, that all persons, including bullion dealers, bankers, and other professed dealers in money, will indifferently substitute one coin for another. But it is obvious that these remarks do not apply to coins intended to serve as tokens, since the current value of tokens exceeds their metallic value, and every one who uses them otherwise than in ordinary circulation will lose the difference. Hence the weight of a token coin is comparatively a matter of indifference, so long as people will receive them, and the deficiency of weight is not too great a temptation to the false coiner.

In England at the present day the force of habit, and the absence of means of discrimination, lead to the depreciation of our gold standard coinage by abrasion. Only while a sovereign exceeds 122·5 grains in weight is it legally a sovereign; but people go on paying and receiving indifferently, in ordinary trade, sovereigns of which the metallic values differ 2*d.* or 4*d.*, and sometimes even 6*d.* or 8*d.* **Every standard coin thus tends to degenerate into a token coin, and such a coin can only be withdrawn from circulation by the state.**

tion. Gold compared with silver, or silver with copper, or paper compared with gold, are subject to the same law that the relatively cheaper medium of exchange will be retained in circulation and the relatively dearer will disappear. The most extreme instance which has ever occurred was in the case of the Japanese currency. At the time of the treaty of 1858, between Great Britain, the United States, and Japan, which partially opened up the last country to European traders, a very curious system of currency existed in Japan. The most valuable Japanese coin was the kobang, consisting of a thin oval disc of gold about 2 inches long, and $1\frac{1}{4}$ inch wide, weighing 200 grains, and ornamented in a very primitive manner. It was passing current in the towns of Japan for four silver itzebus, but was worth in English money about 18s. 5d., whereas the silver itzebu was equal only to about 1s. 4d. Thus the Japanese were estimating their gold money at only about one-third of its value, as estimated according to the relative values of the metals in other parts of the world. The earliest European traders enjoyed a rare opportunity for making profit. By buying up the kobangs at the native rating they trebled their money, until the natives, perceiving what was being done, withdrew from circulation the remainder of the

legal ratio. At the rate adopted by Sir Isaac Newton, gold was overvalued by rather more than $1\frac{1}{2}$ per cent.; to that extent it was more valuable as currency than as metal. Therefore, in accordance with the Law of Gresham, and the principles laid down in Chapter VIII., the full weight silver coin was withdrawn or exported, and gold became the practical measure of value, which it has ever since continued to be.

In every other part of the world, where attempts have been made to combine two metals as concurrent standards of value, similar results have followed. In Massachusetts, in 1762, gold was made a legal tender, as well as silver, at the rate of $2\frac{1}{2}d.$ per grain; but, being overvalued as much as 5 per cent, the silver coinage rapidly disappeared from circulation. Various laws were passed to remedy this inconvenient state of things, but without success so long as this valuation of gold was maintained.

Every sovereign issued from the mint in accordance with these regulations, and bearing the impress authorized by the Queen, is legal tender, and must be accepted by a creditor in discharge of a debt to that amount, provided that it has not been reduced by wear or ill-treatment below the weight of 122·50 grains (7·93787 grams). If a sovereign of less than this *least current weight* be tendered to any person, he is presumed by the law to detect the deficiency, and is bound to cut or deface the coin, and return it to the tenderer, who must bear the loss. If the coin so defaced should prove not to be below the limit, then the defacer has to receive it and bear the loss arising from his mistake. Any justice of the peace may decide disputes arising concerning light sovereigns in a summary manner.

It would obviously be a cause of grievance if a person could be obliged to receive unlimited amounts of this token money in discharge of a debt. Merchants might often have thousands of pounds worth of such coins thrown upon their hands, the full value of which could only be realized by gradually putting it into circulation again. It was therefore provided by the Acts of 1816

Digitized by Google

and 1870, that silver coin shall be a legal tender only to the amount of forty shillings in any one payment. This limit was chosen apparently because the two-pound piece was in 1816 regarded as the largest coin then in circulation, or likely to be issued.

It is the theory of the present English monetary law, as we have seen (p. 107) that every person weighs a sovereign tendered to him, and assures himself, before accepting it, that it does not weigh less than 122·5 grains. In former days it was not uncommon for people to carry pocket-scales for weighing guineas, and such scales may still be occasionally seen in old curiosity shops. But we know that the practice is entirely given up, and that even the largest receivers of coin, such as the banks and railway companies, and even tax-offices, post-offices, etc., do not pay the least regard to the law. Only the Bank of England, its branches, and a few government offices, weigh gold coin in England. The result is that a large part of the gold coinage is worn below the least current weight, and all persons of experience avoid paying old sovereigns to the Bank of England. Only ignorant and unlucky persons, or else large banks and companies which cannot otherwise get rid of light coin, suffer loss.

In 1869 I ascertained, by a careful and extensive inquiry, that 31½ per cent. of the sovereigns and nearly one-half of the ten-shilling pieces were then below the legal limit. The reader who has attended to the remarks on Gresham's Law (p. 80), will see that no amount of coinage of new gold will drive out of circulation these depreciated old coins, because those who export, or melt, or otherwise treat the coins as bullion, will take care to operate upon good new ones.

Great injustice arises in some cases from this defective state of the gold currency. I have heard of one case in which an inexperienced person, after receiving several hundred pounds in gold from a bullion dealer in the city of London, took them straight to the Bank of England for deposit. Most of the sovereigns were there found to be light, and a prodigious charge was made upon the unfortunate depositor. The dealer in bullion had evidently paid him the residuum of a mass of coins, from which he had picked the heavy ones. In a still worse case, lately

Some steps must soon be taken to remedy the increasing deficiency of weight of the gold coinage described above. The withdrawal may no doubt be effected in several ways. One method would be for the Queen to issue a proclamation calling in and prohibiting the circulation of all gold coins more than twenty or twenty-five years old, as it is mostly the older coins which are deficient in weight. Another method would be to oblige all revenue officers, post-masters, and others, under the control of government, to weigh all sovereigns presented to them. If necessary, the bankers of the kingdom generally might be obliged to weigh coin. But it is obvious that great trouble and inconvenience would arise from such measures. The progress of the post-office savings banks would be imperilled if every depositor of a pound were liable to be charged 2 per cent. for lightness. Con-

siderable excitement and trouble followed the issue of the last proclamation of June, 1842, calling in light gold. To make the last holder of a coin pay for the whole cost of its circulation during thirty or forty years past, leads in many cases to gross injustice. **The present law tends to throw the loss upon the poor, who have usually only one or two sovereigns at a time to pay,** whereas rich people, having many, can avoid paying light gold at offices where it will be weighed.

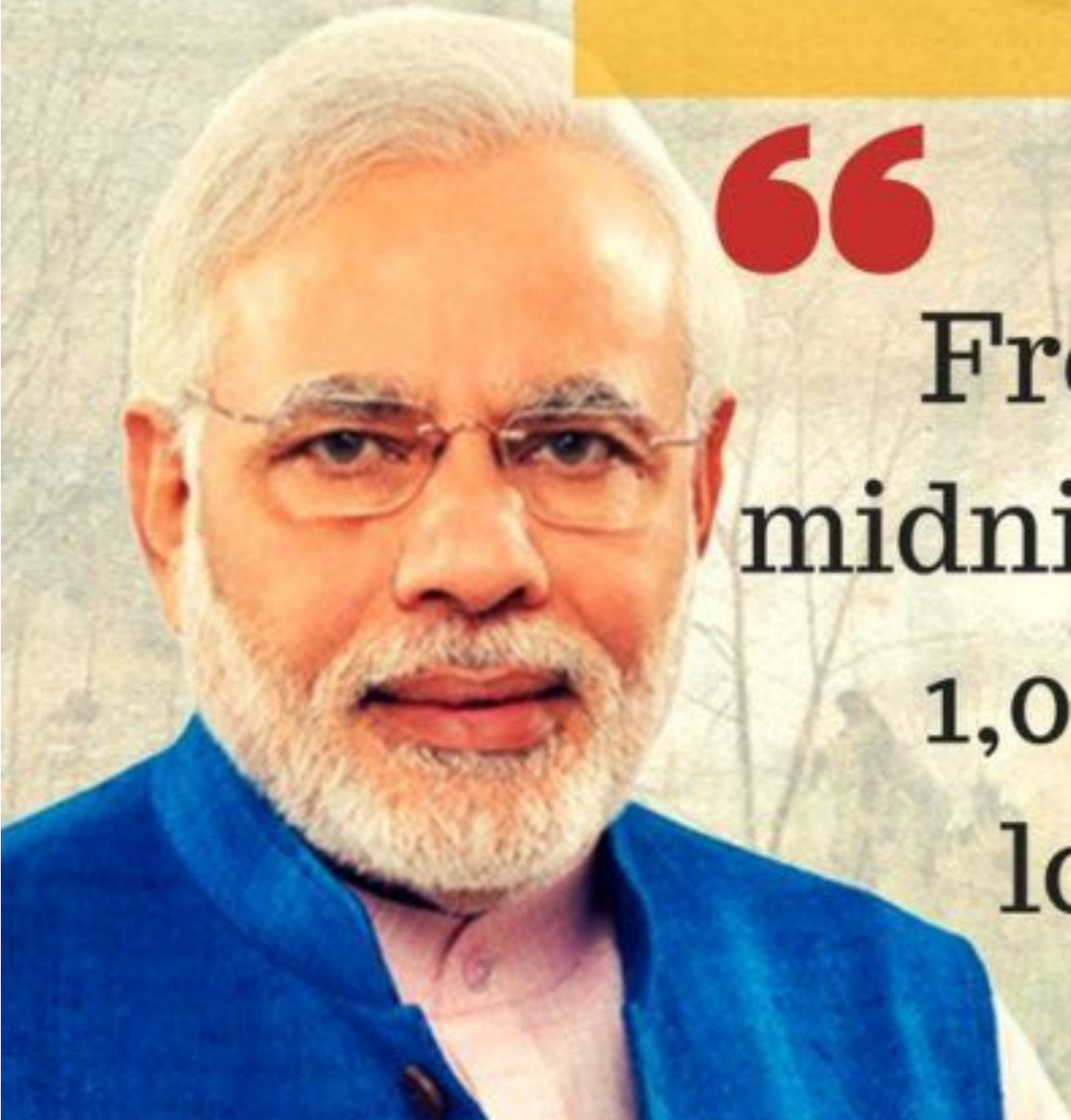
I hold that the only thorough remedy is for the government to bear the loss occasioned by the wear of the gold, as it already bears that of the silver currency. **The Bank of England should be authorized to receive all sovereigns showing no marks of intentional damage or unfair treatment at their full nominal value,** on behalf of the mint, which should recoin the light ones at the public expense. No one would then have any reason for keeping the light gold away from the bank; the currency would soon be purged of the illegally light coins, and would thenceforth be kept up strictly to the standard weight; all loss of time and trouble would be saved to individuals,

on Black Money

“

From 8 November
midnight, Rs 500 and Rs
1,000 notes will no
longer be valid.

”





STATE BANK OF INDIA
ATM

Chopra FURNITURE

Blue and white striped awning

नेताजी गलती

नेताजी गलती

नेहरू

नेहरू

नेहरू

The Enforcement Directorate (ED) has busted a network of jewellers which was converting old Rs.500 and Rs.1000 notes into gold in connivance with bank officials. The money was being laundered using the banking channel through entry operators, including a chartered accountant, and shell companies.

The gold purchased by the accused jewellers in the name of a shell company was again sold to other cash hoarders at prices higher than the legal prevailing rate.

The ED has arrested Shashank Sinha and Vinit Gupta, managers of Axis Bank's Kashmere Gate branch here, for allegedly helping the cash hoarders deposit close to Rs.40 crore in several bank accounts and transfer funds online. The ED has directed the banks concerned to freeze all transactions in 11 accounts for further scrutiny.

But these goals were never met. 97% of the demonetized notes were turned in, meaning that very little black money was caught stranded and the central bank's estimated \$45 billion bonus never transpired. India's black market — as dynamic and active as it is — rarely stores money in cash long-term, as its players prefer other ways of storing wealth, such as jewelry or property, and what cash they were stuck with was mostly exchanged through clever tactics or brute force.

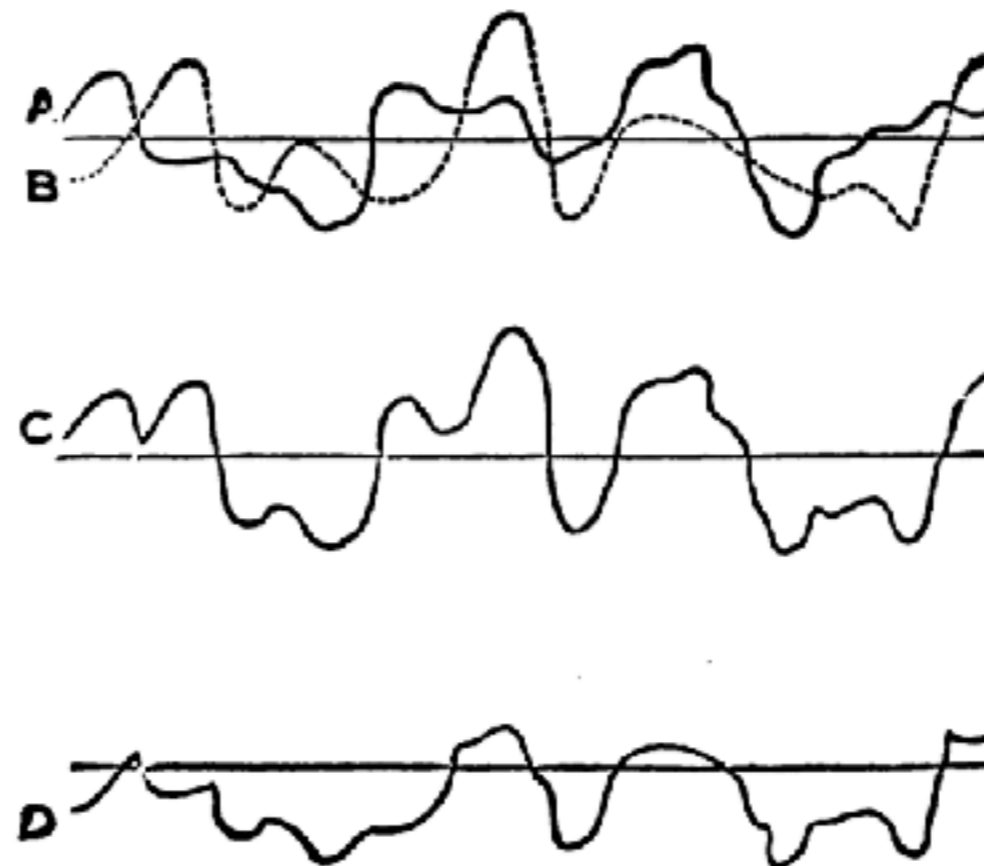
But these goals were never met. **97% of the demonetized notes were turned in**, meaning that very little black money was caught stranded and the central bank's estimated \$45 billion bonus never transpired. India's black market — as dynamic and active as it is — rarely stores money in cash long-term, as its players prefer other ways of storing wealth, such as jewelry or property, and what cash they were stuck with was mostly **exchanged through clever tactics or brute force**.

The other main goal of demonetization was to disrupt the cash-centric and largely untaxed informal economy by getting a larger slice of the population onto the digital economic grid.

Prior to demonetization, Indians used cash for upwards of 95% of all payments and 90% of the country's vendors didn't have the means to accept anything but. Even Uber in India accepted cash payments and most ecommerce sites had a cash on delivery option.

But this was an aspect of Indian life that was to be fundamentally upgraded. Demonetization was a stark success in its ability to get people to open bank accounts for the first time and to get acquainted with electronic payment systems. The way this was carried out was straight forward: people weren't really given another choice.

metal which happens to have sunk in value below the legal ratio of $15\frac{1}{2}$ to 1. Now, if in the accompanying figure we represent by the line A the variation of the value of gold as estimated in terms of some third commodity, say copper, and by the line B the corresponding variations of the value of silver; then, superposing these curves, the line C would be the curve expressing the *extreme* fluctuations of both metals. Now the standard of value always follows the metal which *falls* in value; hence the curve D really shows the course of variation of the standard of value. This line undergoes more frequent undulations than either of the curves of gold or silver, but the fluctuations do not proceed to so great an extent, a point of much greater importance.



Nor is this the whole error of the English writers. A little reflection must show that MM. Wolowski and Courcelle-Seneuil are quite correct in urging that a *compensatory* or, as I should prefer to call it, *equilibratory action*, goes on under the French currency law, and tends to maintain both gold and silver more steady in value than they would otherwise be. If silver becomes more valuable than in the ratio of 1 to $15\frac{1}{2}$ compared with gold, there arises at once a tendency to import gold into any country possessing the double standard, so that it may be coined there, and exchanged for a legally equivalent weight of silver coin, to be exported again. This is no matter of theory only, the process having gone on in France until the principal currency, which was mainly composed of silver in 1849, was in 1860 almost wholly of gold. France absorbed the cheapened metal in vast quantities and emitted the dearer metal, which must have had the effect of preventing gold from falling and silver from rising so much in value as they would otherwise have done. It is obvious that, if gold rose in value compared with silver, the action would be reversed; gold would be absorbed and silver liberated. At any moment the standard of value is doubtless one metal or the other, and not both; yet the fact that there is an alternation tends to make each vary much less than it would otherwise do. It cannot prevent both metals from falling or rising in value compared with other commodities, but it can throw

Imagine two reservoirs of water, each subject to independent variations of supply and demand. In the absence of any connecting pipe the level of the water in each reservoir will be subject to its own fluctuations only. But if we open a connection, the water in both will assume a certain mean level, and the effects of any excessive supply or demand will be distributed over the whole area of both reservoirs. The mass of the metals, gold and silver, circulating in Western Europe in late years, is exactly represented by the water in these reservoirs, and the connecting pipe is the law of the 7th Germinal, an XI, which enables one metal to take the place of the other as an unlimited legal tender.

In short, then, the amount of supply and amount of demand of both the precious metals depend upon a number of accidents, changes, or legislative decisions, which cannot be in any way predicted. The price of silver has fallen in consequence of the German currency reforms, but it is by no means certain that it will fall further than it has already done. That any great rise will really happen in the purchasing power of gold is wholly a matter of speculation. We cannot do more than make random guesses on the subject, and, as a mere guess, I should say that it is not likely to rise. Gold has since 1851 been falling in value, and an increased demand for gold is not likely to do more than slacken, or at the most arrest, the progress of depreciation.

It is remarkable that the changes thus effected in the money of Western Europe are almost the same as those by which the United States had previously abandoned the double standard. Until the year 1853 the silver dollar of the United States mint was a standard coin of unrestricted legal tender, concurrently with the gold coinage of eagles and their fractions. The legal ratio of silver to gold in weight indeed, was 16 to 1, instead of $15\frac{1}{2}$ to 1 as in France. More silver being thus required to make a legal payment in America than elsewhere, gold was naturally preferred for this purpose, and the silver was sent abroad. To remedy this state of things the government of Washington, in 1853, reduced the half-dollar and smaller silver pieces to the condition of token coins, and though the single silver dollar pieces remained of standard weight, they were coined in very small quantities and were practically suppressed. The predominance of an inconvertible paper currency suspended the question of metallic money for a time. The Coinage Act of the United States Congress came into operation on 1st April, 1873, and constituted the gold one-dollar piece the sole unit of value, whilst it restricted the legal tender of the new silver trade dollar, and of the half-dollar and its subdivisions, to an amount not exceeding five dollars in any one payment. Thus the double standard previously existing in theory was finally abolished, and the United States was added to the list of nations adopting the single gold standard.

Becoming a billionaire from
these principles

A precursor to the EU was the European Exchange Rate mechanism ([ERM](#)), which was created in 1979. Countries weren't ready to give up their national currencies, but they agreed to fix their exchange rates with each other instead of "floating" their currency and letting capital markets set the rates. Since Germany had the strongest economy in Europe, each country set their currency's value in Deutschmarks. They agreed to maintain the exchange rate between their currency and the Deutschmark within an acceptable band of plus or minus 6% of the agreed upon rate.

With fixed exchange rates, countries can't just "set it and forget it." People trade currency every day, exchanging their currency to buy imports or sell exports, and the market applies pressure based on what it thinks the actual rate should be based on supply and demand for a currency. To keep the exchange rate fixed, governments need to participate in the market and nudge it in the agreed upon direction.

Governments can manage their currency in two main ways. First, they can take their reserves of foreign currency and buy up their own currency on the open market. That causes the currency to appreciate. Doing the opposite devalues the currency.

Alternatively, governments can influence exchange rates by setting interest rates. Want your currency to appreciate? Raise rates to entice people to buy your currency and lend that money at higher interest rates. Want your currency to depreciate? Cut interest rates so capital needs to go elsewhere in search of juicy profits.

Messing around with interest rates is a big deal, however, because interest rates affect the whole economy. Along with government spending, interest rates are the main lever governments can use to adjust the economy. If the country is experiencing a recession, the government might cut interest rates to spur investment and spending. If inflation is high, the government might raise rates to shrink the supply of money.

In 1990, Britain was a country that arguably could use an external forcing function to tie its hands on monetary policy. Inflation was high, productivity was low, exports were uncompetitive, and no one really believed the government was capable of fixing the issues.

The Prime Minister at the time, Margaret Thatcher, had long opposed entering the ERM, insisting that the price of the pound be set by the markets. By 1990, however, Thatcher lacked the political power to oppose other members of her Conservative party who wanted to fix their exchange rates with the rest of Europe.

The decision to join the ERM was championed by John Major, who was the Chancellor of the Exchequer in Thatcher's cabinet. In October 1990, Britain finally entered the ERM at an exchange rate of 2.95 Deutschmark (DM) for each British pound (GBP). The British government was obligated to keep the exchange rate within 2.78 DM to 3.13 DM.

Shortly thereafter, Major replaced Thatcher as the Prime Minister. The fixed exchange rate system was to be the centerpiece of his economic plan. [Major thought](#) that the ERM would serve as a sort of "autopilot" that kept the British monetary policy on proper course. The government couldn't play with the money supply willy-nilly because its hands were tied by the exchange rate agreement.

And to a certain extent, the policy worked. Between 1990 and 1992, inflation decreased, interest rates eased, and unemployment was low by historical standards. In 1992, however, England felt the impact of a massive global recession, and [unemployment spiked](#) to 12.7% from just 7.7% two years prior.

And so we come to 1992. Ordinarily, Britain could spur investment and spending by cutting interest rates during an employment crisis. But in this case, doing so would push the pound's value below the agreed upon amount. So while the people of Great Britain dealt with a recession, the government's hands were tied; they'd just have to ride it out.

By the spring of 1992, just a year and a half after Britain joined the ERM, the fixed exchange rate posed a serious problem. While putting on a cheery public face, internally the Exchequer (England's Treasury department) realized that the currency was mispriced relative to the Deutschemark. Jonathan Portes, an economist who was at the time a junior staff member there, [wrote](#):

"In May 1992, the immediate problem was obvious. From a domestic point of view, the appropriate level of interest rates, given weak demand, was much lower than that necessary to maintain [the] sterling's position in the ERM.

Moreover, it was becoming increasingly clear that sterling was overvalued; even in the depths of a recession, we still had a large current account deficit [the country was importing more than it exported].

We argued that the fundamental problem was that we'd joined the ERM at the wrong rate; sterling was overvalued, meaning that we were stuck with a structural current account deficit."

The sterling was priced too high. The British government knew it, and the market knew it too as the pound was trading at the lower end of the agreed upon band with the Deutschemark.

What kept the pound from plummeting in value was the British government's guarantee that it would keep the value propped up, and the market believed that it would. As long as everyone believed that England would stay indefinitely committed to buying pounds for around 2.95 Deutschemarks, the status quo was maintained.

Throughout the summer of 1992, the British pound held its position. That is, until Germany threw Britain under the bus and all hell broke loose.

For some time that year, German central bank officials made comments on and off the record that undermined the sterling's strength. The British paper *The Independent* documents the [slights](#):

"On 25 August, for example, Reimut Jochimsen, a Bundesbank council member, issued a speech saying that there was potential for realignment within the ERM. Sterling weakened. On 10 September, an unnamed Bundesbank official was quoted as saying that a devaluation of sterling was inevitable. The pound fell."

The event that ultimately [led to the undoing](#) of the British pound's fixed exchange rate was an interview with the President of the German Bundesbank, Helmut Schlesinger. Schlesinger gave the interview to the *Wall Street Journal* and a German newspaper. He had one condition: If they wanted to directly quote him, they had to let him review the quotes. If they only indirectly paraphrased him, no such permission was necessary.

"The President of the Bundesbank, Professor Helmut Schlesinger, does not rule out the possibility that, even after the realignment and the cut in German interest rates, one or two currencies could come under pressure before the referendum in France. He conceded in an interview that the problems are of course not solved completely by the measures taken."

Since August, Soros and his Quantum Fund had been building a **\$1.5 billion** position to bet that the price of Sterling would fall. Since the British government's full faith and credit was stating that it would not fall, this wasn't necessarily something that was going to happen. But **Stanley Druckenmiller**, a senior member of the fund, saw the report from Schlesinger and immediately realized its importance.

Sebastian Mallaby's book *More Money Than God* recounts the day's events. According to Mallaby, Druckenmiller noted that their \$1.5 billion bet against the pound was about to pay off and that they should consider adding to the position.

Soros retorted with a different strategy: "*Go for the jugular.*"

And what if you want to short a currency like the British pound? In this case, you'd go to a British person or company and ask to borrow money from them. They say, "Sure, here's 100 British pounds. Just give me back the pounds in a few days with some interest, and we'll have some tea and crumpets." Now, you take those 100 British pounds, and you convert them into 295 Deutschmarks at the agreed upon exchange rate.

At this point, you would really like the British pound to lose value relative to the Deutschmark. Why? Because if the British pound depreciates 10%, when you convert the 295 DM back to pounds to repay the loan, you'll have 110 pounds. You can pay back the 100 pounds and a little bit of interest, and you'll still clear about 10 pounds in profit.

So you make money if the pound devalues. But what if the pound appreciates? You'll lose your shirt. Therein lies the brilliance of Soros's bet: if the pound tanked, they would make billions on their short. And if the pound increased in value? Well, that scenario was impossible because everyone knew the sterling was over priced. It already traded at the bottom of its trading band, and the only thing that kept it propped up was government intervention. There was no scenario in which the pound would appreciate.

And so that morning, Soros and his fund increased their short position against the British pound from **\$1.5 to \$10 billion**. It was the perfect bet with a mitigated downside and a limitless upside. It was like betting on a coin flip, were if the coin lands on heads (the pound devalues), they make a lot of money. If the coin lands on tails (the exchange rates remained fixed), they only lose a small amount of money on loan interest. That's the kind of bet Soros would pour money into all the day, even if he had to borrow billions.

British officials first responded by buying **one billion pounds at 8:40 AM**. The purchase had no effect on the price of the pound. The whole world was selling, and the British government didn't have the buying power to fight it all off. It's estimated that the British government spent £27 billion of its reserves buying up pounds to no avail.

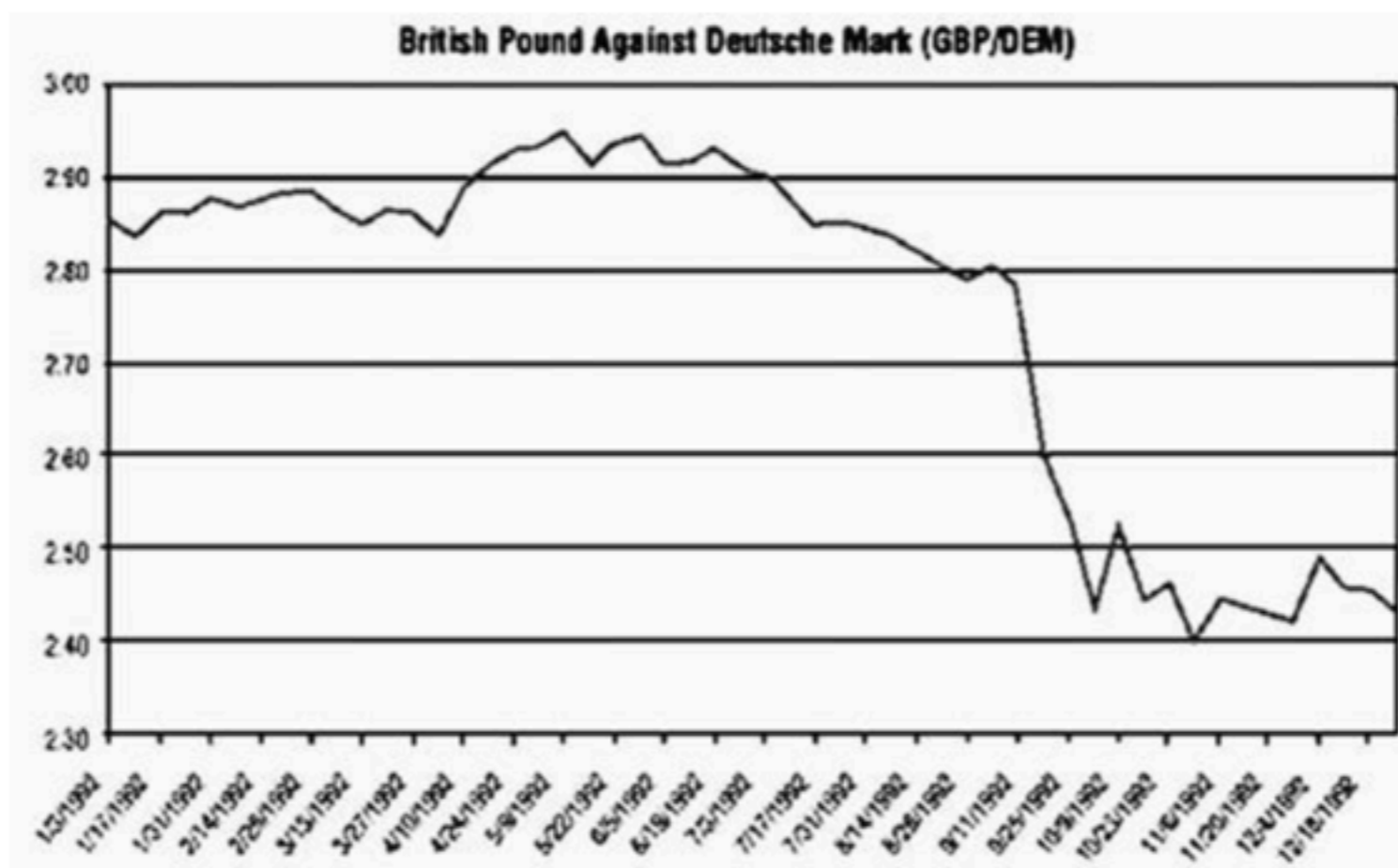
By **9AM**, finance minister Norman Lamont contacted Prime Minister John Major and told him they couldn't possibly buy up enough pounds to keep the currency propped up. The only option left for the British government to keep their currency trading at the right level would be to increase interest rates dramatically and attract people to buy pounds. Major **refused**. Britain was in the midst of a recession, and increasing rates would further shrink the economy. It would be political suicide.

Blood was in the water. Global capital continued to bet against the pound. An hour and a half later, Lamont called the Prime Minister to re-plead his case. The Prime Minister relented. At **11AM**, the British government announced they would increase interest rates 200 basis points, from 10% to 12%.

How did the value of the pound react to this enormous increase in interest rates? Nothing happened. The pound **continued to plummet**. Lamont headed to the Prime Minister's residence to figure out how to salvage the situation, which led them to announce an interest rate increase of another 300 basis points, from 12% to 15%.

What was the effect of this rate increase on the sterling? Again, nothing. As Mallaby later documents in his **book**, Soros and the gang of speculators knew victory was near:

British financial history now refers to September 17, 1992, as "Black Wednesday;" George Soros, however, probably calls it something like "Awesome Wednesday." Once Great Britain floated its currency, the **pound fell** 15% versus the Deutsche Mark and 25% versus the US Dollar.



L3

Currency Markets & Arbitrage

abhi shelat

the bullion-broker and exporter. In the second place, adequate measures must be taken for withdrawing from circulation all coins which are worn below the least legal weight, otherwise they will continue to circulate as token coins for an indefinite length of time. All commerce consists in the exchange of commodities of equal value, and the principal money should consist of pieces of metal so nearly equal in metallic contents, that all persons, including bullion dealers, bankers, and other professed dealers in money, will indifferently substitute one coin for another. But it is obvious that these remarks do not apply to coins intended to serve as tokens, since the current value of tokens exceeds their metallic value, and every one who uses them otherwise than in ordinary circulation will lose the difference. Hence the weight of a token coin is comparatively a matter of indifference, so long as people will receive them, and the deficiency of weight is not too great a temptation to the false coiner.

In England at the present day the force of habit, and the absence of means of discrimination, lead to the depreciation of our gold standard coinage by abrasion. Only while a sovereign exceeds 122·5 grains in weight is it legally a sovereign; but people go on paying and receiving indifferently, in ordinary trade, sovereigns of which the metallic values differ 2*d.* or 4*d.*, and sometimes even 6*d.* or 8*d.* **Every standard coin thus tends to degenerate into a token coin, and such a coin can only be withdrawn from circulation by the state.**

Every sovereign issued from the mint in accordance with these regulations, and bearing the impress authorized by the Queen, is legal tender, and must be accepted by a creditor in discharge of a debt to that amount, provided that it has not been reduced by wear or ill-treatment below the weight of 122.50 grains (7.93787 grams). If a sovereign of less than this *least current weight* be tendered to any person, he is presumed by the law to detect the deficiency, and is bound to cut or deface the coin, and return it to the tenderer, who must bear the loss. If the coin so defaced should prove not to be below the limit, then the defacer has to receive it and bear the loss arising from his mistake. Any justice of the peace may decide disputes arising concerning light sovereigns in a summary manner.

In 1869 I ascertained, by a careful and extensive inquiry, that 31½ per cent. of the sovereigns and nearly one-half of the ten-shilling pieces were then below the legal limit. The reader who has attended to the remarks on Gresham's Law (p. 80), will see that no amount of coinage of new gold will drive out of circulation these depreciated old coins, because those who export, or melt, or otherwise treat the coins as bullion, will take care to operate upon good new ones.

Great injustice arises in some cases from this defective state of the gold currency. I have heard of one case in which an inexperienced person, after receiving several hundred pounds in gold from a bullion dealer in the city of London, took them straight to the Bank of England for deposit. Most of the sovereigns were there found to be light, and a prodigious charge was made upon the unfortunate depositor. The dealer in bullion had evidently paid him the residuum of a mass of coins, from which he had picked the heavy ones. In a still worse case, lately

Some steps must soon be taken to remedy the increasing deficiency of weight of the gold coinage described above. The withdrawal may no doubt be effected in several ways. One method would be for the Queen to issue a proclamation calling in and prohibiting the circulation of all gold coins more than twenty or twenty-five years old, as it is mostly the older coins which are deficient in weight. Another method would be to oblige all revenue officers, post-masters, and others, under the control of government, to weigh all sovereigns presented to them. If necessary, the bankers of the kingdom generally might be obliged to weigh coin. But it is obvious that great trouble and inconvenience would arise from such measures. The progress of the post-office savings banks would be imperilled if every depositor of a pound were liable to be charged 2 per cent. for lightness. Con-

siderable excitement and trouble followed the issue of the last proclamation of June, 1842, calling in light gold. To make the last holder of a coin pay for the whole cost of its circulation during thirty or forty years past, leads in many cases to gross injustice. **The present law tends to throw the loss upon the poor, who have usually only one or two sovereigns at a time to pay,** whereas rich people, having many, can avoid paying light gold at offices where it will be weighed.

I hold that the only thorough remedy is for the government to bear the loss occasioned by the wear of the gold, as it already bears that of the silver currency. **The Bank of England should be authorized to receive all sovereigns showing no marks of intentional damage or unfair treatment at their full nominal value,** on behalf of the mint, which should recoin the light ones at the public expense. No one would then have any reason for keeping the light gold away from the bank; the currency would soon be purged of the illegally light coins, and would thenceforth be kept up strictly to the standard weight; all loss of time and trouble would be saved to individuals,

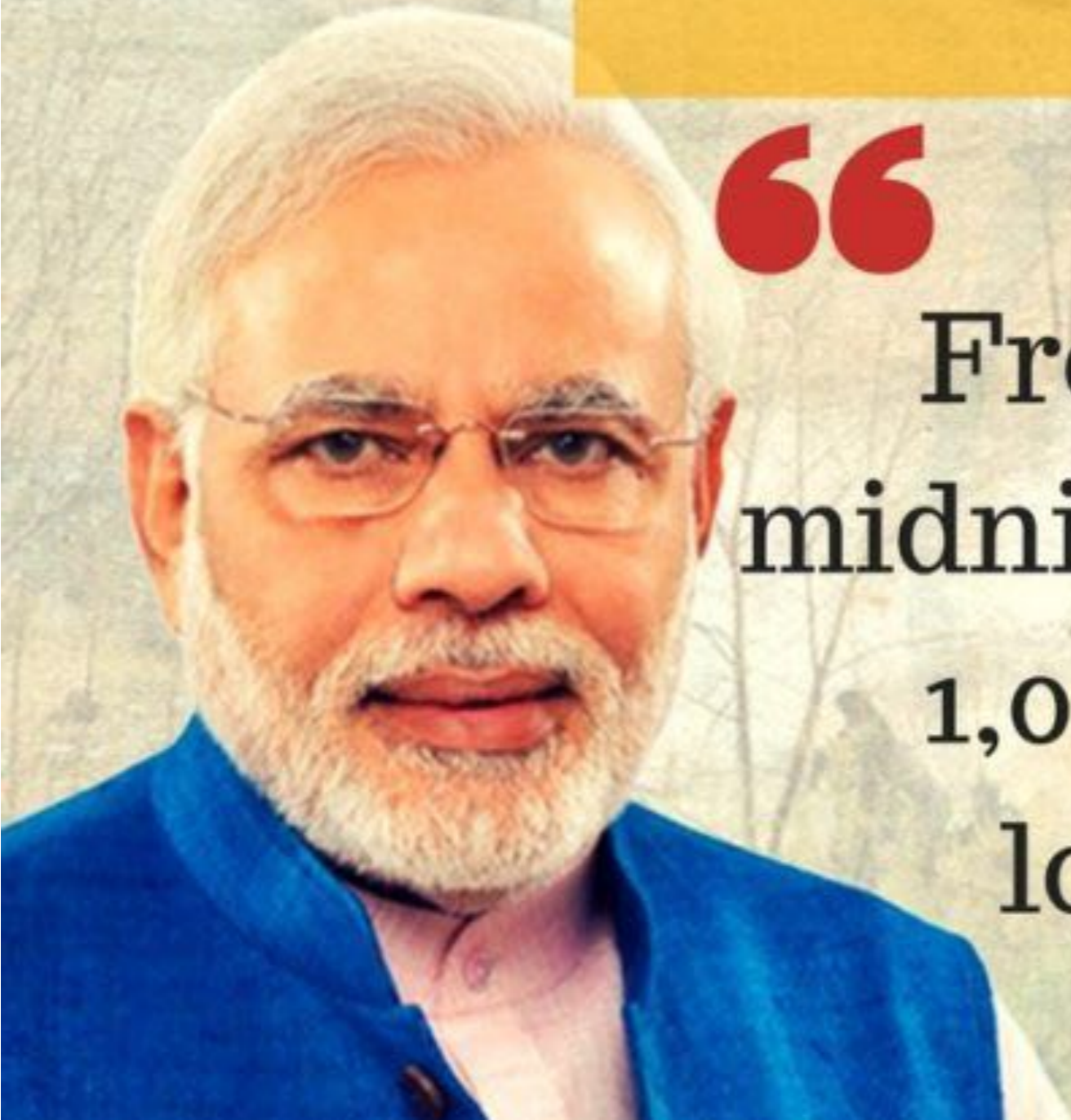
Running a currency takes
resources

on Black Money

“

From 8 November
midnight, Rs 500 and Rs
1,000 notes will no
longer be valid.

”





बैंक ऑफ इंडिया
STATE BANK OF INDIA
ATM

Chopra
FURNITURE

नेताजी गलती

नेताजी गलती

नेताजी गलती

नेहा

But these goals were never met. 97% of the demonetized notes were turned in, meaning that very little black money was caught stranded and the central bank's estimated \$45 billion bonus never transpired. India's black market — as dynamic and active as it is — rarely stores money in cash long-term, as its players prefer other ways of storing wealth, such as jewelry or property, and what cash they were stuck with was mostly exchanged through clever tactics or brute force.

But these goals were never met. **97% of the demonetized notes were turned in**, meaning that very little black money was caught stranded and the central bank's estimated \$45 billion bonus never transpired. India's black market — as dynamic and active as it is — rarely stores money in cash long-term, as its players prefer other ways of storing wealth, such as jewelry or property, and what cash they were stuck with was mostly **exchanged through clever tactics or brute force**.

The other main goal of demonetization was to disrupt the cash-centric and largely untaxed informal economy by getting a larger slice of the population onto the digital economic grid.

Prior to demonetization, Indians used cash for upwards of 95% of all payments and 90% of the country's vendors didn't have the means to accept anything but. Even Uber in India accepted cash payments and most ecommerce sites had a cash on delivery option.

But this was an aspect of Indian life that was to be fundamentally upgraded. Demonetization was a stark success in its ability to get people to open bank accounts for the first time and to get acquainted with electronic payment systems. The way this was carried out was straight forward: people weren't really given another choice.

The Mint operates six facilities and employs approximately 1,700 employees across the United States.



The Mint operates six facilities and employs approximately 1,700 employees across the United States.

The production of numismatic products is financed through sales to the public. The production of circulating coinage is financed through sales of coins at face value to the Federal Reserve Banks (FRBs).



The Mint operates six facilities and employs approximately 1,700 employees across the United States.

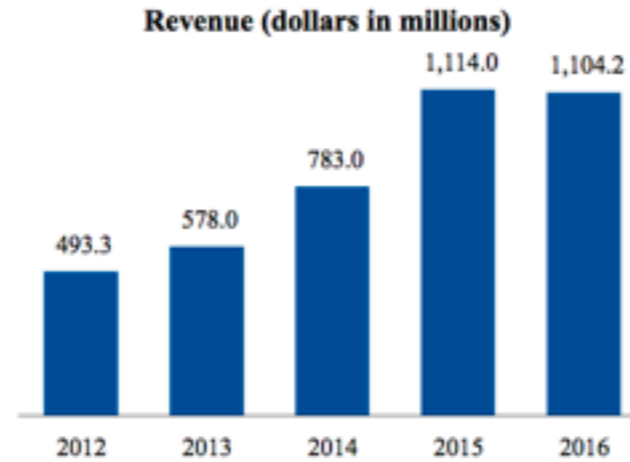


The production of numismatic products is financed through sales to the public. The production of circulating coinage is financed through sales of coins at face value to the Federal Reserve Banks (FRBs).

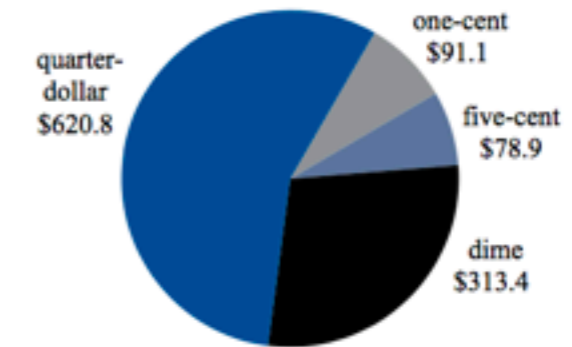
FY 2016 Protection costs increased by 10.6 percent to \$45.0 million compared to \$40.7 million last year.

CIRCULATING COINAGE

The Mint is the sole manufacturer of legal tender coinage in the United States. The Mint's highest priority is to efficiently and effectively mint and issue circulating coinage.

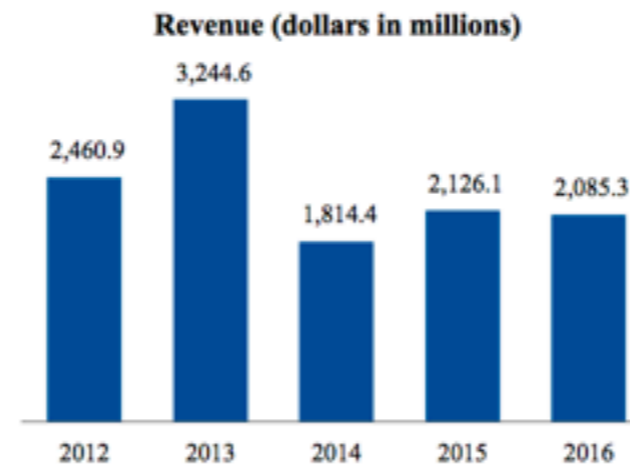


Revenue by Denomination (dollars in millions)

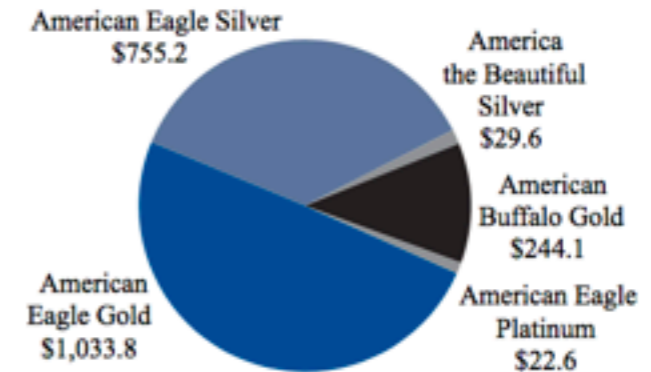


BULLION COINS

The Mint is the world's largest producer of gold and silver bullion coins. The bullion coin program provides consumers a simple and tangible means to acquire precious metal coins. Investors purchase bullion coins for the intrinsic metal value and the United States Government's guarantee of each coin's metal weight, content, and purity.

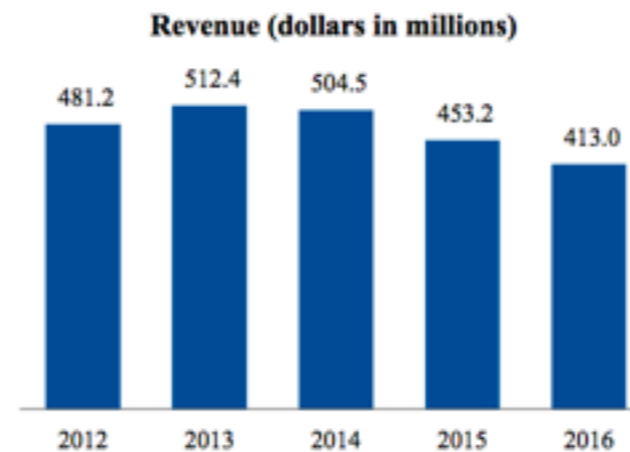


Revenue by Program (dollars in millions)

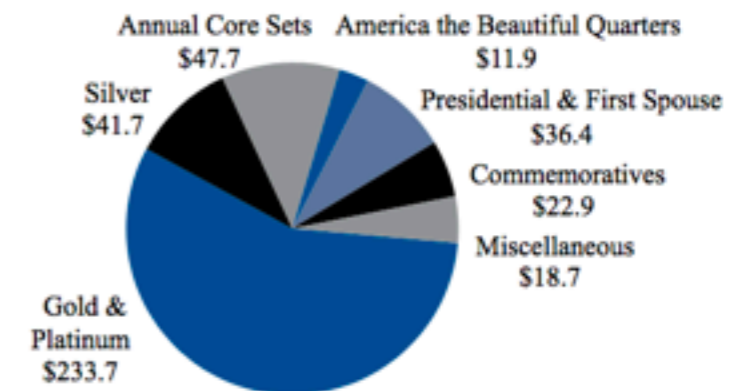


NUMISMATIC PRODUCTS

The Mint prepares and distributes numismatic products for collectors and those who desire high-quality versions of coinage. Most of the Mint's recurring products are required by Federal statute. Others are required by individual public laws.



Revenue by Program (dollars in millions)



UNIT COST OF PRODUCING AND DISTRIBUTING COINS BY DENOMINATION

2016	One-Cent	Five-Cent	Dime	Quarter-Dollar
Cost of Goods Sold	\$ 0.0131	\$ 0.0551	\$ 0.0269	\$ 0.0672
Selling, General & Administrative	\$ 0.0017	\$ 0.0071	\$ 0.0034	\$ 0.0080
Distribution to FRB	\$ 0.0002	\$ 0.0010	\$ 0.0005	\$ 0.0011
Total Unit Cost	\$ 0.0150	\$ 0.0632	\$ 0.0308	\$ 0.0763
2015	One-Cent	Five-Cent	Dime	Quarter-Dollar
Cost of Goods Sold	\$ 0.0125	\$ 0.0664	\$ 0.0315	\$ 0.0755
Selling, General & Administrative	\$ 0.0015	\$ 0.0068	\$ 0.0033	\$ 0.0076
Distribution to FRB	\$ 0.0003	\$ 0.0012	\$ 0.0006	\$ 0.0013
Total Unit Cost	\$ 0.0143	\$ 0.0744	\$ 0.0354	\$ 0.0844
2014	One-Cent	Five-Cent	Dime	Quarter-Dollar
Cost of Goods Sold	\$ 0.0143	\$ 0.0699	\$ 0.0338	\$ 0.0775
Selling, General & Administrative	\$ 0.0021	\$ 0.0102	\$ 0.0049	\$ 0.0109
Distribution to FRB	\$ 0.0002	\$ 0.0008	\$ 0.0004	\$ 0.0011
Total Unit Cost	\$ 0.0166	\$ 0.0809	\$ 0.0391	\$ 0.0895

DEPARTMENT OF THE TREASURY UNITED STATES MINT**STATEMENTS OF NET COST**

For the years ended September 30, 2016 and 2015

	2016	2015
	(dollars in thousands)	
Numismatic Production and Sales		
Gross Cost	\$ 2,402,850	\$ 2,445,903
Less Earned Revenue	(2,467,131)	(2,547,728)
Net Program Cost (Revenue)	(64,281)	(101,825)
Numismatic Production and Sales of Circulating Coins		
Gross Cost	5,590	5,599
Less Earned Revenue (Note 16)	(5,590)	(5,599)
Net Program Cost (Revenue)	-	-
Circulating Production and Sales		
Gross Cost	525,535	573,142
Less Earned Revenue (Note 16)	(525,535)	(573,142)
Net Program Cost (Revenue)	-	-
Net Cost (Revenue) Before Protection of Assets	(64,281)	(101,825)
Protection of Assets		
Protection Costs	45,017	40,724
Less Earned Revenue	-	-
Net Cost of Protection of Assets	45,017	40,724
Net Cost (Revenue) from Operations (Notes 14 and 15)	\$ (19,264)	\$ (61,101)

The accompanying notes are an integral part of these financial statements

DEPARTMENT OF THE TREASURY UNITED STATES MINT

STATEMENTS OF BUDGETARY RESOURCES

For the years ended September 30, 2016 and 2015

	2016	2015
	(dollars in thousands)	
Budgetary Resources:		
Unobligated balance, brought forward, October 1	\$ 576,217	\$ 377,478
Recoveries of prior-year unpaid obligations	16,618	15,469
Other changes in unobligated balance	(57,941)	(10,985)
Unobligated balance from prior year budget authority, net	<u>534,894</u>	<u>381,962</u>
Spending Authority from Offsetting Collections	3,043,410	3,131,164
Total Budgetary Resources	<u>\$ 3,578,304</u>	<u>\$ 3,513,126</u>
Status of Budgetary Resources:		
Obligations Incurred (Note 17)	\$ 3,277,573	\$ 2,936,909
Unobligated balance, end of year	300,731	576,217
Apportioned	183,851	576,217
Unapportioned	116,880	-
Total Budgetary Resources	<u>\$ 3,578,304</u>	<u>\$ 3,513,126</u>
Change in Obligated Balances:		
Unpaid obligations:		
Unpaid obligations, brought forward, October 1	\$ 431,928	\$ 409,279
Obligations Incurred (Note 17)	3,277,573	2,936,909
Gross Outlays	(3,265,655)	(2,898,791)
Recoveries of Prior Year Unpaid Obligations	(16,618)	(15,469)
Unpaid obligations, end of year	<u>\$ 427,228</u>	<u>\$ 431,928</u>
Uncollected Payments:		
Uncollected customer payments from Federal		
Sources, Brought Forward, October 1	\$ -	\$ (5,984)
Change in uncollected customer payments from Federal sources	-	5,984
Uncollected payments, Federal sources, end of year	<u>\$ -</u>	<u>\$ -</u>
Memorandum (non-add) entries:		
Obligated balance, start of year	\$ 431,928	\$ 403,295
Obligated Balance, end of year	<u>\$ 427,228</u>	<u>\$ 431,928</u>
Budget Authority and Outlays, Net:		
Budget Authority, gross	\$ 3,043,410	\$ 3,131,164
Actual offsetting collections	(3,046,469)	(3,137,163)
Change in uncollected customer payments from Federal Sources	-	5,984
Recoveries of prior year paid obligations	3,059	15

The following chart reflects the amount of reimbursable obligations incurred against amount apportioned under categories B apportionments.

(dollars in thousands)	2016	2015
Category B		
Total Operating Expenses	\$3,248,985	\$2,910,728
Numismatic Capital	18,116	10,967
Circulating and Protection Capital	10,472	15,214
Total Apportionment		
Categories of Obligations Incurred	\$3,277,573	\$2,936,909

BITCOIN NETWORK ENERGY CONSUMPTION 2017—2018

Estimated TWh year



Source: BitcoinEnergyConsumption.com



tion. Gold compared with silver, or silver with copper, or paper compared with gold, are subject to the same law that the relatively cheaper medium of exchange will be retained in circulation and the relatively dearer will disappear. The most extreme instance which has ever occurred was in the case of the Japanese currency. At the time of the treaty of 1858, between Great Britain, the United States, and Japan, which partially opened up the last country to European traders, a very curious system of currency existed in Japan. The most valuable Japanese coin was the kobang, consisting of a thin oval disc of gold about 2 inches long, and $1\frac{1}{4}$ inch wide, weighing 200 grains, and ornamented in a very primitive manner. It was passing current in the towns of Japan for four silver itzebus, but was worth in English money about 18s. 5d., whereas the silver itzebu was equal only to about 1s. 4d. Thus the Japanese were estimating their gold money at only about one-third of its value, as estimated according to the relative values of the metals in other parts of the world. The earliest European traders enjoyed a rare opportunity for making profit. By buying up the kobangs at the native rating they trebled their money, until the natives, perceiving what was being done, withdrew from circulation the remainder of the

legal ratio. At the rate adopted by Sir Isaac Newton, gold was overvalued by rather more than $1\frac{1}{2}$ per cent.; to that extent it was more valuable as currency than as metal. Therefore, in accordance with the Law of Gresham, and the principles laid down in Chapter VIII., the full weight silver coin was withdrawn or exported, and gold became the practical measure of value, which it has ever since continued to be.

In every other part of the world, where attempts have been made to combine two metals as concurrent standards of value, similar results have followed. In Massachusetts, in 1762, gold was made a legal tender, as well as silver, at the rate of $2\frac{1}{2}d.$ per grain; but, being overvalued as much as 5 per cent, the silver coinage rapidly disappeared from circulation. Various laws were passed to remedy this inconvenient state of things, but without success so long as this valuation of gold was maintained.

Nor is this the whole error of the English writers. A little reflection must show that MM. Wolowski and Courcelle-Seneuil are quite correct in urging that a *compensatory* or, as I should prefer to call it, *equilibratory action*, goes on under the French currency law, and tends to maintain both gold and silver more steady in value than they would otherwise be. If silver becomes more valuable than in the ratio of 1 to 15½ compared with gold, there arises at once a tendency to import gold into any country possessing the double standard, so that it may be coined there, and exchanged for a legally equivalent weight of silver coin, to be exported again. This is no matter of theory only, the process having gone on in France until the principal currency, which was mainly composed of silver in 1849, was in 1860 almost wholly of gold. France absorbed the cheapened metal in vast quantities and emitted the dearer metal, which must have had the effect of preventing gold from falling and silver from rising so much in value as they would otherwise have done. It is obvious that, if gold rose in value compared with silver, the action would be reversed; gold would be absorbed and silver liberated. At any moment the standard of value is doubtless one metal or the other, and not both; yet the fact that there is an alternation tends to make each vary much less than it would otherwise do. It cannot prevent both metals from falling or rising in value compared with other commodities, but it can throw

Imagine two reservoirs of water, each subject to independent variations of supply and demand. In the absence of any connecting pipe the level of the water in each reservoir will be subject to its own fluctuations only. But if we open a connection, the water in both will assume a certain mean level, and the effects of any excessive supply or demand will be distributed over the whole area of both reservoirs. The mass of the metals, gold and silver, circulating in Western Europe in late years, is exactly represented by the water in these reservoirs, and the connecting pipe is the law of the 7th Germinal, an XI, which enables one metal to take the place of the other as an unlimited legal tender.

In short, then, the amount of supply and amount of demand of both the precious metals depend upon a number of accidents, changes, or legislative decisions, which cannot be in any way predicted. The price of silver has fallen in consequence of the German currency reforms, but it is by no means certain that it will fall further than it has already done. That any great rise will really happen in the purchasing power of gold is wholly a matter of speculation. We cannot do more than make random guesses on the subject, and, as a mere guess, I should say that it is not likely to rise. Gold has since 1851 been falling in value, and an increased demand for gold is not likely to do more than slacken, or at the most arrest, the progress of depreciation.

It is remarkable that the changes thus effected in the money of Western Europe are almost the same as those by which the United States had previously abandoned the double standard. Until the year 1853 the silver dollar of the United States mint was a standard coin of unrestricted legal tender, concurrently with the gold coinage of eagles and their fractions. The legal ratio of silver to gold in weight indeed, was 16 to 1, instead of $15\frac{1}{2}$ to 1 as in France. More silver being thus required to make a legal payment in America than elsewhere, gold was naturally preferred for this purpose, and the silver was sent abroad. To remedy this state of things the government of Washington, in 1853, reduced the half-dollar and smaller silver pieces to the condition of token coins, and though the single silver dollar pieces remained of standard weight, they were coined in very small quantities and were practically suppressed. The predominance of an inconvertible paper currency suspended the question of metallic money for a time. The Coinage Act of the United States Congress came into operation on 1st April, 1873, and constituted the gold one-dollar piece the sole unit of value, whilst it restricted the legal tender of the new silver trade dollar, and of the half-dollar and its subdivisions, to an amount not exceeding five dollars in any one payment. Thus the double standard previously existing in theory was finally abolished, and the United States was added to the list of nations adopting the single gold standard.

Becoming a billionaire from
these principles

Major Pairs		Bid	Ask
EUR/USD	↑	1.1691 ⁰	1.1692 ⁴
USD/EUR	—	0.8552 ⁶	0.8553 ⁶
GBP/USD	↓	1.3145 ¹	1.3146 ⁷
USD/GBP	↑	0.7606 ⁵	0.7607 ⁴
USD/CAD	—	1.2997 ⁴	1.2999 ³
CAD/USD	—	0.7692 ⁷	0.7693 ⁹
USD/CHF	↓	0.9621 ⁵	0.9623 ³
CHF/USD	↑	1.0391 ⁴	1.0393 ⁴
USD/JPY	—	112.32 ²	112.33 ⁵
JPY/USD	—	0.0089 ⁰	0.0089 ⁰

		Bid	Ask
EUR/GBP	↑	0.8893 ³	0.8894 ⁸
GBP/EUR	↓	1.1242 ⁵	1.1244 ⁴
EUR/CHF	↓	1.1248 ⁹	1.1250 ⁹
CHF/EUR	↑	0.8888 ²	0.8889 ⁸
AUD/USD	—	0.7202 ⁶	0.7203 ⁸
USD/AUD	—	1.3881 ⁶	1.3883 ⁹
EUR/JPY	—	131.32 ²	131.34 ¹
JPY/EUR	—	0.0076 ¹	0.0076 ¹
GBP/JPY	↓	147.64 ⁹	147.67 ³
JPY/GBP	—	0.0067 ⁷	0.0067 ⁷

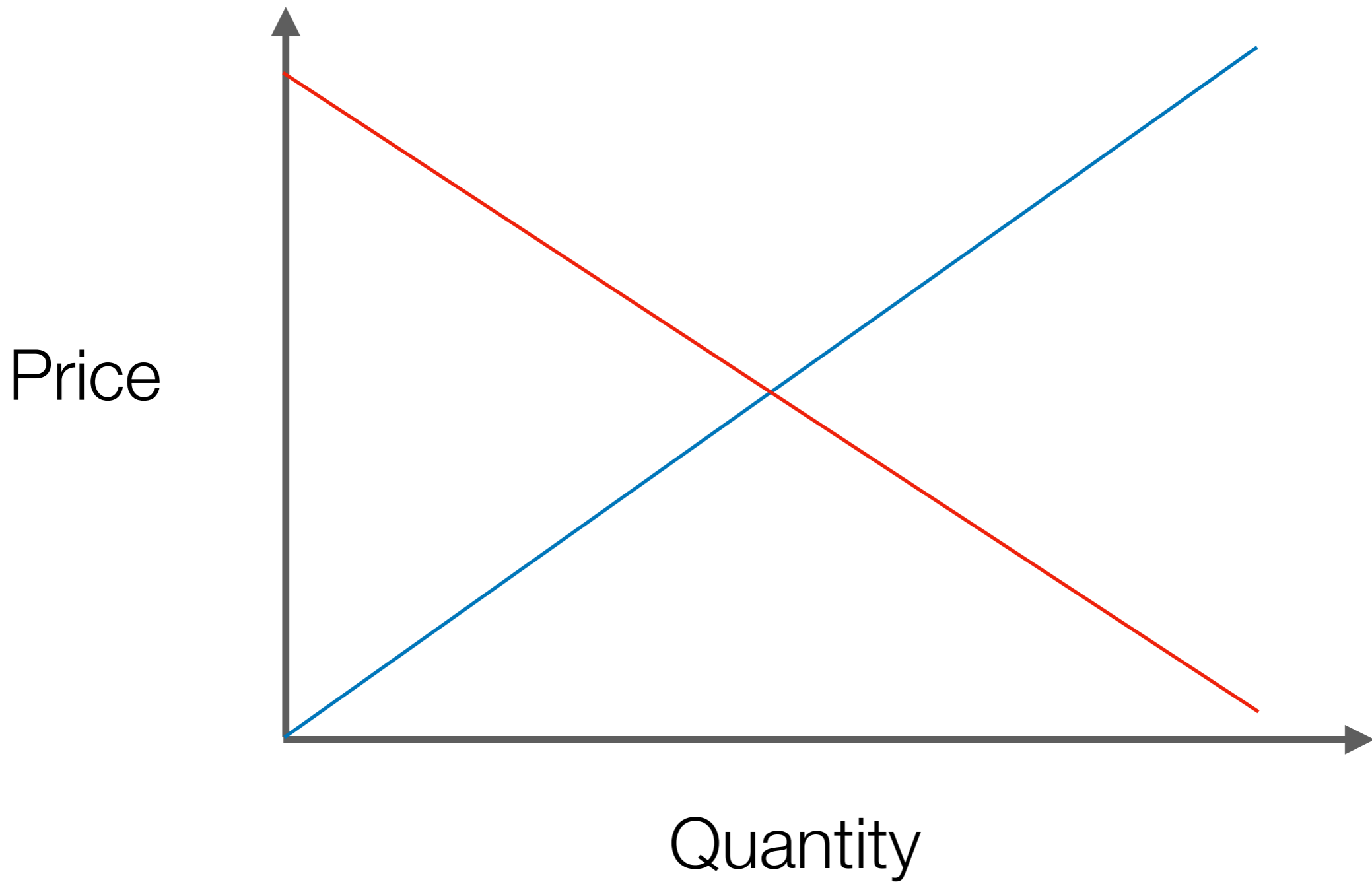
Major Pairs		Bid	Ask
EUR/USD	↑	1.1691 ⁰	1.1692 ⁴
USD/EUR	—	0.8552 ⁶	0.8553 ⁶
GBP/USD	↓	1.3145 ¹	1.3146 ⁷
USD/GBP	↑	0.7606 ⁵	0.7607 ⁴
USD/CAD	—	1.2997 ⁴	1.2999 ³
CAD/USD	—	0.7692 ⁷	0.7693 ⁹
USD/CHF	↓	0.9621 ⁵	0.9623 ³
CHF/USD	↑	1.0391 ⁴	1.0393 ⁴
USD/JPY	—	112.32 ²	112.33 ⁵
JPY/USD	—	0.0089 ⁰	0.0089 ⁰

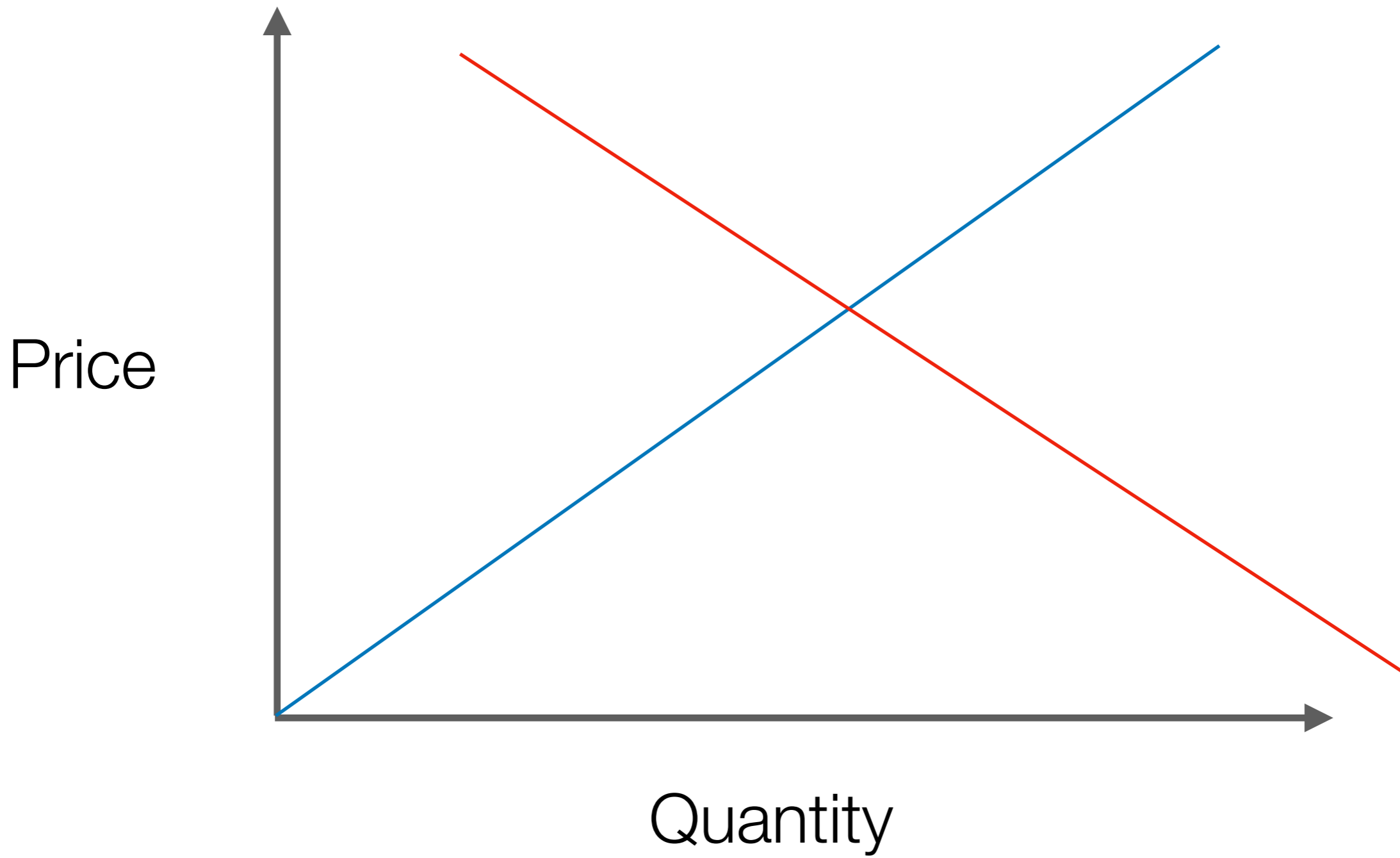
		Bid	Ask
EUR/GBP	↑	0.8893 ³	0.8894 ⁸
GBP/EUR	↓	1.1242 ⁵	1.1244 ⁴
EUR/CHF	↓	1.1248 ⁹	1.1250 ⁹
CHF/EUR	↑	0.8888 ²	0.8889 ⁸
AUD/USD	—	0.7202 ⁶	0.7203 ⁸
USD/AUD	—	1.3881 ⁶	1.3883 ⁹
EUR/JPY	—	131.32 ²	131.34 ¹
JPY/EUR	—	0.0076 ¹	0.0076 ¹
GBP/JPY	↓	147.64 ⁹	147.67 ³
JPY/GBP	—	0.0067 ⁷	0.0067 ⁷

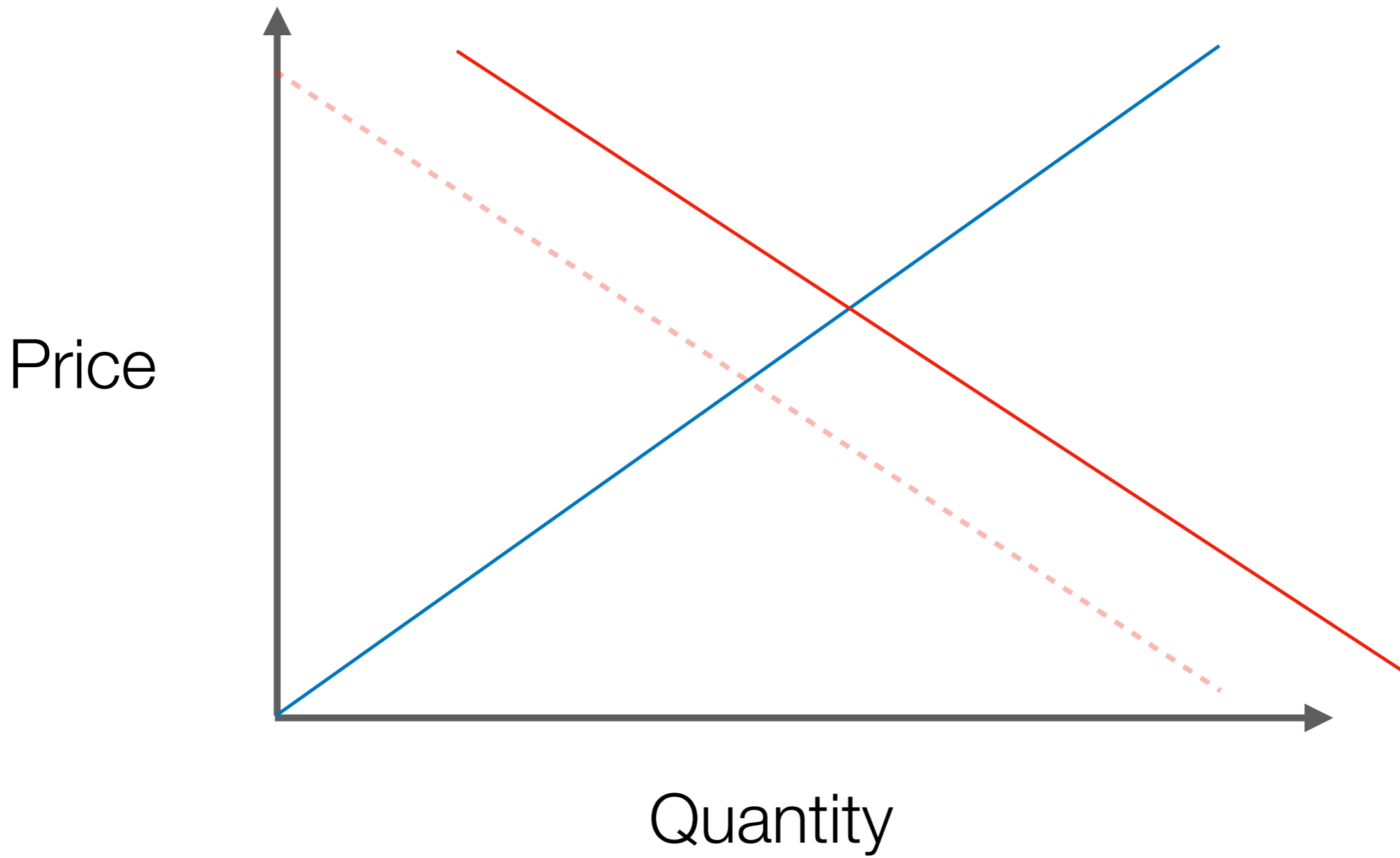


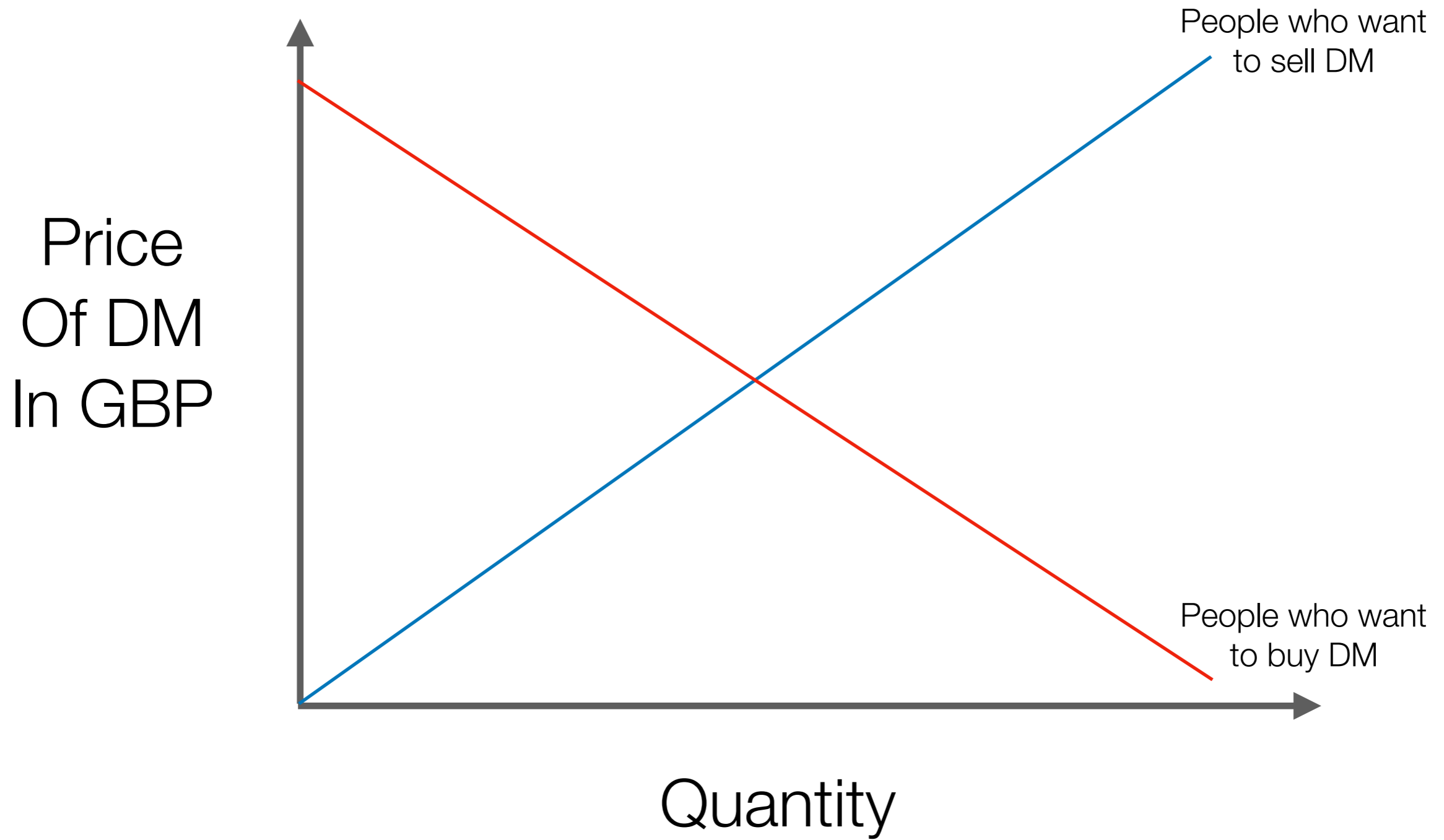
Price

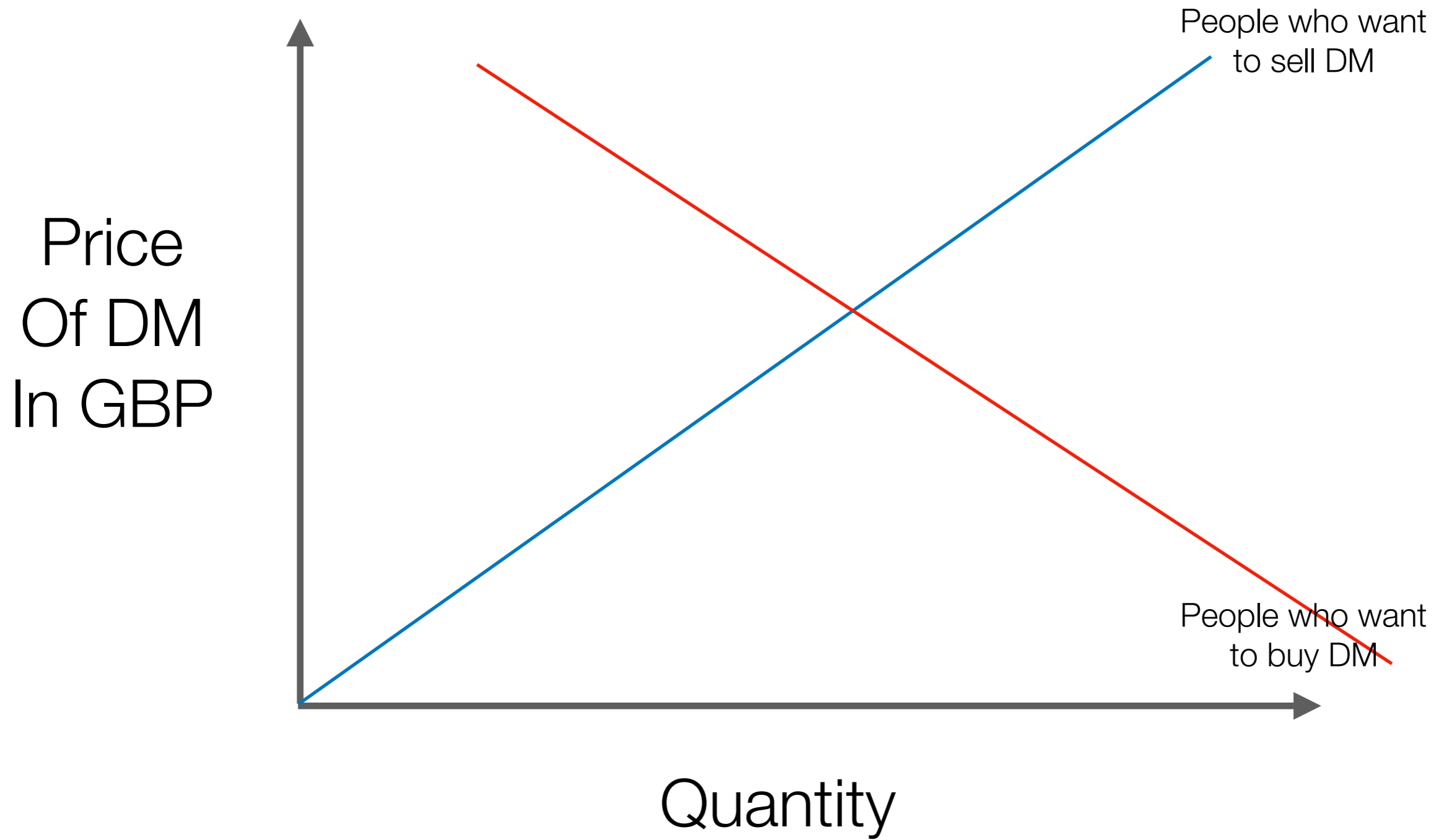
Quantity











A precursor to the EU was the European Exchange Rate mechanism ([ERM](#)), which was created in 1979. Countries weren't ready to give up their national currencies, but they agreed to fix their exchange rates with each other instead of "floating" their currency and letting capital markets set the rates. Since Germany had the strongest economy in Europe, each country set their currency's value in Deutschmarks. They agreed to maintain the exchange rate between their currency and the Deutschmark within an acceptable band of plus or minus 6% of the agreed upon rate.

With fixed exchange rates, countries can't just "set it and forget it." People trade currency every day, exchanging their currency to buy imports or sell exports, and the market applies pressure based on what it thinks the actual rate should be based on supply and demand for a currency. To keep the exchange rate fixed, governments need to participate in the market and nudge it in the agreed upon direction.

Governments can manage their currency in two main ways. First, they can take their reserves of foreign currency and buy up their own currency on the open market. That causes the currency to appreciate. Doing the opposite devalues the currency.

Alternatively, governments can influence exchange rates by setting interest rates. Want your currency to appreciate? Raise rates to entice people to buy your currency and lend that money at higher interest rates. Want your currency to depreciate? Cut interest rates so capital needs to go elsewhere in search of juicy profits.

Messing around with interest rates is a big deal, however, because interest rates affect the whole economy. Along with government spending, interest rates are the main lever governments can use to adjust the economy. If the country is experiencing a recession, the government might cut interest rates to spur investment and spending. If inflation is high, the government might raise rates to shrink the supply of money.

In 1990, Britain was a country that arguably could use an external forcing function to tie its hands on monetary policy. Inflation was high, productivity was low, exports were uncompetitive, and no one really believed the government was capable of fixing the issues.

The Prime Minister at the time, Margaret Thatcher, had long opposed entering the ERM, insisting that the price of the pound be set by the markets. By 1990, however, Thatcher lacked the political power to oppose other members of her Conservative party who wanted to fix their exchange rates with the rest of Europe.

The decision to join the ERM was championed by John Major, who was the Chancellor of the Exchequer in Thatcher's cabinet. In October 1990, Britain finally entered the ERM at an exchange rate of 2.95 Deutschmark (DM) for each British pound (GBP). The British government was obligated to keep the exchange rate within 2.78 DM to 3.13 DM.

Shortly thereafter, Major replaced Thatcher as the Prime Minister. The fixed exchange rate system was to be the centerpiece of his economic plan. **Major thought** that the ERM would serve as a sort of "autopilot" that kept the British monetary policy on proper course. The government couldn't play with the money supply willy-nilly because its hands were tied by the exchange rate agreement.

And to a certain extent, the policy worked. Between 1990 and 1992, inflation decreased, interest rates eased, and unemployment was low by historical standards. In 1992, however, England felt the impact of a massive global recession, and **unemployment spiked** to 12.7% from just 7.7% two years prior.

And so we come to 1992. Ordinarily, Britain could spur investment and spending by cutting interest rates during an employment crisis. But in this case, doing so would push the pound's value below the agreed upon amount. So while the people of Great Britain dealt with a recession, the government's hands were tied; they'd just have to ride it out.

By the spring of 1992, just a year and a half after Britain joined the ERM, the fixed exchange rate posed a serious problem. While putting on a cheery public face, internally the Exchequer (England's Treasury department) realized that the currency was mispriced relative to the Deutschemark. Jonathan Portes, an economist who was at the time a junior staff member there, [wrote](#):

"In May 1992, the immediate problem was obvious. From a domestic point of view, the appropriate level of interest rates, given weak demand, was much lower than that necessary to maintain [the] sterling's position in the ERM.

Moreover, it was becoming increasingly clear that sterling was overvalued; even in the depths of a recession, we still had a large current account deficit [the country was importing more than it exported].

We argued that the fundamental problem was that we'd joined the ERM at the wrong rate; sterling was overvalued, meaning that we were stuck with a structural current account deficit."

The sterling was priced too high. The British government knew it, and the market knew it too as the pound was trading at the lower end of the agreed upon band with the Deutschemark.

What kept the pound from plummeting in value was the British government's guarantee that it would keep the value propped up, and the market believed that it would. As long as everyone believed that England would stay indefinitely committed to buying pounds for around 2.95 Deutschemarks, the status quo was maintained.

Throughout the summer of 1992, the British pound held its position. That is, until Germany threw Britain under the bus and all hell broke loose.

For some time that year, German central bank officials made comments on and off the record that undermined the sterling's strength. The British paper *The Independent* documents the [slights](#):

"On 25 August, for example, Reimut Jochimsen, a Bundesbank council member, issued a speech saying that there was potential for realignment within the ERM. Sterling weakened. On 10 September, an unnamed Bundesbank official was quoted as saying that a devaluation of sterling was inevitable. The pound fell."

The event that ultimately [led to the undoing](#) of the British pound's fixed exchange rate was an interview with the President of the German Bundesbank, Helmut Schlesinger. Schlesinger gave the interview to the *Wall Street Journal* and a German newspaper. He had one condition: If they wanted to directly quote him, they had to let him review the quotes. If they only indirectly paraphrased him, no such permission was necessary.

"The President of the Bundesbank, Professor Helmut Schlesinger, does not rule out the possibility that, even after the realignment and the cut in German interest rates, one or two currencies could come under pressure before the referendum in France. He conceded in an interview that the problems are of course not solved completely by the measures taken."

Since August, Soros and his Quantum Fund had been building a **\$1.5 billion** position to bet that the price of Sterling would fall. Since the British government's full faith and credit was stating that it would not fall, this wasn't necessarily something that was going to happen. But **Stanley Druckenmiller**, a senior member of the fund, saw the report from Schlesinger and immediately realized its importance.

Sebastian Mallaby's book *More Money Than God* recounts the day's events. According to Mallaby, Druckenmiller noted that their \$1.5 billion bet against the pound was about to pay off and that they should consider adding to the position.

Soros retorted with a different strategy: "*Go for the jugular.*"

And what if you want to short a currency like the British pound? In this case, you'd go to a British person or company and ask to borrow money from them. They say, "Sure, here's 100 British pounds. Just give me back the pounds in a few days with some interest, and we'll have some tea and crumpets." Now, you take those 100 British pounds, and you convert them into 295 Deutschmarks at the agreed upon exchange rate.

At this point, you would really like the British pound to lose value relative to the Deutschmark. Why? Because if the British pound depreciates 10%, when you convert the 295 DM back to pounds to repay the loan, you'll have 110 pounds. You can pay back the 100 pounds and a little bit of interest, and you'll still clear about 10 pounds in profit.

So you make money if the pound devalues. But what if the pound appreciates? You'll lose your shirt. Therein lies the brilliance of Soros's bet: if the pound tanked, they would make billions on their short. And if the pound increased in value? Well, that scenario was impossible because everyone knew the sterling was over priced. It already traded at the bottom of its trading band, and the only thing that kept it propped up was government intervention. There was no scenario in which the pound would appreciate.

And so that morning, Soros and his fund increased their short position against the British pound from **\$1.5 to \$10 billion**. It was the perfect bet with a mitigated downside and a limitless upside. It was like betting on a coin flip, were if the coin lands on heads (the pound devalues), they make a lot of money. If the coin lands on tails (the exchange rates remained fixed), they only lose a small amount of money on loan interest. That's the kind of bet Soros would pour money into all the day, even if he had to borrow billions.

British officials first responded by buying **one billion pounds at 8:40 AM**. The purchase had no effect on the price of the pound. The whole world was selling, and the British government didn't have the buying power to fight it all off. It's estimated that the British government spent £27 billion of its reserves buying up pounds to no avail.

By **9AM**, finance minister Norman Lamont contacted Prime Minister John Major and told him they couldn't possibly buy up enough pounds to keep the currency propped up. The only option left for the British government to keep their currency trading at the right level would be to increase interest rates dramatically and attract people to buy pounds. Major **refused**. Britain was in the midst of a recession, and increasing rates would further shrink the economy. It would be political suicide.

Blood was in the water. Global capital continued to bet against the pound. An hour and a half later, Lamont called the Prime Minister to re-plead his case. The Prime Minister relented. At **11AM**, the British government announced they would increase interest rates 200 basis points, from 10% to 12%.

How did the value of the pound react to this enormous increase in interest rates? Nothing happened. The pound **continued to plummet**. Lamont headed to the Prime Minister's residence to figure out how to salvage the situation, which led them to announce an interest rate increase of another 300 basis points, from 12% to 15%.

What was the effect of this rate increase on the sterling? Again, nothing. As Mallaby later documents in his **book**, Soros and the gang of speculators knew victory was near:

British officials first responded by buying **one billion pounds at 8:40 AM**. The purchase had no effect on the price of the pound. The whole world was selling, and the British government didn't have the buying power to fight it all off. It's estimated that the British government spent £27 billion of its reserves buying up pounds to no avail.

Blood was in the water. Global capital continued to bet against the pound. An hour and a half later, Lamont called the Prime Minister to re-plead his case. The Prime Minister relented. At 11AM, the British government announced they would increase interest rates 200 basis points, from 10% to 12%.

How did the value of the pound react to this enormous increase in interest rates? Nothing happened. The pound **continued to plummet**. Lamont headed to the Prime Minister's residence to figure out how to salvage the situation, which led them to announce an interest rate increase of another 300 basis points, from 12% to 15%.

What was the effect of this rate increase on the sterling? Again, nothing. As Mallaby later documents in his **book**, Soros and the gang of speculators knew victory was near:

British officials first responded by buying **one billion pounds at 8:40 AM**. The purchase had no effect on the price of the pound. The whole world was selling, and the British government didn't have the buying power to fight it all off. It's estimated that the British government spent £27 billion of its reserves buying up pounds to no avail.

How did the value of the pound react to this enormous increase in interest rates? Nothing happened. The pound **continued to plummet**. Lamont headed to the Prime Minister's residence to figure out how to salvage the situation, which led them to announce an interest rate increase of another 300 basis points, from 12% to 15%.

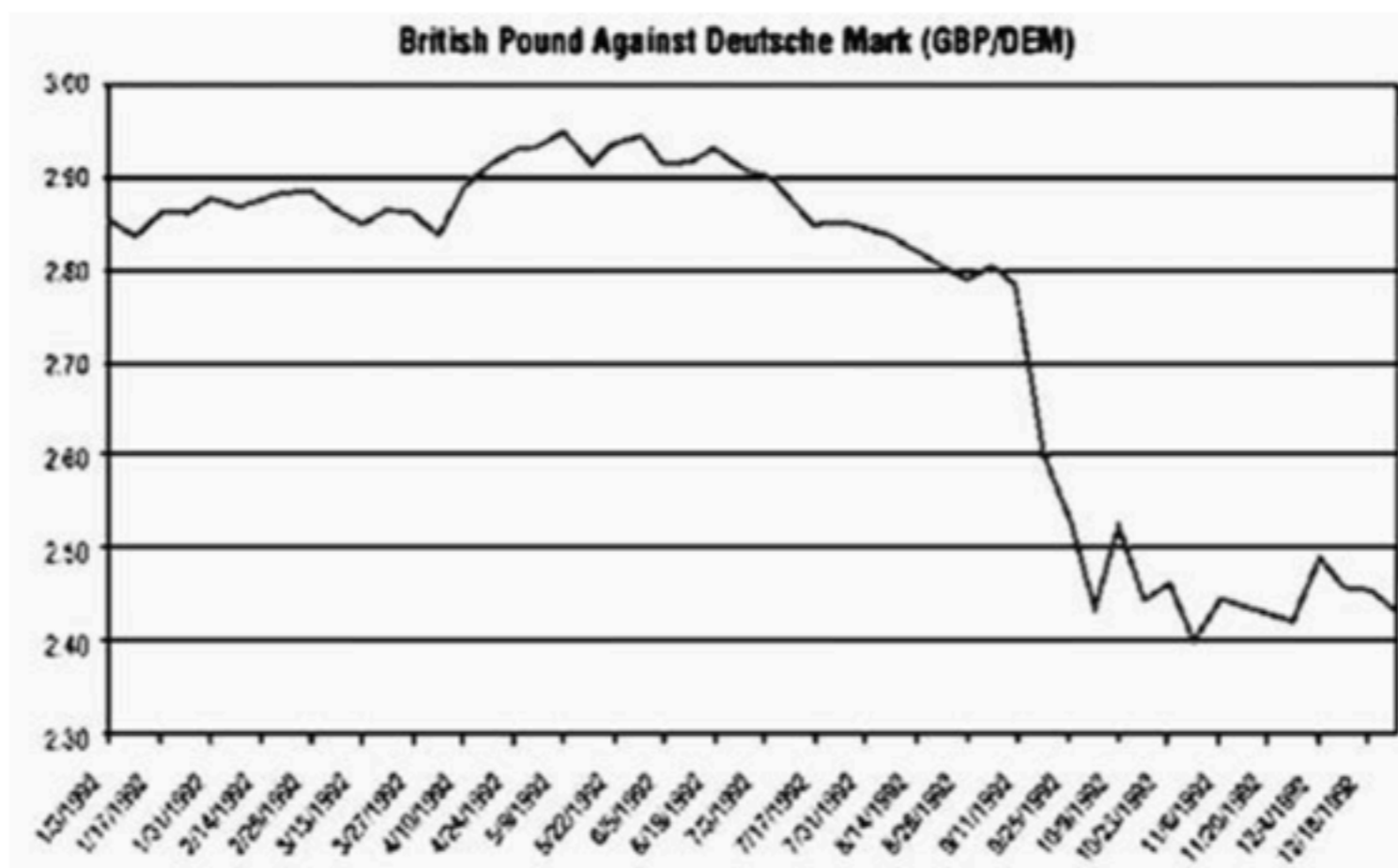
What was the effect of this rate increase on the sterling? Again, nothing. As Mallaby later documents in his **book**, Soros and the gang of speculators knew victory was near:

British officials first responded by buying **one billion pounds at 8:40 AM**. The purchase had no effect on the price of the pound. The whole world was selling, and the British government didn't have the buying power to fight it all off. It's estimated that the British government spent £27 billion of its reserves buying up pounds to no avail.

What was the effect of this rate increase on the sterling? Again, nothing. As Mallaby later documents in his **book**, Soros and the gang of speculators knew victory was near:

British officials first responded by buying **one billion pounds at 8:40 AM**. The purchase had no effect on the price of the pound. The whole world was selling, and the British government didn't have the buying power to fight it all off. It's estimated that the British government spent £27 billion of its reserves buying up pounds to no avail.

British financial history now refers to September 17, 1992, as "Black Wednesday;" George Soros, however, probably calls it something like "Awesome Wednesday." Once Great Britain floated its currency, the **pound fell** 15% versus the Deutsche Mark and 25% versus the US Dollar.



L4: Currency markets + arbitrage

What happens to GBP?

British retail sales jumped 3.3 percent in August compared with the same month a year earlier, better than all forecasts in a Reuters poll of economists, as shoppers maintained their strong summer spending spree.

Sales rose by 0.3 percent in August from July, the Office for National Statistics said, defying a median forecast for a fall of 0.2 percent. The numbers follow other data showing the UK economy performed relatively well in recent months and that UK consumer prices in August rose at their fastest pace in six months.

What happens to GBP?

British retail sales jumped 3.3 percent in August compared with the same month a year earlier, better than all forecasts in a Reuters poll of economists, as shoppers maintained their strong summer spending spree.

Sales rose by 0.3 percent in August from July, the Office for National Statistics said, defying a median forecast for a fall of 0.2 percent. The numbers follow other data showing the UK economy performed relatively well in recent months and that UK consumer prices in August rose at their fastest pace in six months.

FOREIGN EXCHANGE ANALYSIS

SEPTEMBER 20, 2018 / 4:29 AM / UPDATED 3 HOURS AGO

Pound surges, buoyed by retail sales and Brexit hopes

What happens to this currency?

Thousands of public school teachers and university professors marched against Macri's fiscal belt tightening plans in capital Buenos Aires on Thursday, saying that the administration was funding the army and police while letting education and welfare programs suffer.

What happens to this currency?

Thousands of public school teachers and university professors marched against Macri's fiscal belt tightening plans in capital Buenos Aires on Thursday, saying that the administration was funding the army and police while letting education and welfare programs suffer.

FOREIGN EXCHANGE ANALYSIS

SEPTEMBER 13, 2018 / 2:44 PM / 7 DAYS AGO

Argentina's peso drops 3.5 percent to new record low close

“It is absurd that Europe pays for 80 percent of its energy import bill – worth 300 billion euros a year – in U.S. dollars when only roughly 2 percent of our energy imports come from the United States,” he said.

...

While Norway prices its substantial supplies to the EU in euros, an EU official said, other countries use dollars. Among the most important of these are Gulf states and Russia.

FRB: Beige Book Sep'2018

Reports from the Federal Reserve Districts suggested that the economy expanded at a moderate pace through the end of August. Dallas reported relatively brisk growth, while Philadelphia, St. Louis, and Kansas City indicated somewhat below average growth. Consumer spending continued to grow at a modest pace since the last report, and tourism activity expanded, to varying degrees, across the nation. Manufacturing activity grew at a moderate rate in most Districts, though St. Louis described business as little changed and Richmond reported a decline in activity. Transportation activity expanded, with a few Districts characterizing growth as robust. Home construction activity was mixed but up modestly, on balance. However, home sales were somewhat softer, on balance--in some cases due to reduced demand, in others due more to low inventories. Commercial real estate construction was also mixed, while both sales and leasing activity expanded modestly. Lending activity grew throughout the nation. Some Districts noted weakness in agricultural conditions. Businesses generally remained optimistic about the near-term outlook, though most Districts noted concern and uncertainty about trade tensions--particularly though not only among manufacturers. A number of Districts noted that such concerns had prompted some businesses to scale back or postpone capital investment.

Theresa May's proposed new economic partnership with the EU "will not work", the head of the European Council has said.

Donald Tusk said the plans risked undermining the EU's single market.

He was speaking at the end of an EU summit in Salzburg where leaders of the 27 remaining member states discussed Brexit.

“Wednesday as data showed inflation unexpectedly accelerated in August. Consumer prices [rose](#) 2.7 percent from a year earlier, compared with economists’ median forecast for a reading of 2.4 percent. ”

Table 1. Assets, liabilities, and capital of the Federal Reserve System

Billions of dollars

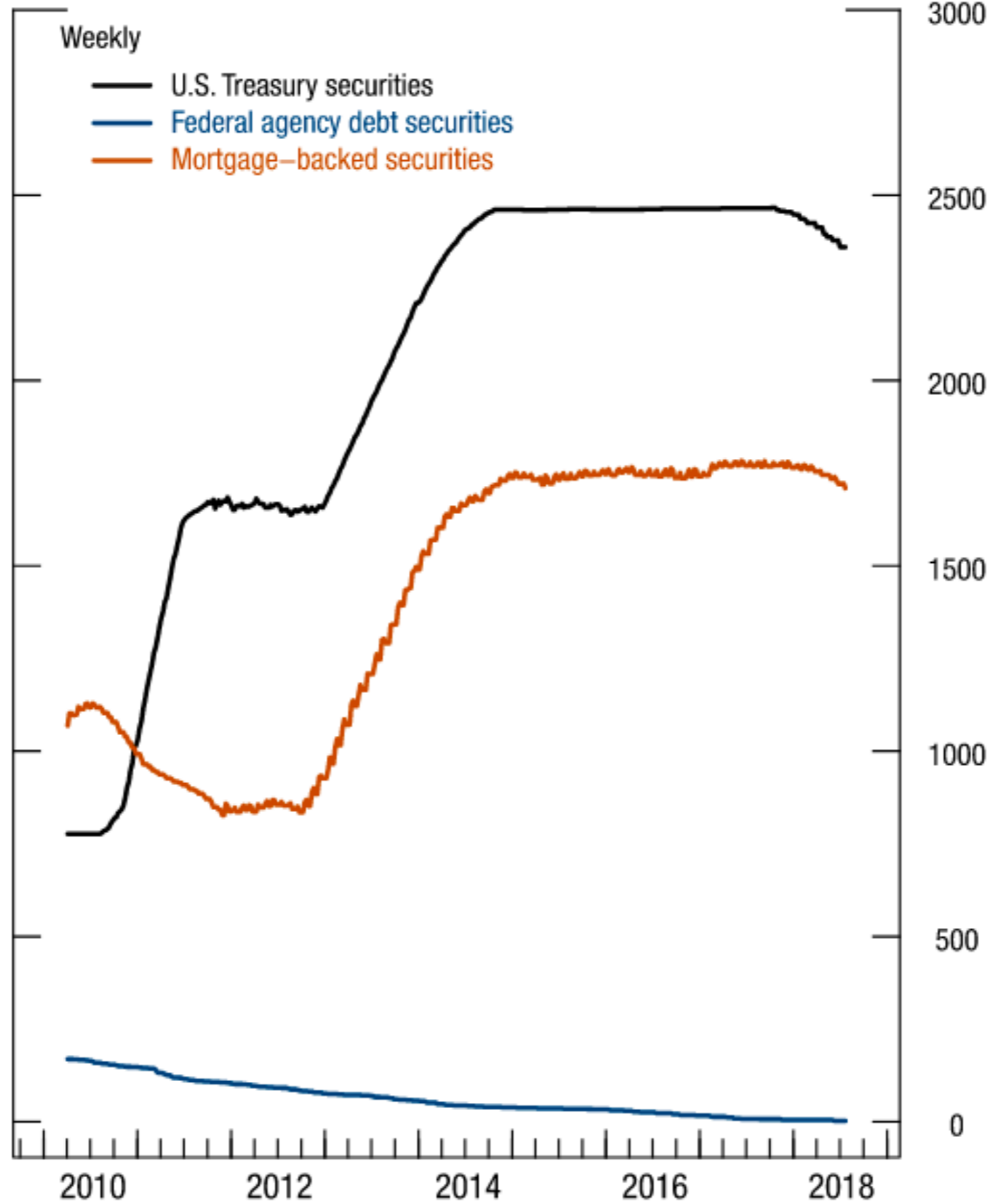
Make Full Screen 

Item	Current July 25, 2018	Change from April 25, 2018	Change from July 26, 2017
Total assets	4,278	-95	-188
Selected assets			
Securities held outright	4,072	-91	-170
U.S. Treasury securities ¹	2,360	-53	-105
Federal agency debt securities ¹	2	-2	-6
Mortgage-backed securities ²	1,710	-35	-59
Memo: Overnight securities lending ³	18	1	-4
Memo: Net commitments to purchase mortgage-backed securities ⁴	8	-1	-11
Unamortized premiums on securities held outright ⁵	148	-5	-17
Unamortized discounts on securities held outright ⁵	-14	+*	+1
Lending to depository institutions ⁶	*	+*	+*
Central bank liquidity swaps ⁷	*	+*	+*
Net portfolio holdings of Maiden Lane LLC ⁸	2	+*	+*
Foreign currency denominated assets ⁹	21	-1	+*

- In addition, the FOMC directed the FRBNY to continue rolling over at auction the amount of principal payments from the Federal Reserve's holdings of Treasury securities maturing during June that exceeded \$18 billion and to continue reinvesting in agency mortgage-backed securities (MBS) the amount of principal payments from the Federal Reserve's holdings of agency debt and agency MBS received during June that exceeded \$12 billion. Effective in July 2018, the FOMC directed the FRBNY to increase these principal payment reinvestment thresholds to \$24 billion per calendar month for Treasury securities and \$16 billion per calendar month for agency debt and agency MBS. Small deviations from these amounts for operational reasons are acceptable. Additional information on these implementation steps is available at www.federalreserve.gov/newsevents/pressreleases/monetary20180613a1.htm and www.newyorkfed.org/markets/rrp_op_policies.html.
-

Securities Held Outright

\$ Billions



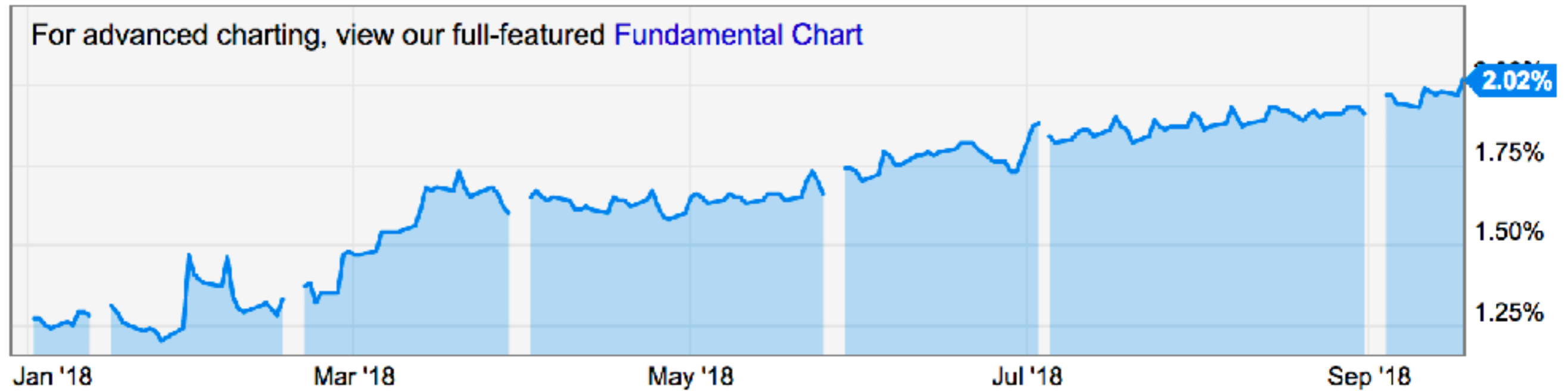
Note: On a settlement basis rather than a commitment basis.

4 Week Treasury Bill Rate Chart

[View Full Chart](#)

5d 1m 3m 6m **YTD** 1y 5y 10y Max

[Export Data](#) [Save Image](#) [Print Image](#)



4 Week Treasury Bill Rate Historical Data

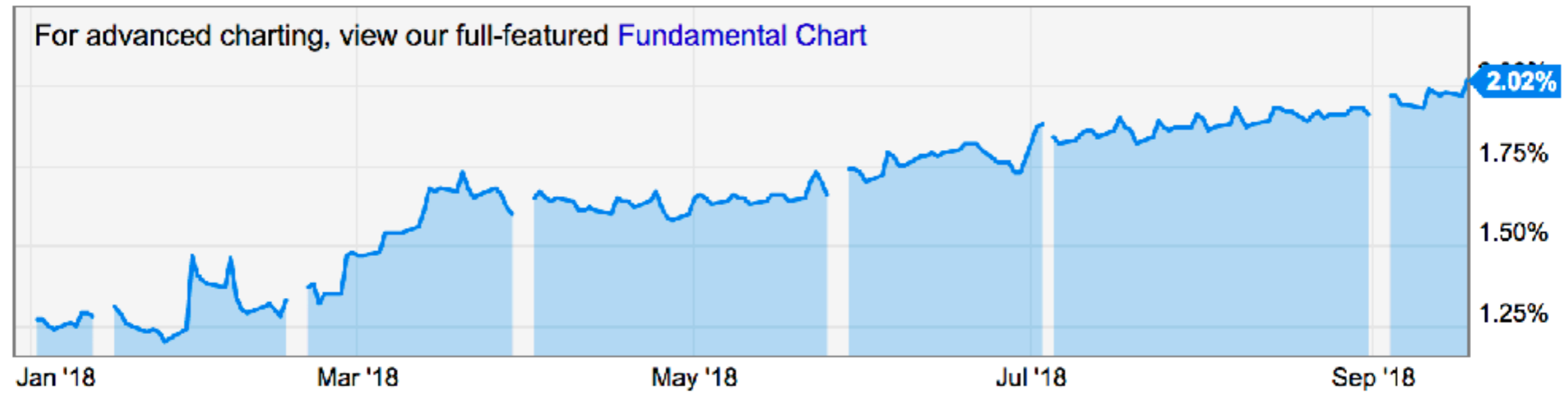
What should happen to the USD?

4 Week Treasury Bill Rate Chart

[View Full Chart](#)

5d 1m 3m 6m YTD 1y 5y 10y Max

Export Data Save Image Print Image



4 Week Treasury Bill Rate Historical Data

FRED Trade Weighted U.S. Dollar Index: Major Currencies

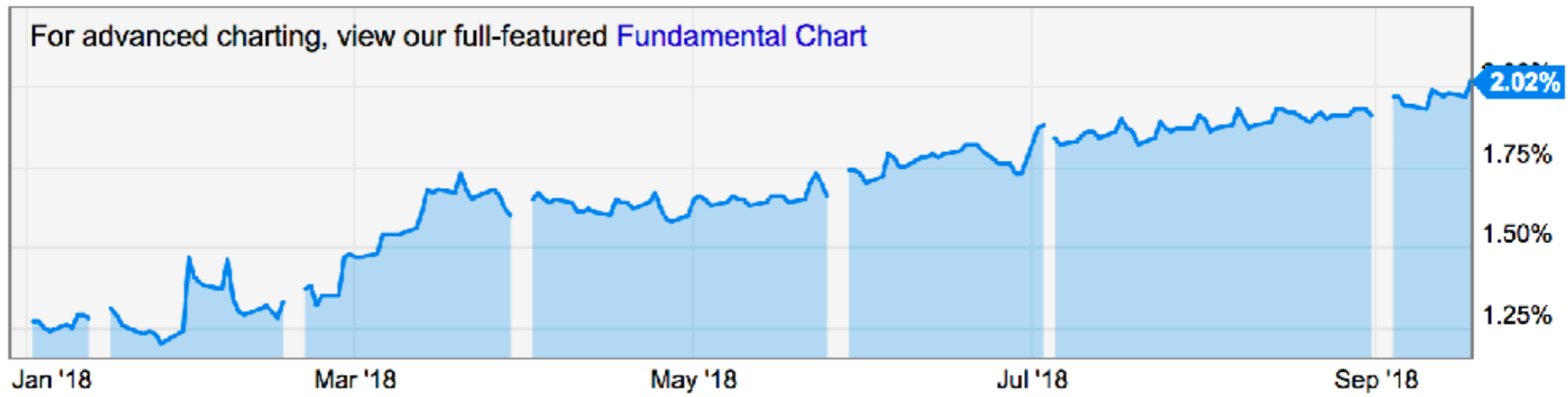


4 Week Treasury Bill Rate Chart

[View Full Chart](#)

5d 1m 3m 6m **YTD** 1y 5y 10y Max

[Export Data](#) [Save Image](#) [Print Image](#)



4 Week Treasury Bill Rate Historical Data

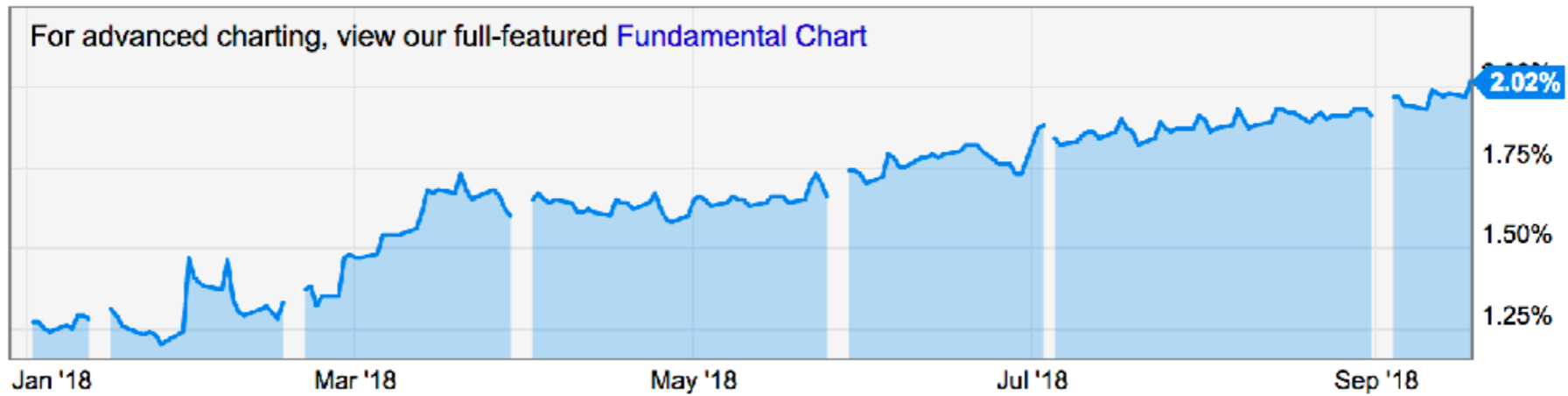
How should BOND funds react?

4 Week Treasury Bill Rate Chart

[View Full Chart](#)

5d 1m 3m 6m **YTD** 1y 5y 10y Max

[Export Data](#) [Save Image](#) [Print Image](#)



4 Week Treasury Bill Rate Historical Data

How should BOND funds react?

Vanguard Total Bond Market ETF (BND) [Add to Watchlists](#) [Create an Alert](#)

78.52 ▲ **+0.07** **+0.09%** NYSE Arca Sep 20, 14:13 Delayed 2m USD

Quote **Fundamental Chart** Technicals Holdings Data News Performance

BND Price Chart

[View Full Chart](#)



- On June 13, 2018, the Federal Open Market Committee (FOMC) announced that it had decided to raise the target range for the federal funds rate to 1-3/4 to 2 percent, from 1-1/2 to 1-3/4 percent. Additional information on the FOMC's decision is available at www.federalreserve.gov/newsevents/pressreleases/monetary20180613a.htm and www.federalreserve.gov/monetarypolicy/fomcminutes20180613.htm.
- To implement this monetary policy stance, the FOMC directed the Federal Reserve Bank of New York (FRBNY) to conduct open market operations (OMOs), including overnight reverse repurchase operations, as necessary to maintain the federal funds rate in a target range of 1-3/4 to 2 percent. In related actions, effective June 14, 2018, the Board of Governors of the Federal Reserve System (Board) raised the interest rate paid on required and excess reserve balances to 1.95 percent and approved a 1/4 percentage point increase in the discount rate (the primary credit rate) to 2.50 percent.

-

Savings Account

Overview

Fees

Rates

Benefits

Resources

[Open now](#)

[Not ready to open online?](#) ▼

We're committed to making your experience with us as easy as possible. View the [Bank of America Rewards Savings Account Clarity Statement](#)[®]

Rates

As your balances grow, your interest rate may increase too

Rewards Savings Account⁶

Account balance amount	Standard Annual Percentage Yield (APY) ⁷
Less than \$2,500	0.03%
\$2,500 and over	0.03%

If you're enrolled in Preferred Rewards

Gold Tier APY ⁷	Platinum Tier APY ⁷	Platinum Honors Tier APY ⁷
0.04%	0.05%	0.06%
0.04%	0.05%	0.06%

Preferred Rewards clients get extra interest based on their relationship tier

[How to qualify](#)

Mid-market rates as of 2016-03-31 17:40 UTC

Currency code ▲▼	Currency name ▲▼	Units per EUR	EUR per Unit
USD	US Dollar	1.1386632306	0.8762227907
EUR	Euro	1.0000000000	1.0000000000
GBP	British Pound	0.7921136388	1.2624451227
INR	Indian Rupee	75.3658843112	0.0132888030
AUD	Australian Dollar	1.4869681878	0.6729873514
CAD	Canadian Dollar	1.4796754127	0.6758238945
SGD	Singapore Dollar	1.5347639238	0.6515660060
CHF	Swiss Franc	1.0917416715	0.9159676012
MYR	Malaysian Ringgit	4.4140052400	0.2265516114
JPY	Japanese Yen	128.1388820287	0.0078040325
CNY	Chinese Yuan Renminbi	7.3411003512	0.1362193612
NZD	New Zealand Dollar	1.8484648003	0.6068250248
THB	Thai Baht	39.9627318192	0.0250233143
HUF	Hungarian Forint	313.9042436792	0.0031856849
AED	Emirati Dirham	4.1823100458	0.2391023117

Mid-market rates as of 2016-03-31 17:39 UTC

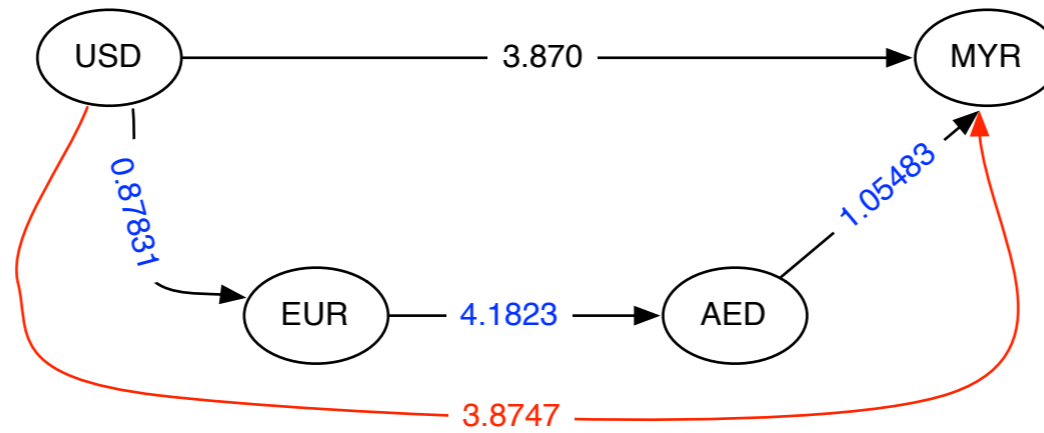
Currency code ▲▼	Currency name ▲▼	Units per AED	AED per Unit
USD	US Dollar	0.2722570108	3.6730000000
EUR	Euro	0.2391289974	4.1818433177
GBP	British Pound	0.1893997890	5.2798369266
INR	Indian Rupee	18.0207422309	0.0554918100
AUD	Australian Dollar	0.3552885418	2.8145257760
CAD	Canadian Dollar	0.3538334124	2.8261987234
SGD	Singapore Dollar	0.3668652245	2.7250538559
CHF	Swiss Franc	0.2610688193	3.8304105746
MYR	Malaysian Ringgit	1.0548325819	0.9480177576
JPY	Japanese Yen	30.6389242807	0.0328371564
CNY	Chinese Yuan Renminbi	1.7555154332	0.5696332719
NZD	New Zealand Dollar	0.3941937299	2.5355237088
THB	Thai Baht	9.5553789460	0.1046530970
HUF	Hungarian Forint	75.0637936939	0.0133220019
AED	Emirati Dirham	1.0000000000	1.0000000000

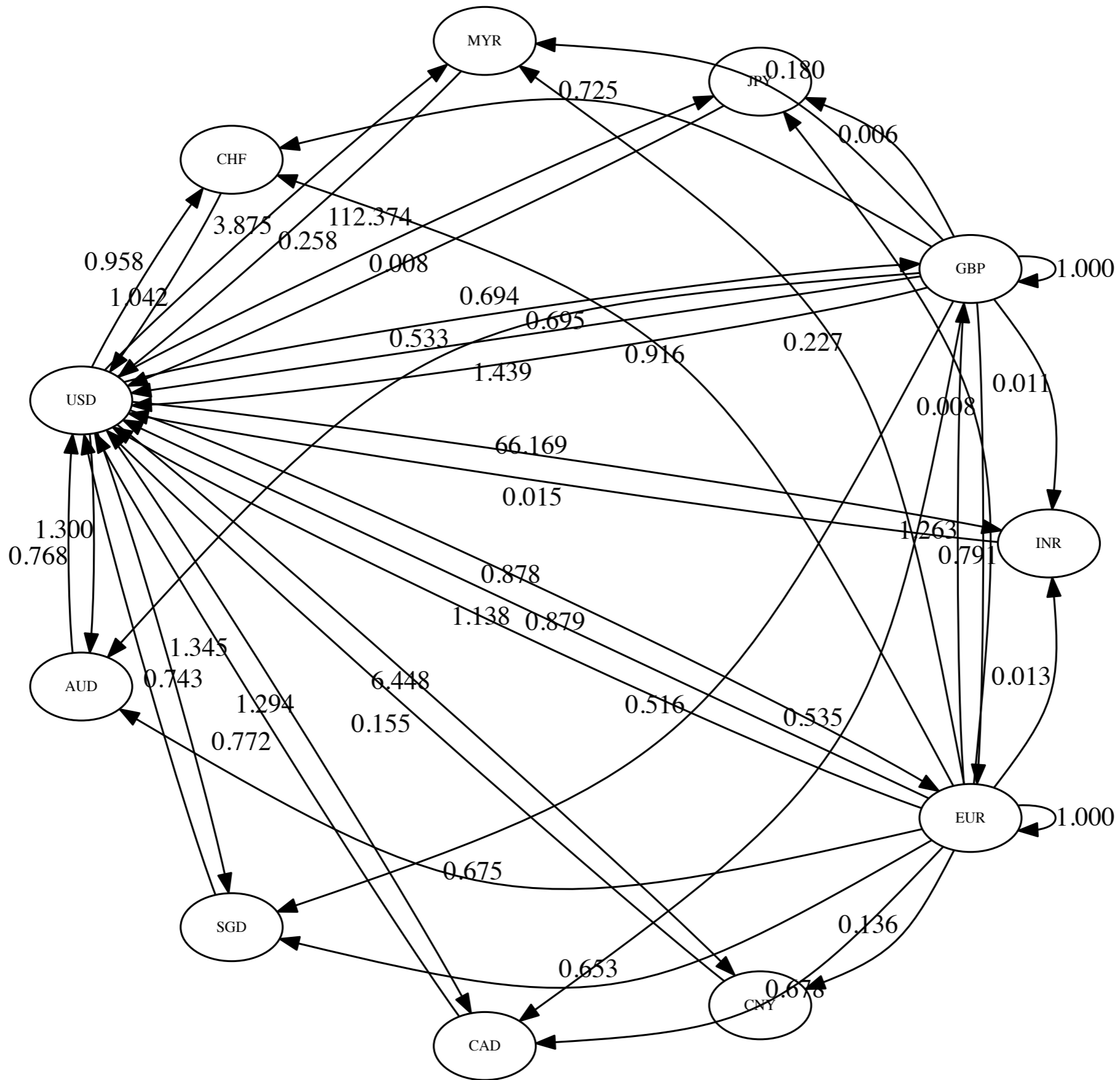
Mid-market rates as of 2016-03-31 17:40 UTC

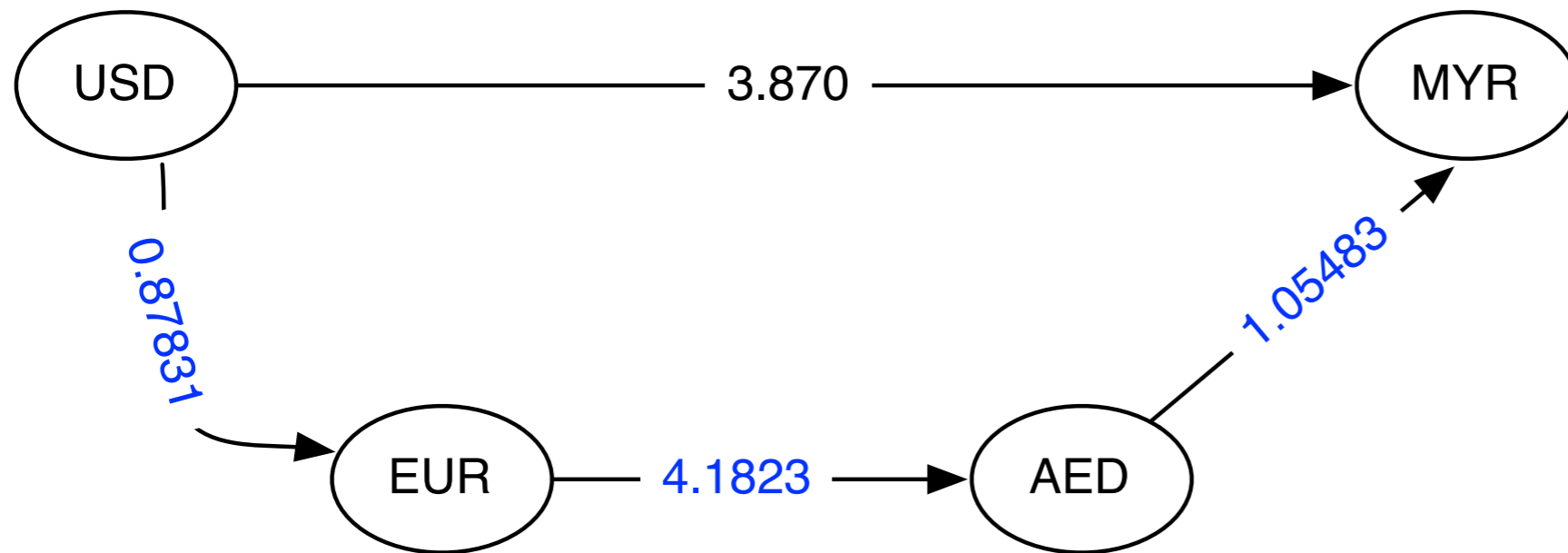
Currency code ▲▼	Currency name ▲▼	Units per EUR	EUR per Unit
USD	US Dollar	1.1386632306	0.8762227907
EUR	Euro	1.0000000000	1.0000000000
GBP	British Pound	0.7921136388	1.2624451227
INR	Indian Rupee	75.3658843112	0.0132888030
AUD	Australian Dollar	1.4869681878	0.6729873514
CAD	Canadian Dollar	1.4796754127	0.6758238945
SGD	Singapore Dollar	1.5347639238	0.6515660060
CHF	Swiss Franc	1.0917416715	0.9159676012
MYR	Malaysian Ringgit	4.4140052400	0.2265516114
JPY	Japanese Yen	128.1388820287	0.0078040325
CNY	Chinese Yuan Renminbi	7.3411003512	0.1362193612
NZD	New Zealand Dollar	1.8484648003	0.6068250248
THB	Thai Baht	39.9627318192	0.0250233143
HUF	Hungarian Forint	313.9042436792	0.0031856849
AED	Emirati Dirham	4.1823100458	0.2391023117

Mid-market rates as of 2016-03-31 17:39 UTC

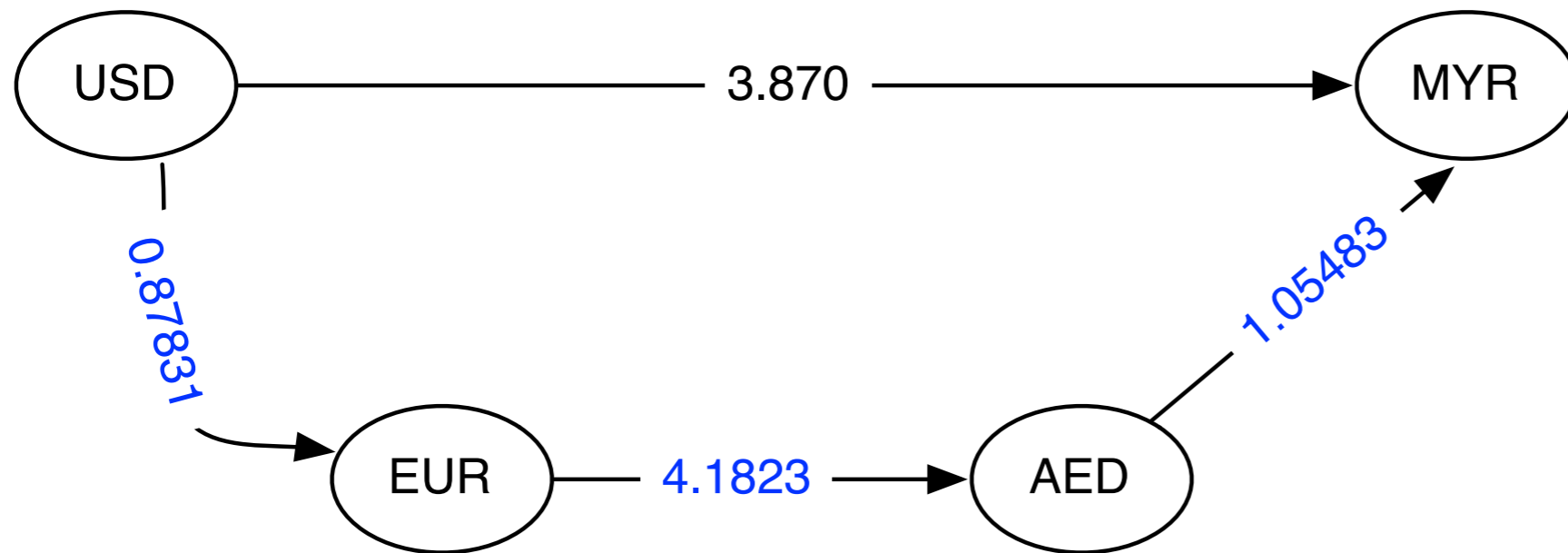
Currency code ▲▼	Currency name ▲▼	Units per AED	AED per Unit
USD	US Dollar	0.2722570108	3.6730000000
EUR	Euro	0.2391289974	4.1818433177
GBP	British Pound	0.1893997890	5.2798369266
INR	Indian Rupee	18.0207422309	0.0554918100
AUD	Australian Dollar	0.3552885418	2.8145257760
CAD	Canadian Dollar	0.3538334124	2.8261987234
SGD	Singapore Dollar	0.3668652245	2.7250538559
CHF	Swiss Franc	0.2610688193	3.8304105746
MYR	Malaysian Ringgit	1.0548325819	0.9480177576
JPY	Japanese Yen	30.6389242607	0.0328371564
CNY	Chinese Yuan Renminbi	1.7555154332	0.5696332719
NZD	New Zealand Dollar	0.3941937299	2.5355237088
THB	Thai Baht	9.5553789460	0.1046530970
HUF	Hungarian Forint	75.0637936939	0.0133220019
AED	Emirati Dirham	1.0000000000	1.0000000000



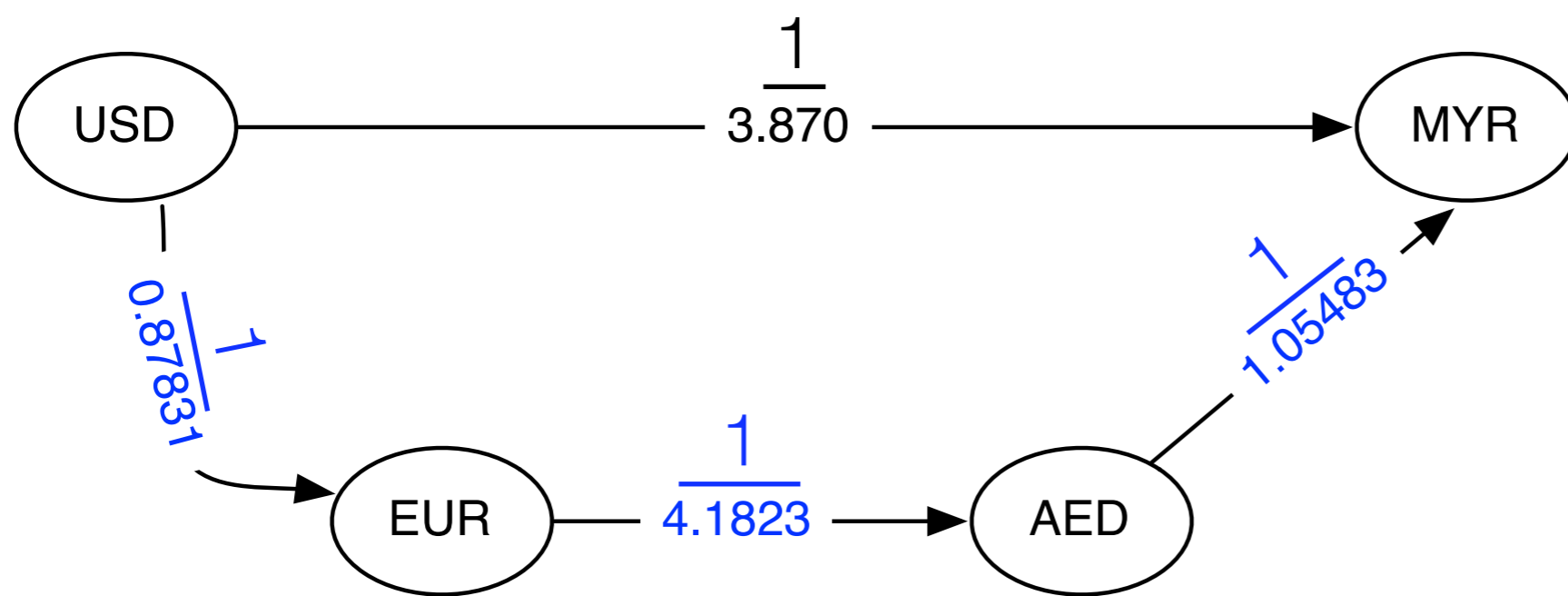




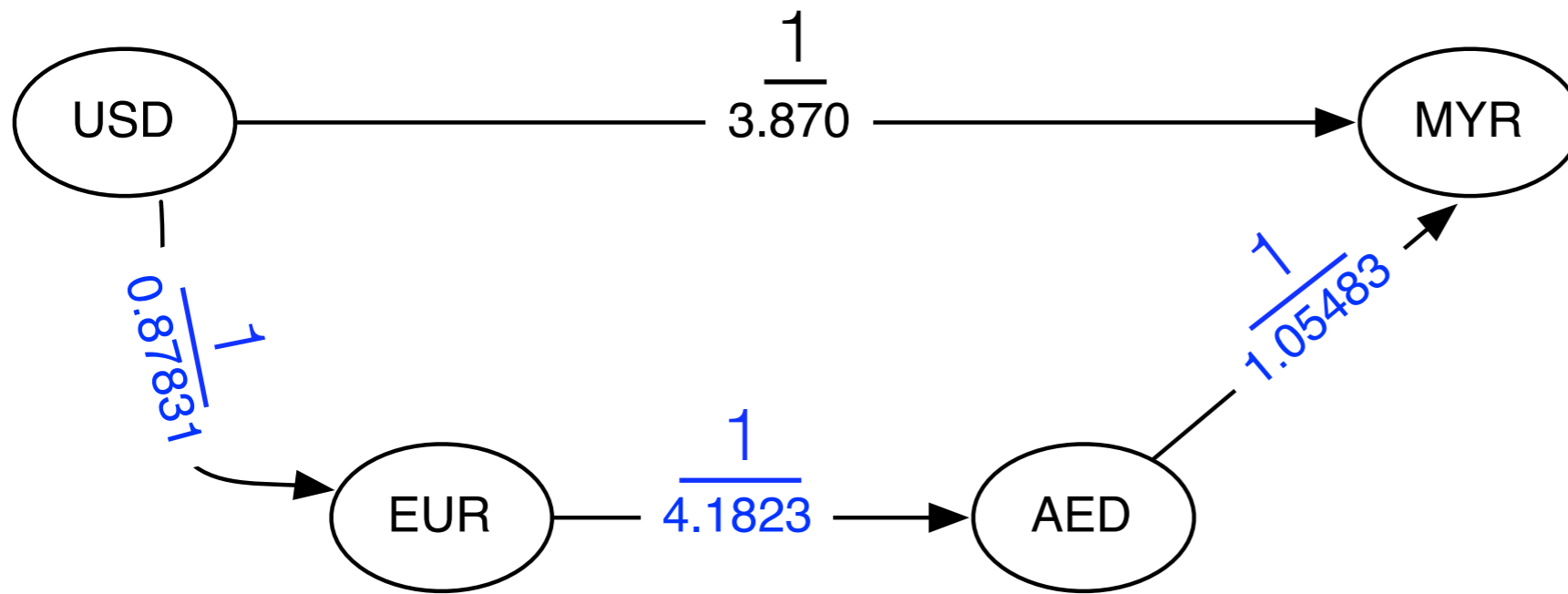
Trying to find
Max weight
(mult) Paths



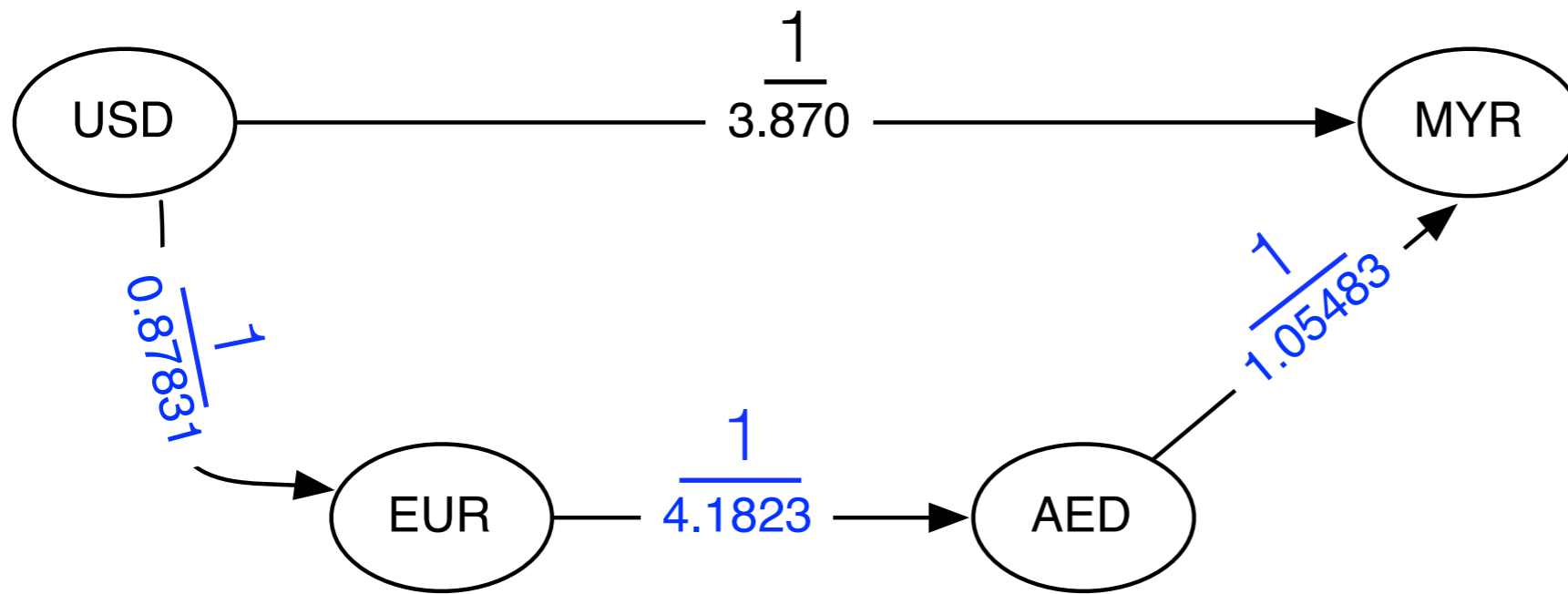
Trying to find
Max weight
(mult) Paths



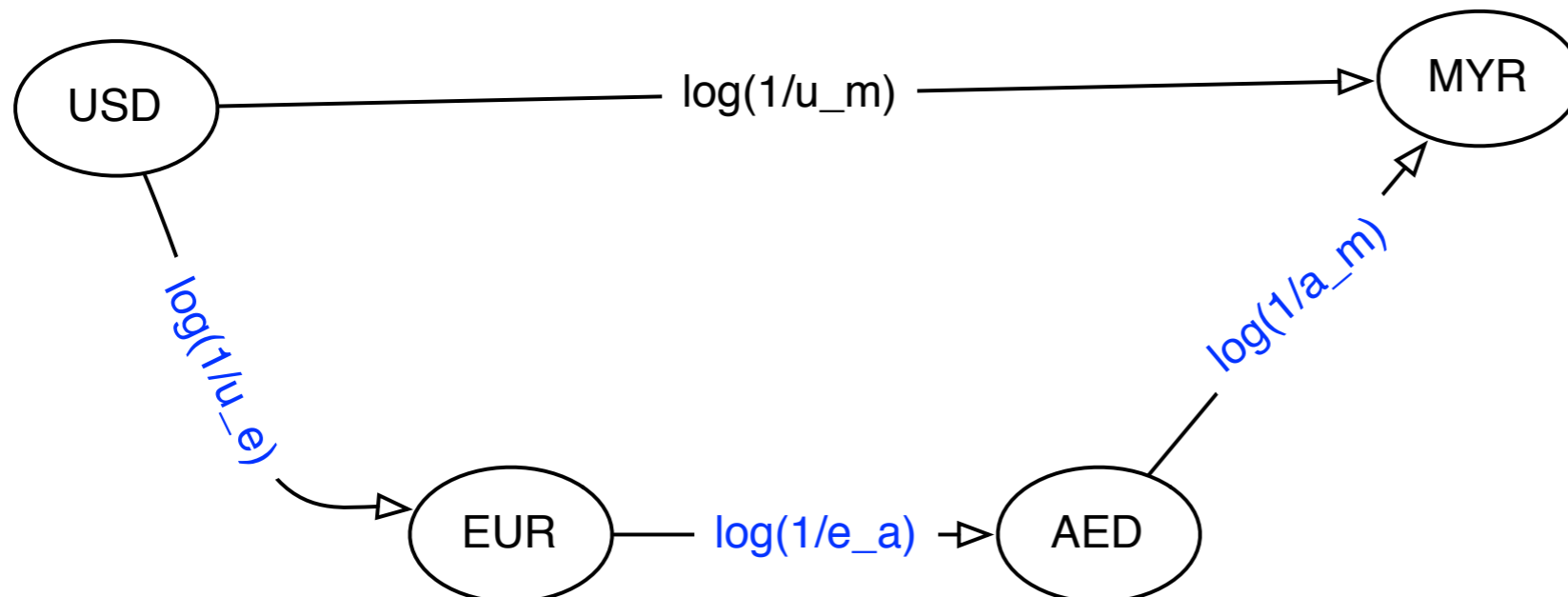
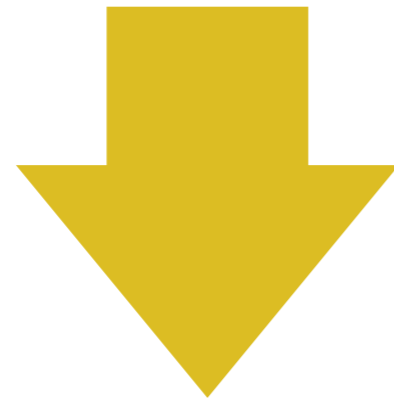
Trying to find
MIN weight
(mult) Paths

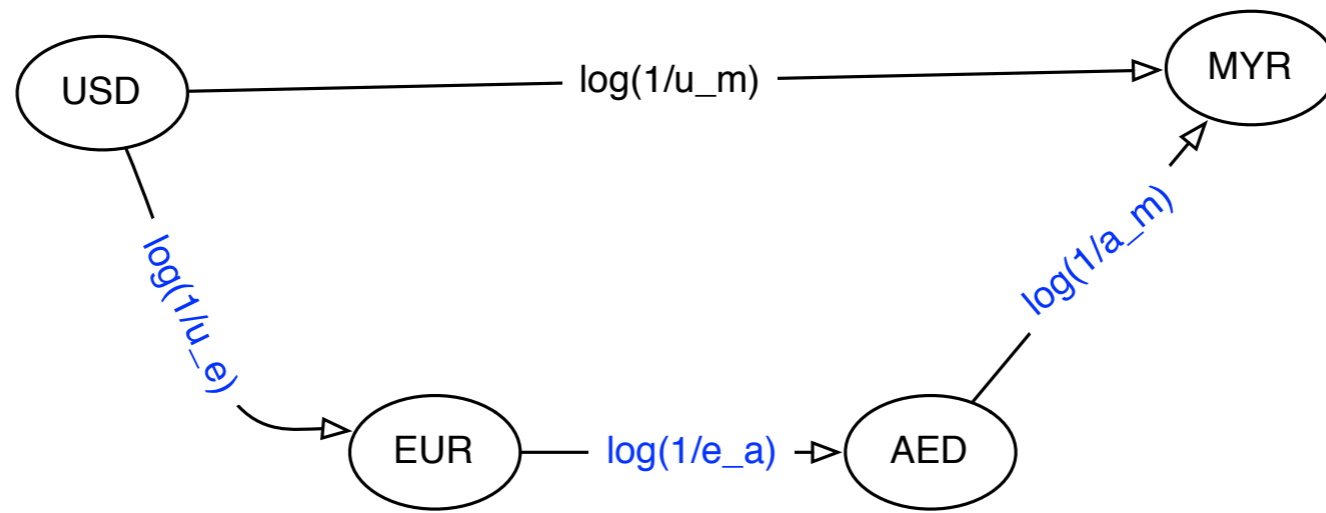


Trying to find
MIN weight
(mult) Paths



Trying to find
MIN weight
 (mult) Paths





SSSP(G, s)

SHORT $_{i,v}$ =

SSSP(G, s)

$$\text{SHORT}_{i,v} = \begin{cases} \infty & i = 0 \\ 0 & v = s \\ \min_{x \in V} \left\{ \begin{array}{l} \text{SHORT}_{i-1,v} \\ \text{SHORT}_{i-1,x} + w(x,v) \end{array} \right\} & \end{cases}$$

max len of a simple path:

Bellman-Ford(G, s)

BELLMAN-FORD(G, s)

1 $\text{SHORT}_{0,s} \leftarrow 0$

2 $\forall v \in V - \{s\}, \text{SHORT}_{0,v} \leftarrow \infty$

3 **for** $i = 1, \dots, V - 1$

4 **do for** each $v \in V - \{s\}$

5 **do** $\text{SHORT}_{i,v} = \min_{x \in \text{Adj}(v)} \left\{ \begin{array}{l} \text{SHORT}_{i-1,v} \\ w(x, v) + \text{SHORT}_{i-1,x} \end{array} \right\}$

BELLMAN-FORD(G, s)

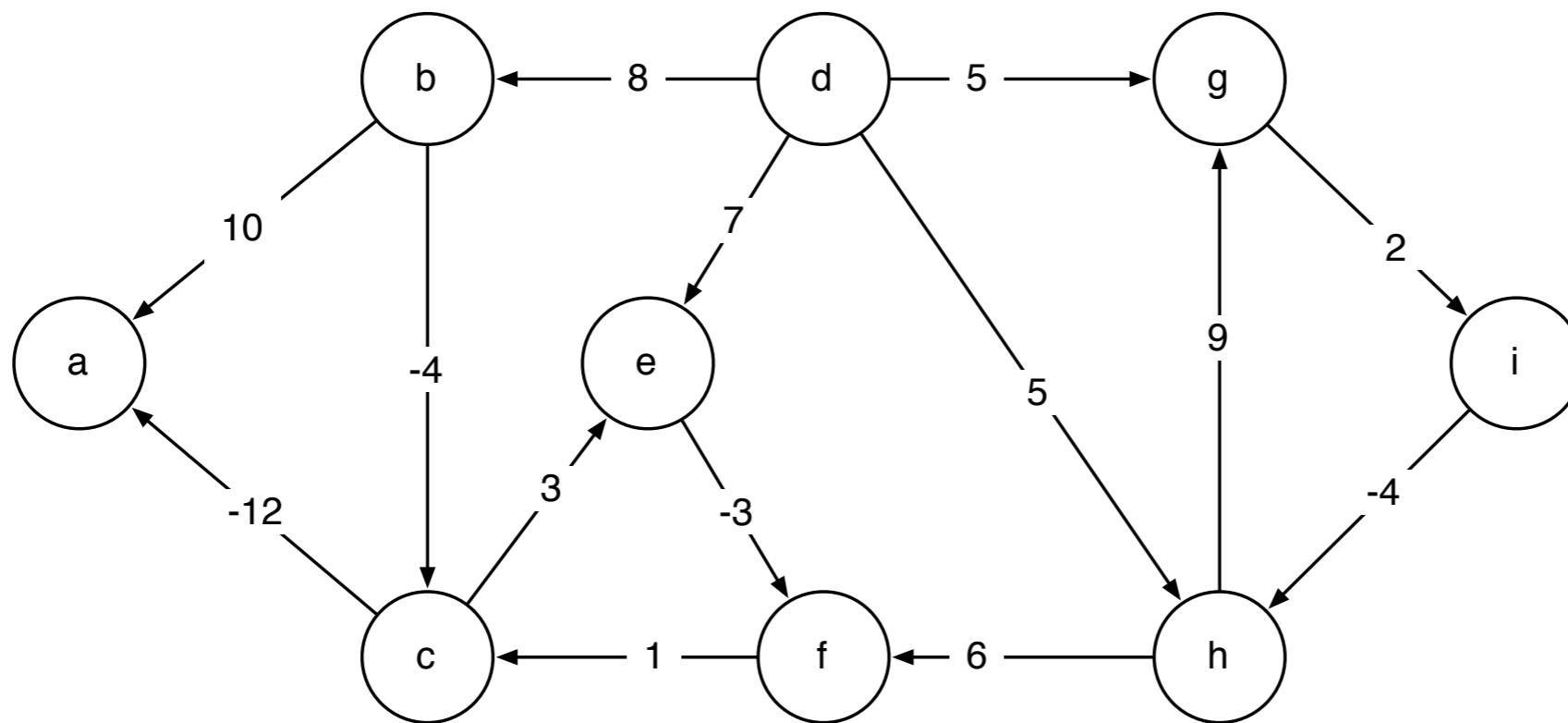
1 $\text{SHORT}_{0,s} \leftarrow 0$

2 $\forall v \in V - \{s\}, \text{SHORT}_{0,v} \leftarrow \infty$

3 **for** $i = 1, \dots, V - 1$

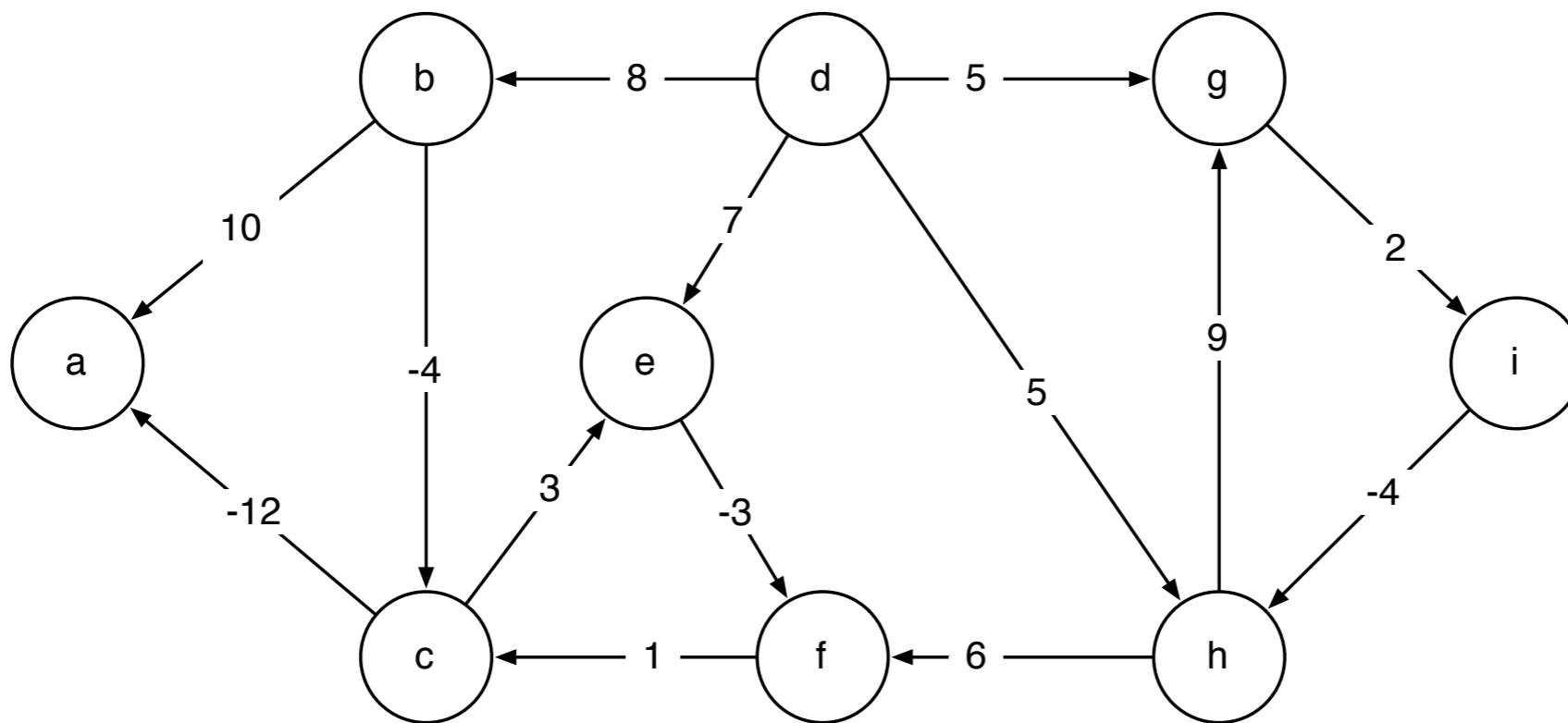
4 **do for** each $e = (x, y) \in E$

5 **do** $\text{SHORT}_{i,y} = \min \left\{ \begin{array}{l} \text{SHORT}_{i-1,y} \\ \text{SHORT}_{i,y} \\ w(x, y) + \text{SHORT}_{i-1,x} \end{array} \right\}$



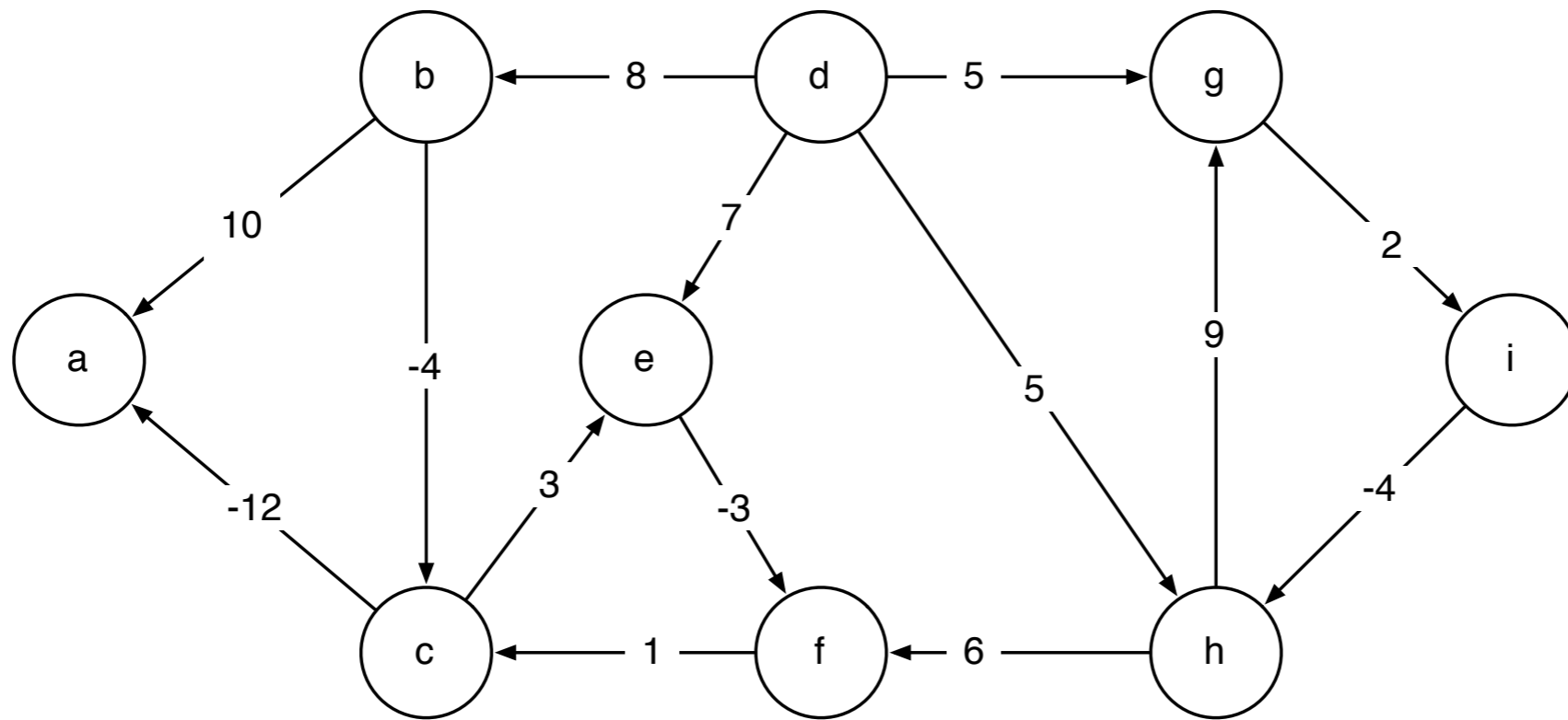
$$\text{SHORT}_{i,v} = \begin{cases} \infty & i = 0 \\ 0 & v = s \\ \min_{x \in V} \left\{ \begin{array}{l} \text{SHORT}_{i-1,v} \\ \text{SHORT}_{i-1,x} + w(x,v) \end{array} \right\} & \end{cases}$$

	8						
0	0						
	7						
	5						
	5						



$$\text{SHORT}_{i,v} = \begin{cases} \infty & i = 0 \\ 0 & v = s \\ \min_{x \in V} \left\{ \begin{array}{l} \text{SHORT}_{i-1,v} \\ \text{SHORT}_{i-1,x} + w(x,v) \end{array} \right\} & \end{cases}$$

		18					
	8	8					
		4					
0	0	0					
	7	7					
		4					
	5	5					
	5	5					
		7					



$$\text{SHORT}_{i,v} = \begin{cases} \infty & i = 0 \\ 0 & v = s \\ \min_{x \in V} \left\{ \begin{array}{l} \text{SHORT}_{i-1,v} \\ \text{SHORT}_{i-1,x} + w(x,v) \end{array} \right\} & \end{cases}$$

		18	-8				
	8	8	8				
		4	4				
0	0	0	0				
	7	7	7				
		4	4				
	5	5	5				
	5	5	3				
		7	7				

Optimization

BELLMAN-FORD(G, s)

```
1  SHORT0,s ← 0
2  ∀v ∈ V − {s}, SHORT0,v ← ∞
3  for i = 1, ..., V − 1
4      do for each e = (x, y) ∈ E
5          do SHORTi,y = min {
```

$$\left. \begin{array}{l} \text{SHORT}_{i-1,y} \\ \text{SHORT}_{i,y} \\ w(x, y) + \text{SHORT}_{i-1,x} \end{array} \right\}$$

BELLMAN-FORD(G, s)

```
1  ds ← 0
2  ∀v ∈ V − {s}, dv ← ∞
3  for i = 1, ..., V − 1
4      do for each e = (x, y) ∈ E
5          do dy ← min { dy, w(x, y) + dx }
```

running time

BELLMAN-FORD(G, s)

1 $d_s \leftarrow 0$

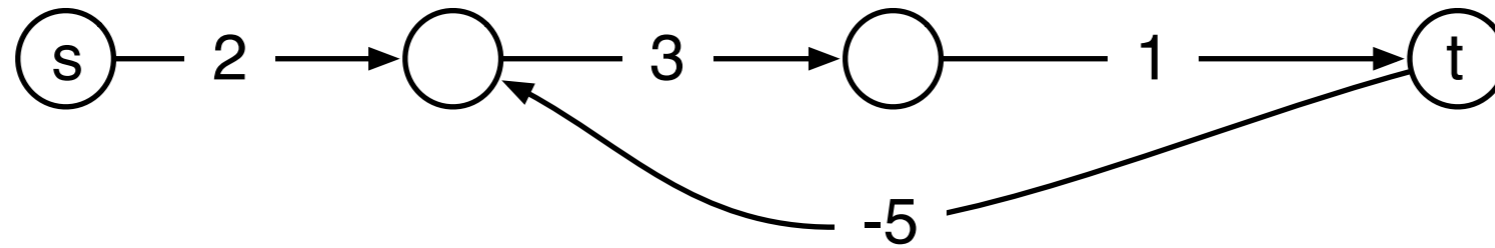
2 $\forall v \in V - \{s\}, d_v \leftarrow \infty$

3 **for** $i = 1, \dots, V - 1$

4 **do for** each $e = (x, y) \in E$

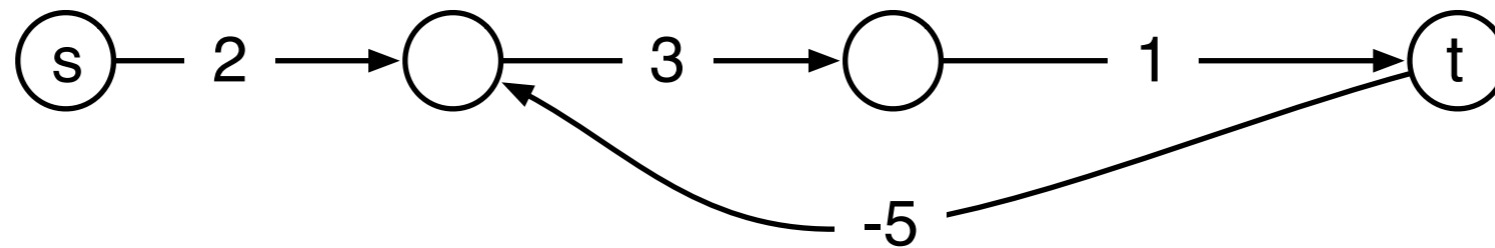
5 **do** $d_y \leftarrow \min \{ d_y, w(x, y) + d_x \}$

negative cycles?



s	0				
a					
b					
t					

negative cycles?



s	0	0	0	0
a	2	2	2	1
b		5	5	5
t			6	6

L5

Hard to agree

abhi shelat

Name:

“For the second time in less than a week, Michel Barnier has signalled his desire to move ahead on the Brexit negotiations, less than seven months before the United Kingdom is slated to leave the European Union on March 29, 2019. On Monday, Barnier, the EU’s chief negotiator, told a forum in Slovenia that “if we are realistic, we are able to reach an agreement on the first stage of the negotiation, which is the Brexit treaty, within six or eight weeks.”

What should happen to the GBP and why?

“The ECB president told the European Parliament ... “Underlying inflation is expected to increase further over the coming months as the tightening labor market is pushing up wage growth,” Draghi said on Monday. “Domestic price pressures are strengthening and broadening.””

What should happen to the EURO and why?

The simple model

n parties, party i holds private value v_i . m are faulty.

The simple model

n parties, party i holds private value v_i . m are faulty.

Parties communicate via 2-party msgs.

Network fail-safe, low delay, authenticated.

The simple model

n parties, party i holds private value v_i . m are faulty.

Parties communicate via 2-party msgs.

Network fail-safe, low delay, authenticated.

Goal: compute a value for each party such that:

The simple model

n parties, party i holds private value v_i . m are faulty.

Parties communicate via 2-party msgs.

Network fail-safe, low delay, authenticated.

Goal: compute a value for each party such that:

All non-faulty parties compute same vector **V**

The simple model

n parties, party i holds private value v_i . m are faulty.

Parties communicate via 2-party msgs.

Network fail-safe, low delay, authenticated.

Goal: compute a value for each party such that:

All non-faulty parties compute same vector \mathbf{V}

If party i is not faulty, value $\mathbf{V}_i =$ private value v_i

Reaching Consensus

[PLS protocol for $n=4$]

1. Pick your value v_i
2. Send v_i to every party.

Receive (a_1, \dots, a_4) , take majority in each slot, excluding report of player i for slot i .

Reaching Consensus

[PLS protocol for $n=4$]

1. Pick your value v_i
2. Send v_i to every party.
3. After receiving $a_i=(v_1, \dots, v_4)$ from each other party, send your list of received values a_i to every party.

Receive (a_1, \dots, a_4) , take majority in each slot, excluding report of player i for slot i .

Reaching Consensus

[PLS protocol for $n=4$]

1. Pick your value v_i
2. Send v_i to every party.
3. After receiving $a_i=(v_1, \dots, v_4)$ from each other party, send your list of received values a_i to every party.
4. Receive (a_1, \dots, a_4) , take majority in each slot, excluding report of player i for slot i .

Why does PLS $n=4$ work?

What happens if everyone is honest?

P1 output: (_ , _ , _ , _)

P2 output: (_ , _ , _ , _)

P3 output: (_ , _ , _ , _)

P4 output: (_ , _ , _ , _)

Why does PLS $n=4$ work?

What happens if one party, say P1, is faulty?

P2 output: (__, __, __, __)

P3 output: (__, __, __, __)

P4 output: (__, __, __, __)

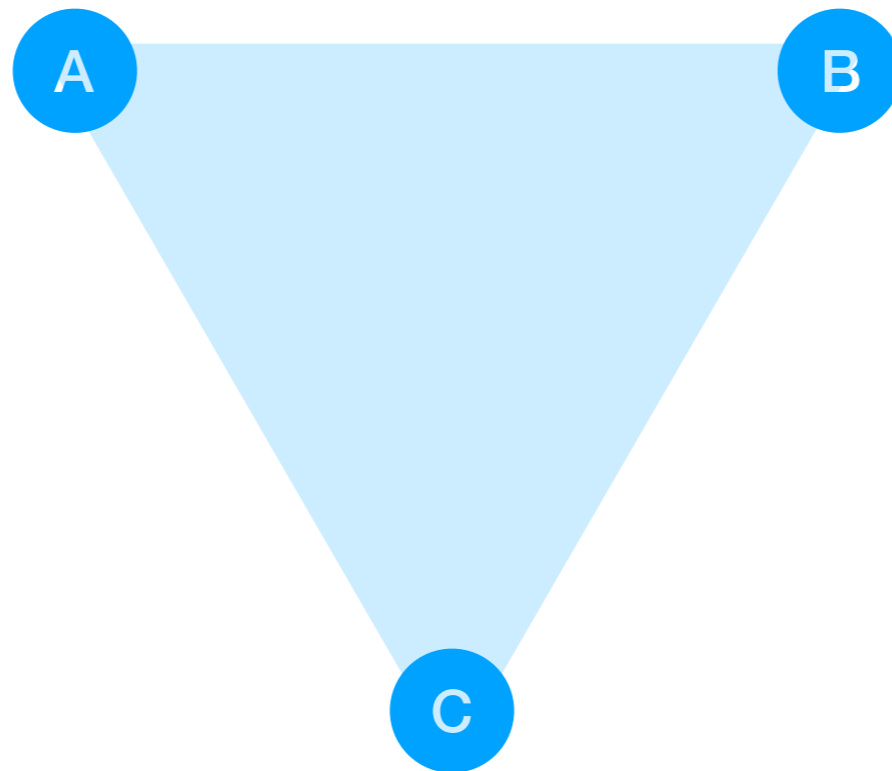
PLS can be generalized

Works whenever $n > 3m$

Works whenever $n > 3m$

Only works with $n > 3m$

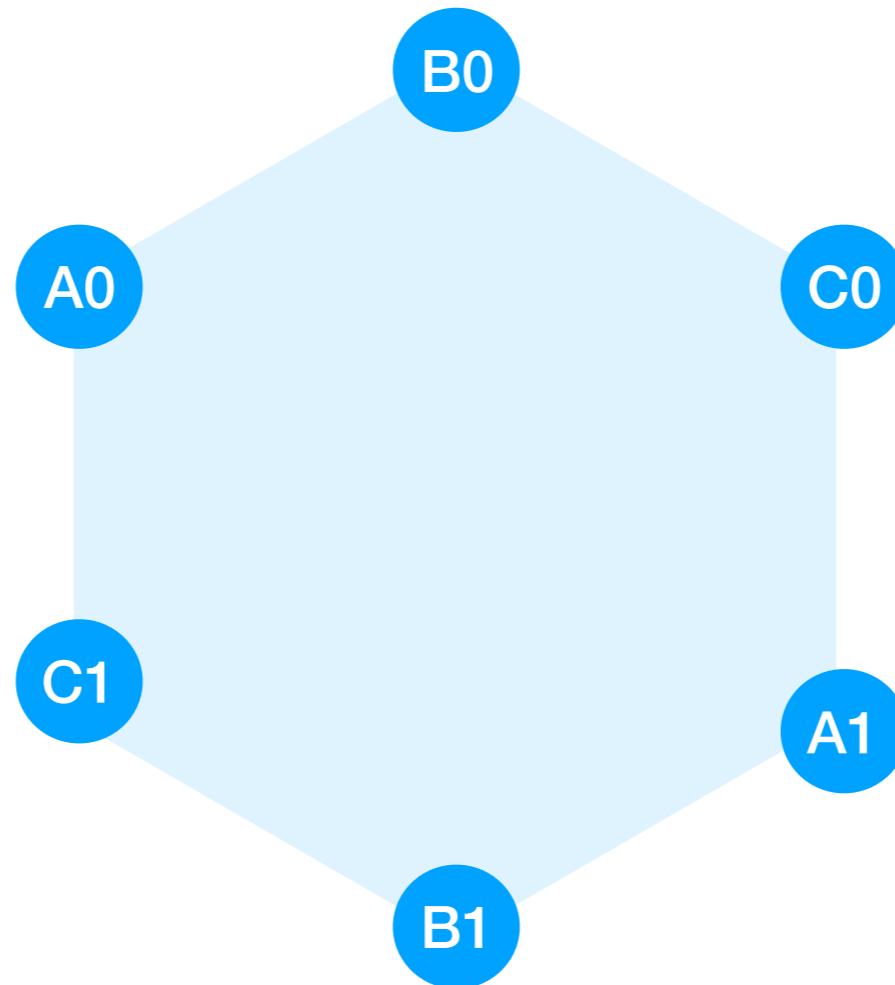
[Fischer-Lynch-Merritt proof]



Consider $n=3$, $m=1$ parties.

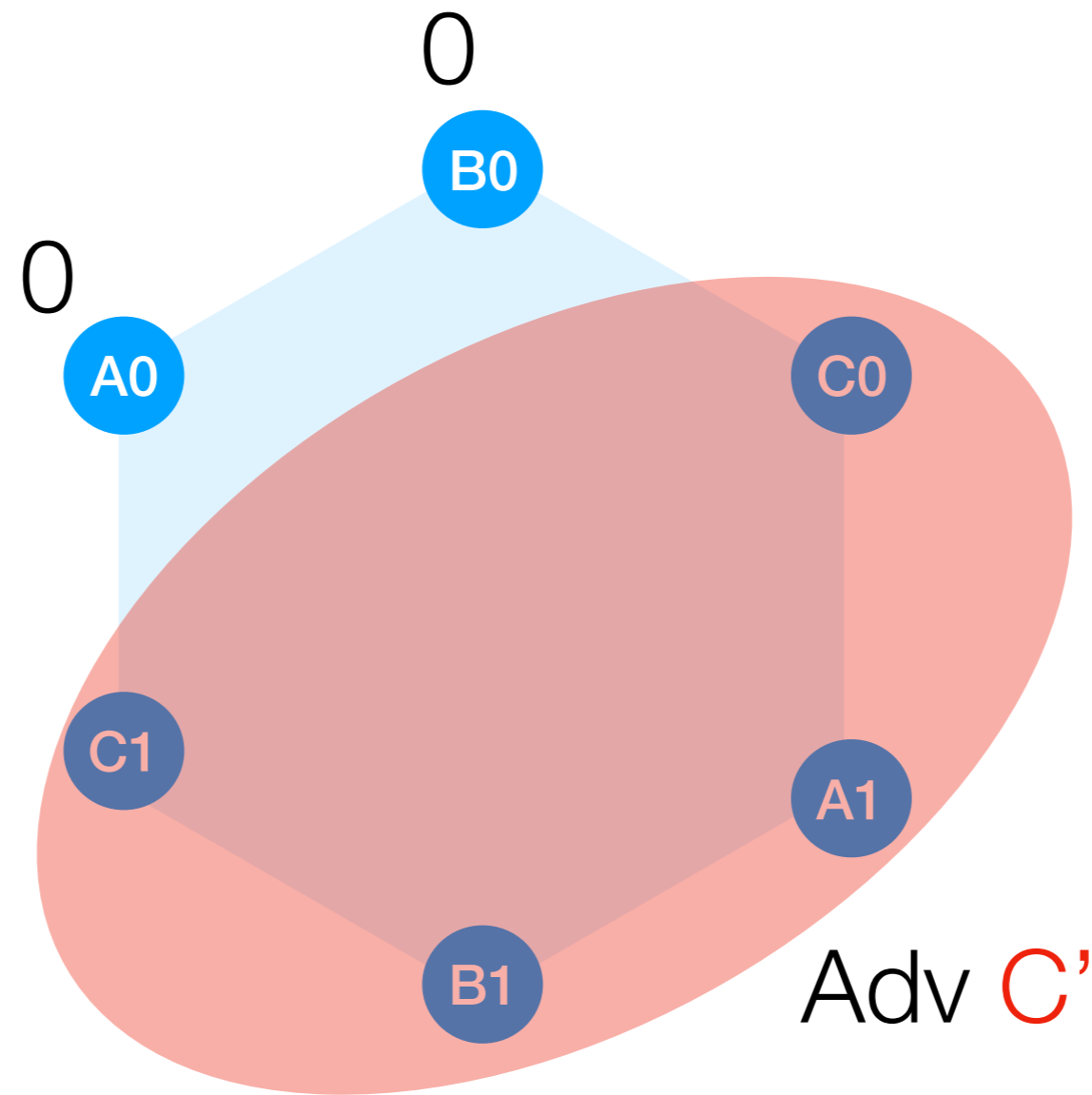
Only works with $n > 3m$

[Fischer-Lynch-Merritt proof]



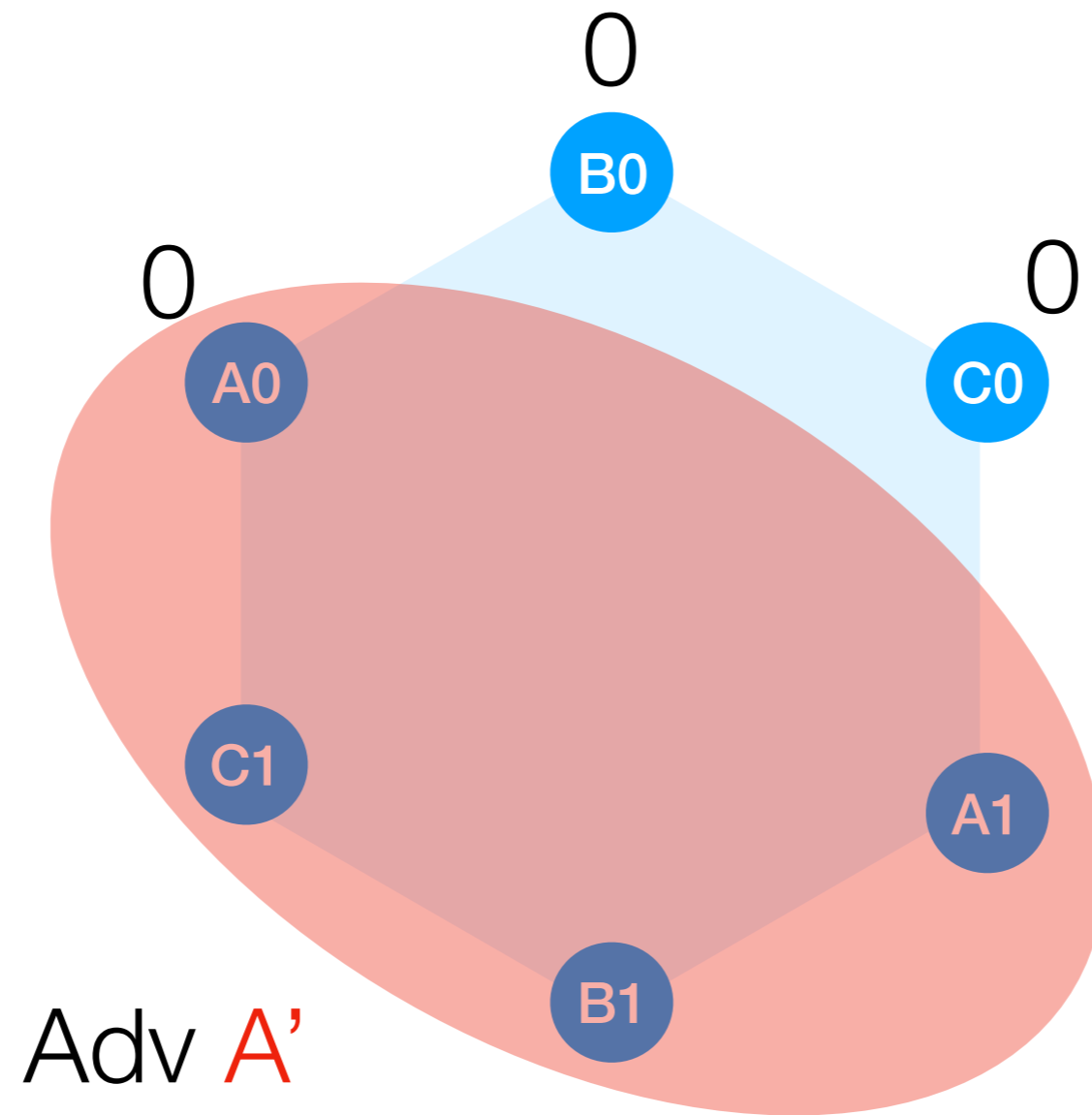
Duplicate parties, P_i running protocol with input i .

Only works with $n > 3m$



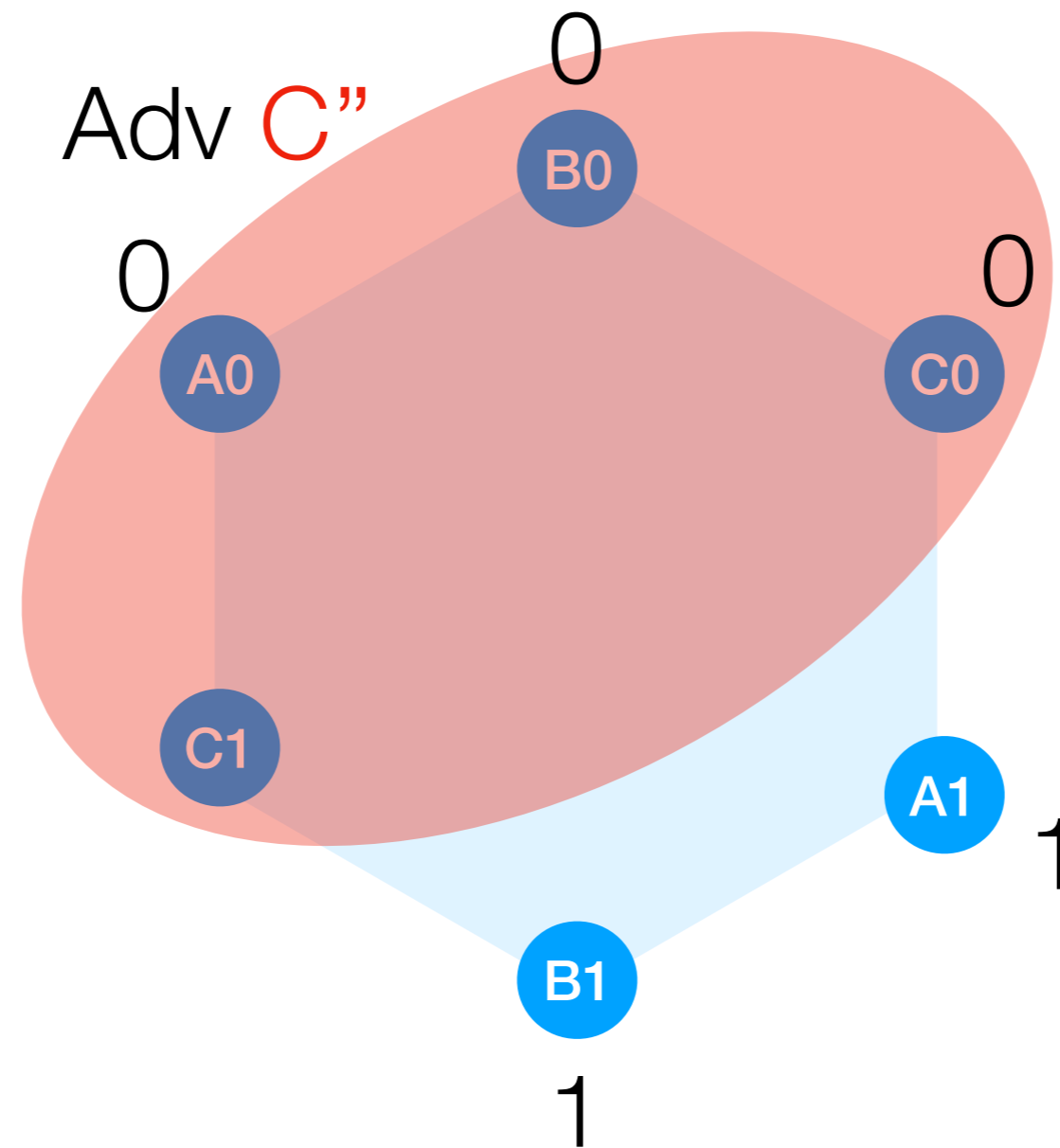
By consensus, honest parties output 0.

Only works with $n > 3m$



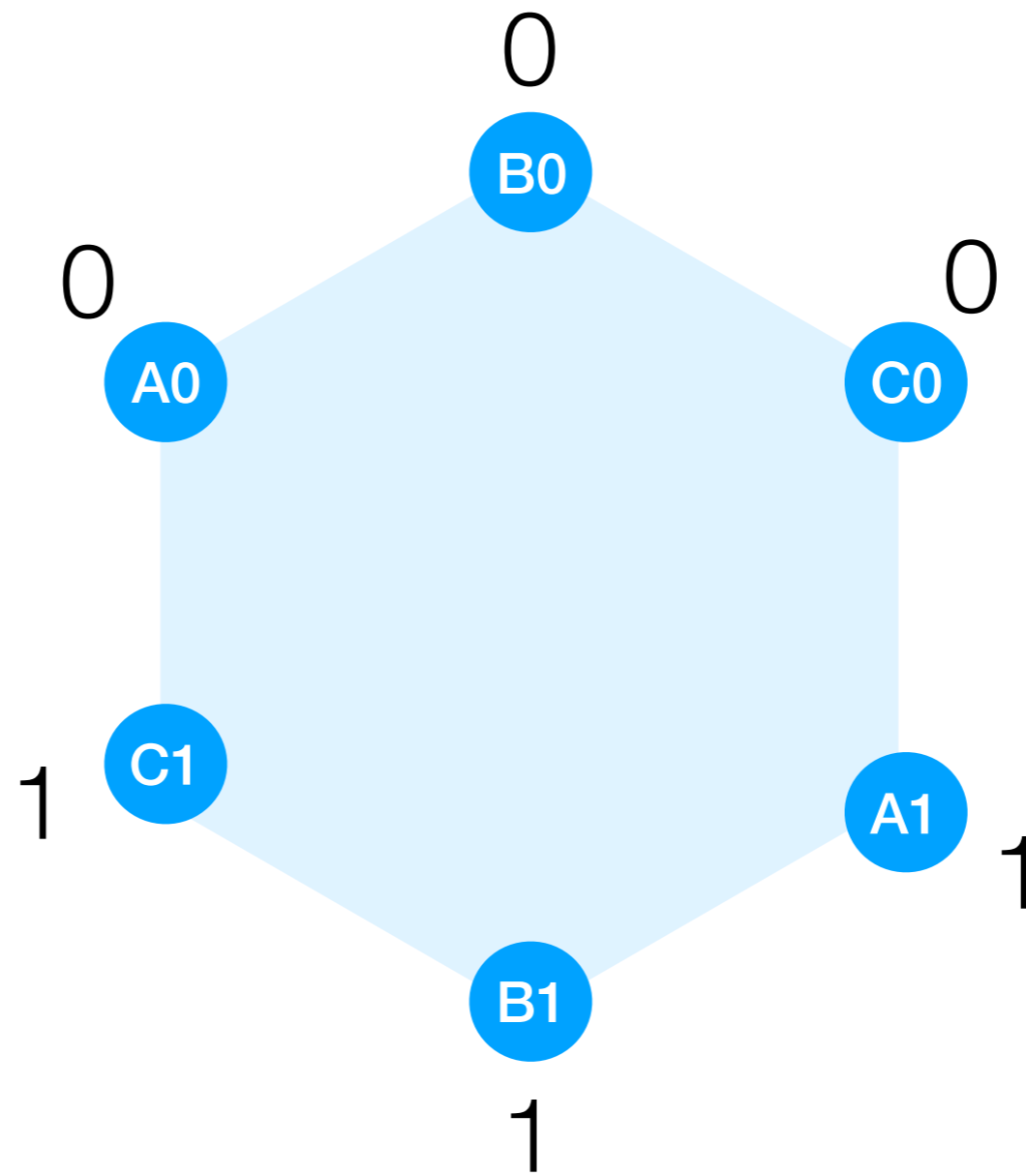
By consensus, honest parties output 0.

Only works with $n > 3m$



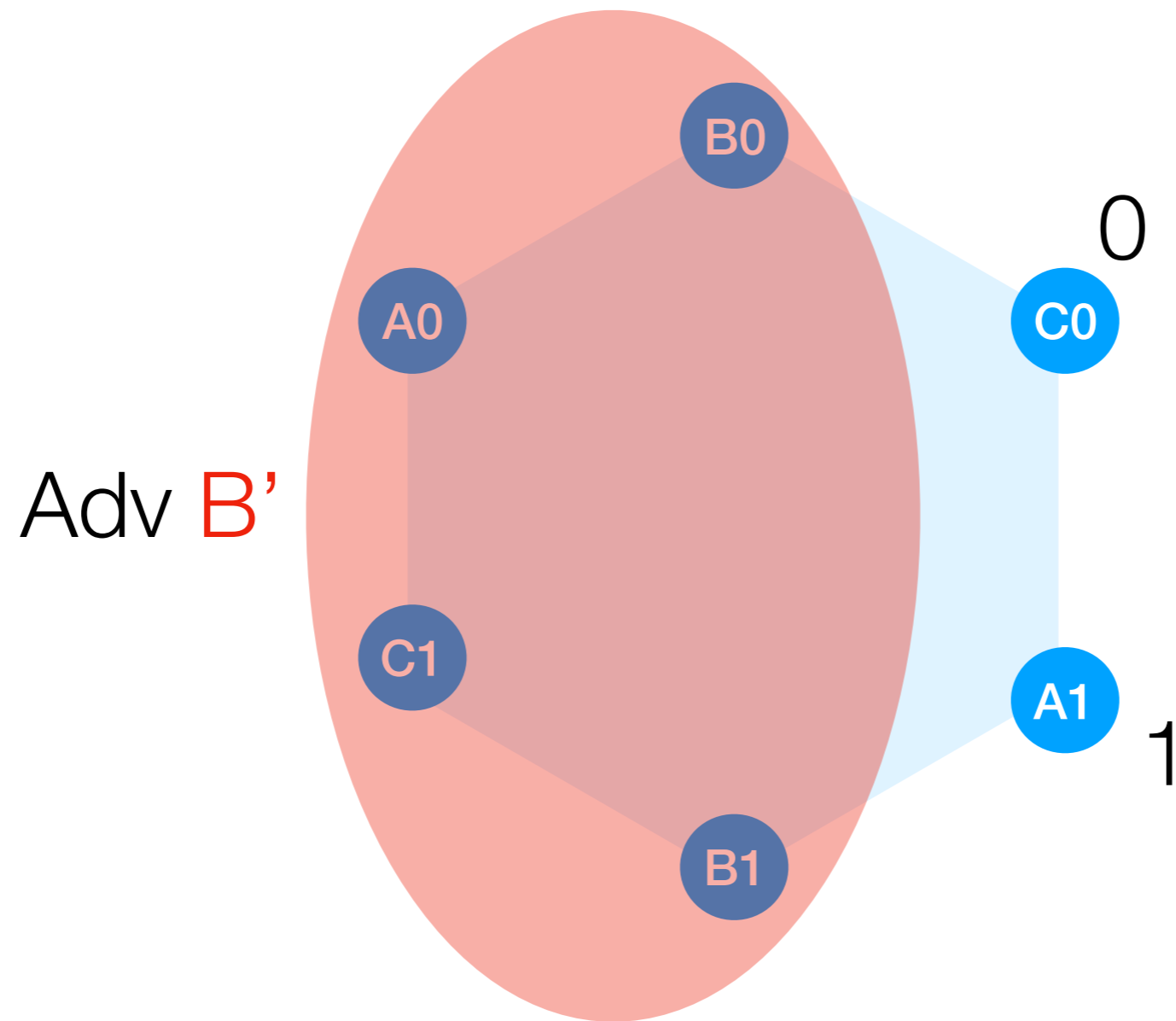
By consensus, honest parties output 0.

Only works with $n > 3m$



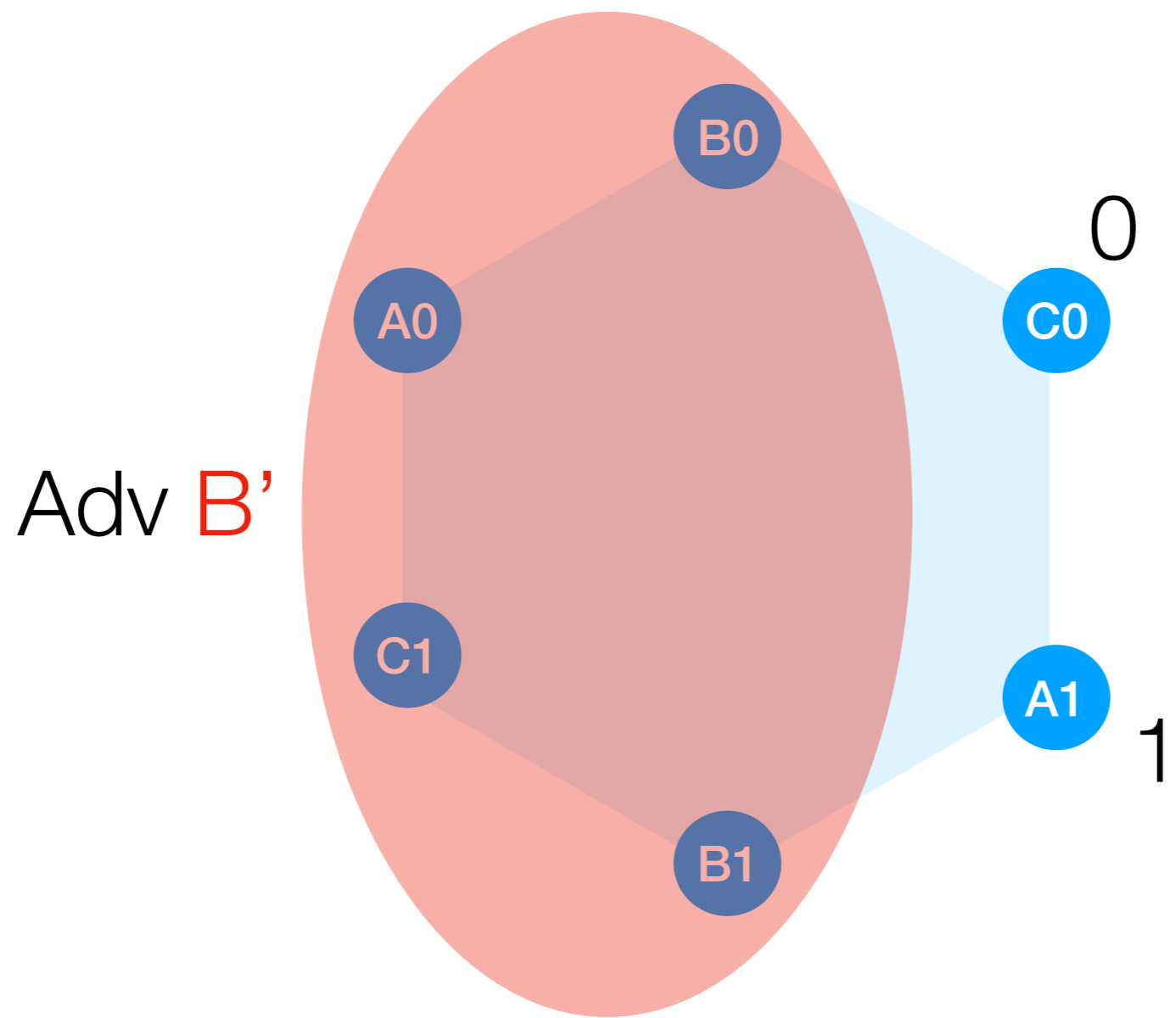
These must be the outputs.

Only works with $n > 3m$



Thus, there exists Adv B' which violates consistency.

Given PLS/FLM
impossibility, how can
Bitcoin tolerate $1/2$
adversary?



New adv model

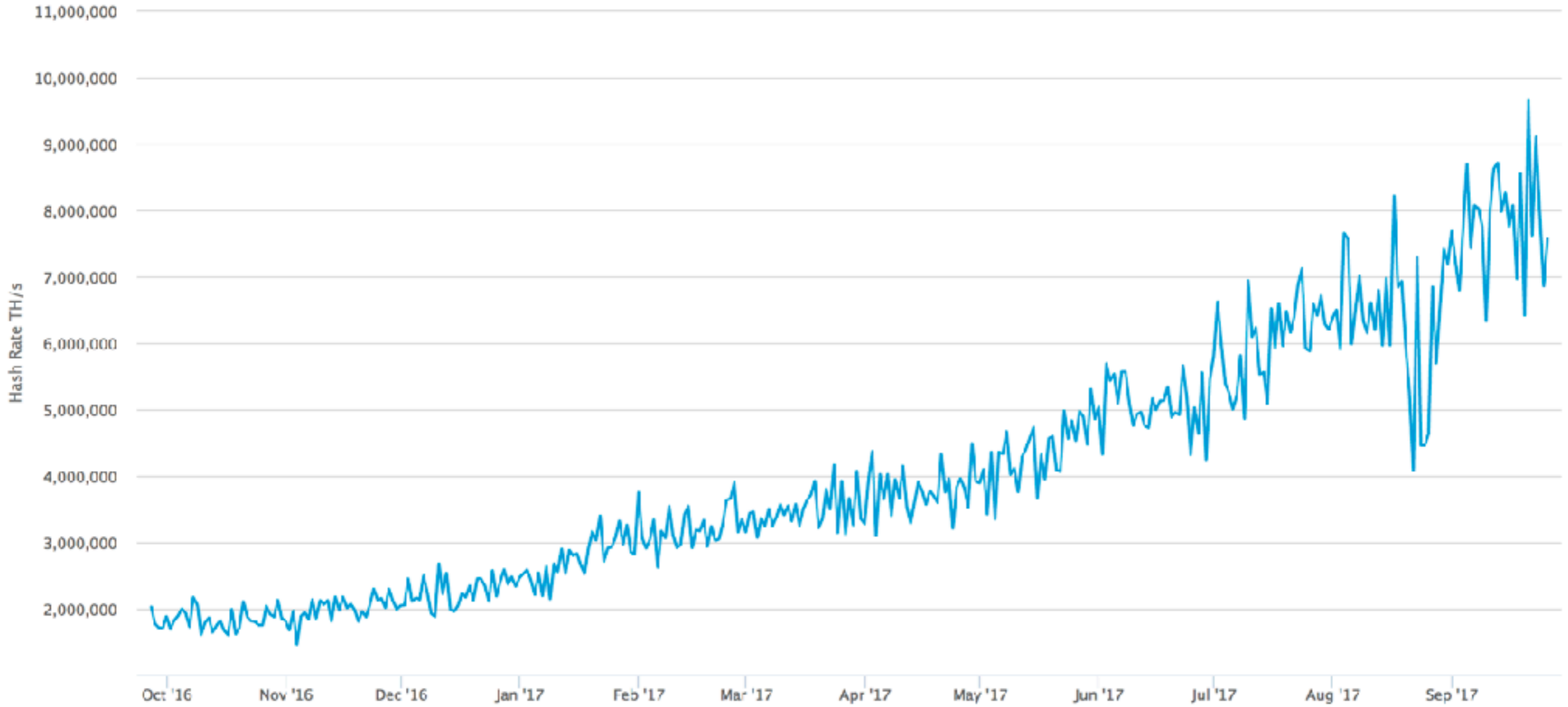
Adv controls $< 1/2$ of CPUs

How realistic is this model?

Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.

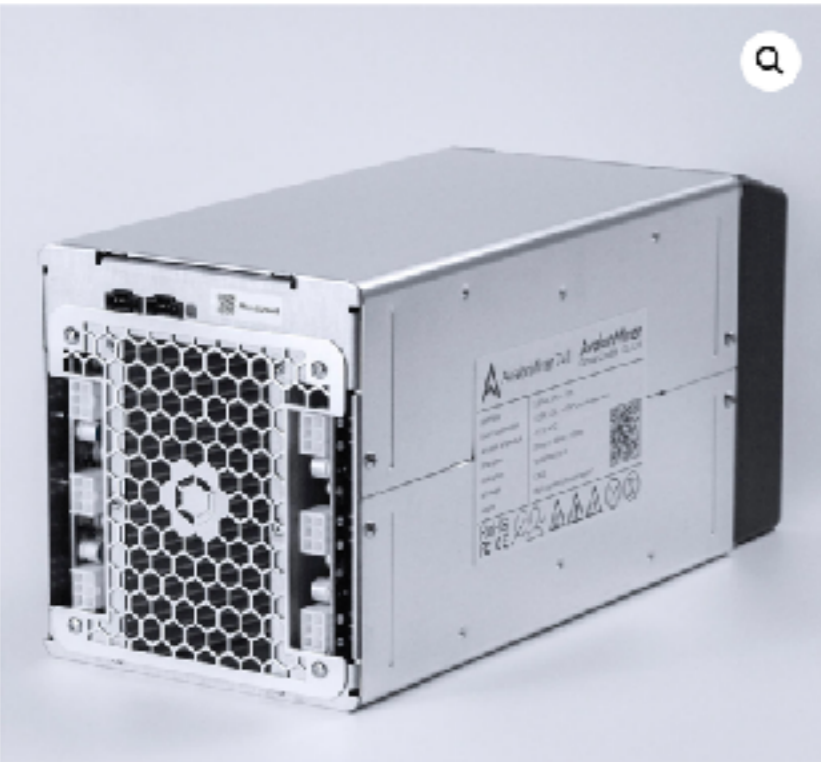
Source: blockchain.info



From blockchain.info

8m TH/s

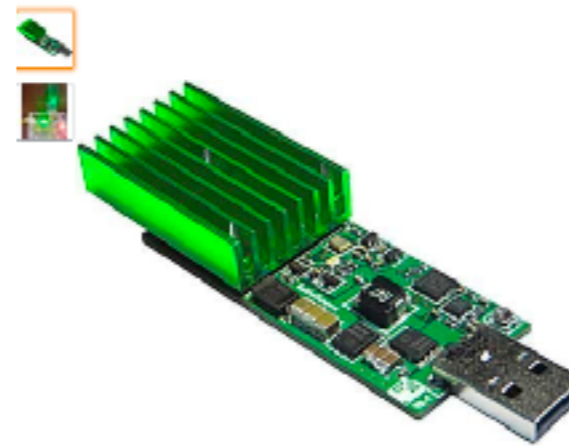
Home / AvalonMiner 741



AvalonMiner 741

\$798.00

Out of stock



GEKKOSCIENCE

GekkoScience Compac USB Stick Bitcoin Miner
8gh/s+ (BM1384)

★★★★☆ · 39 customer reviews | 50 answered questions

Note: This item is only available from third-party sellers (see all offers).

Available from these sellers.

- 15+gh/s mining speed (higher speed requires usb port above spec)
- 31-35 watts per gh!
- Completely silent operation
- Bitcoin BM1384 chips
- ▶ See more product details

New (1) from \$69.97 + \$4.56 shipping

[Report incorrect product information.](#)

7.3 TH/s (RTHS) (7.3-8 RTH/s in field)

≈ 1150W, +0% ~ +15% (with 93% PSU efficiency @ 25 C)

0.16 Joules/GigaHash at the wall

Max 12.53

88 x A3212 16nm ASIC

Ethereum Network HashRate Growth Chart

Reset zoom



Source: Etherscan.io
Click and drag in the plot area to zoom in



Incentives

Not clear how to use a 51%
attack to earn back the
investment in mining hardware.

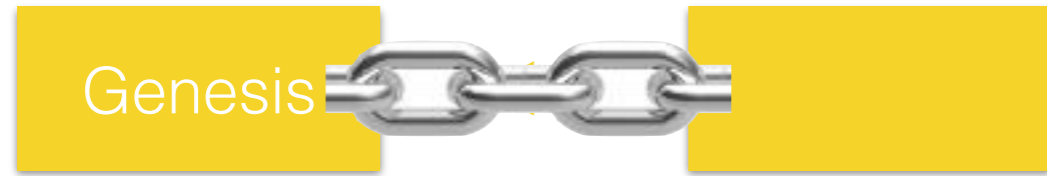
L6: Blockchains

abhi shelat
17f-money

What is a blockchain

Genesis

What is a blockchain

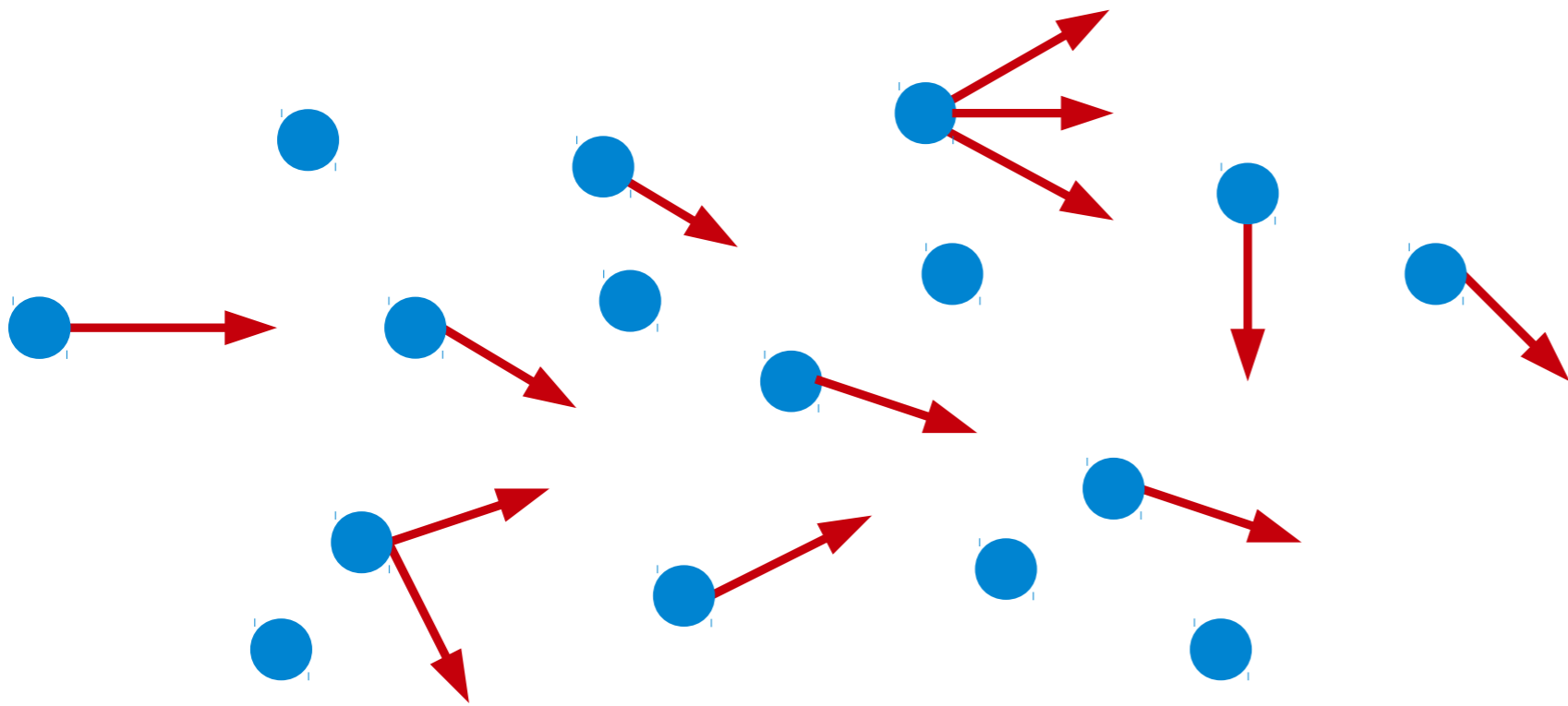


What is a blockchain

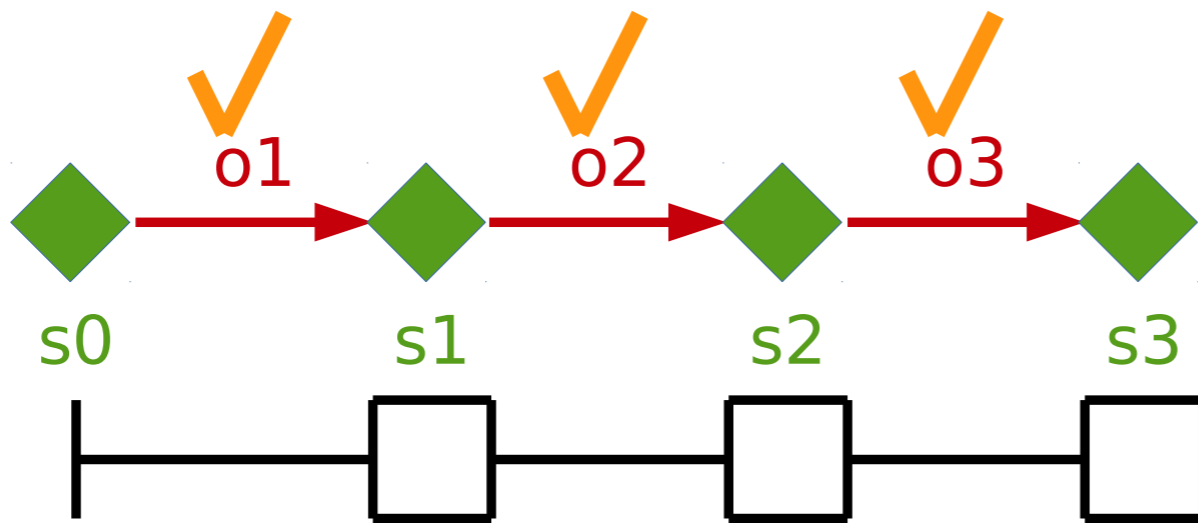



What does it do?

Expenses in the year 1846		1844	
commencing from the 1 st		Amt. brought over	
	cts		off 43 63
Stage passage to Columbia	\$ 7 00	one coat cloth	4 25
Dinner at Union Court House	38	booking utensils	5 75
Stay in Columbia all night	75	2 Breeches for James	2 10
Breakfast	50	Board for Emily 10 days	2 50
Passage to Charleston	6 50	Board for Charlost 10 days	2 50
Staying all night in Columbia	1 00	Tent poles & towing them	1 02
Boy for carrying my trunk to the boat	25	one suit of clothes for James	1 50
Omnibus in Charleston town	75	James board for 5 days	1 25
Staying a day in Charleston	1 75	Barcas & his child Board 18 days	4 25
Passage to Weldon Is. 6.	13 00	Ann's Board for 3 days	75
Breakfast on board of the Boat	50	one trip for Ann	1 00
Passage to Richmond	4 25	My expenses to Lunenburg Court	6 58
Supper	50	Washing 12 garments	75
Omnibus in Richmond	50	one whip	1 50
4 days board at the bell Tavern etc	5 00	Pikeage gate	19.
8 garments washed	50	Crossing the James River	25
4 drinks of liquor	25	Staying all night	1 58
1 qt of whiskey for negroes	25	Crossing North river	25
	43 63		82 20



Nodes
produce
transactions 



Nodes
Run a protocol to
construct the **public**
ledger 

Height	Age	Relayed By
382148	4 minutes	BTCC Pool
382147	6 minutes	Eligius
382146	10 minutes	KnCMiner
382145	20 minutes	F2Pool
382144	40 minutes	BitFury
382143	42 minutes	BTCC Pool

Latest Transactions

[c42b3e34126db1e65e37e9413...](#)

0.4106 BTC

[ae328c6591f5054f4676df95d...](#)

0.02970983 BTC

[0b6e60fc852b43d48e57e68fe...](#)

0.5613794 BTC

Height	Age	Relayed By
382148	4 minutes	BTCC Pool
382147	6 minutes	Eligius
382146	10 minutes	KnCMiner
382145	20 minutes	F2Pool
382144	40 minutes	BitFury
382143	42 minutes	BTCC Pool

Latest Transactions

[c42b3e34126db1e65e37e9413...](#)

0.4106 BTC

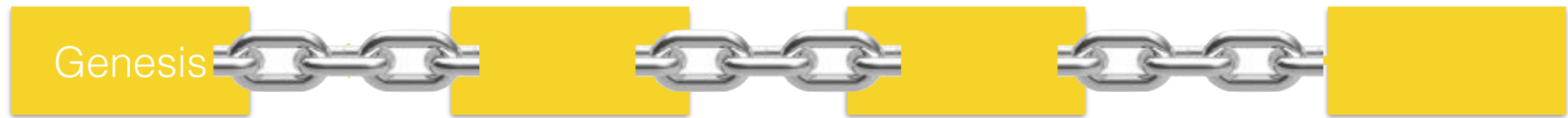
[ae328c6591f5054f4676df95d...](#)

0.02970983 BTC

[0b6e60fc852b43d48e57e68fe...](#)

0.5613794 BTC

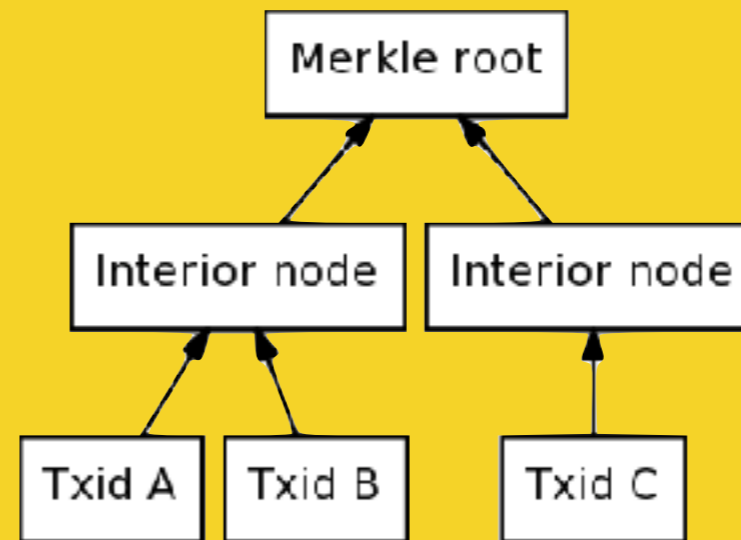
Blockchain datastructure



Blockchain datastructure

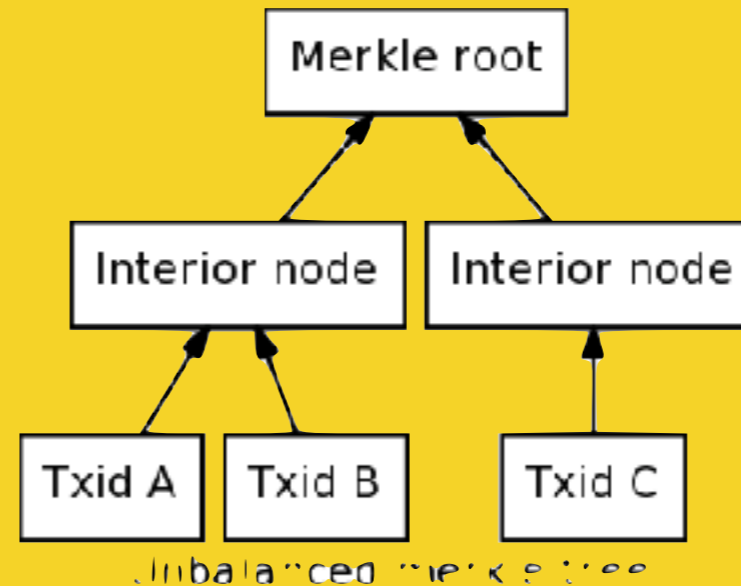


- 4 Version
- 32 previousBlockHash
- 32 MerkleRoot of Transactions
- 4 Time
- 4 Bits
- 4 Nonce



Unbalanced merkle tree

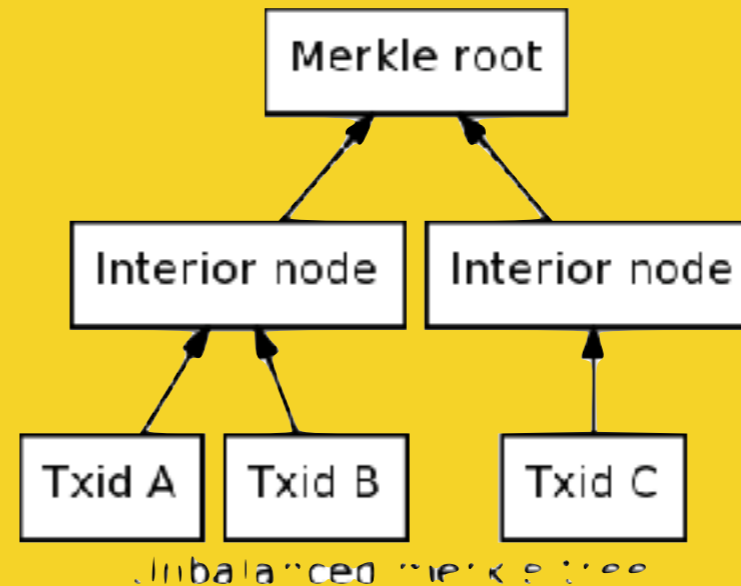
- 4 Version
- 32 previousBlockHash
- 32 MerkleRoot of Transactions
- 4 Time
- 4 Bits
- 4 Nonce



Each block is named by:

SHA256(SHA256(Vers || Prev || Merkle || Time || Bits || Nonce)

4 Version
 32 previousBlockHash
 32 MerkleRoot of Transactions
 4 Time
 4 Bits
 4 Nonce

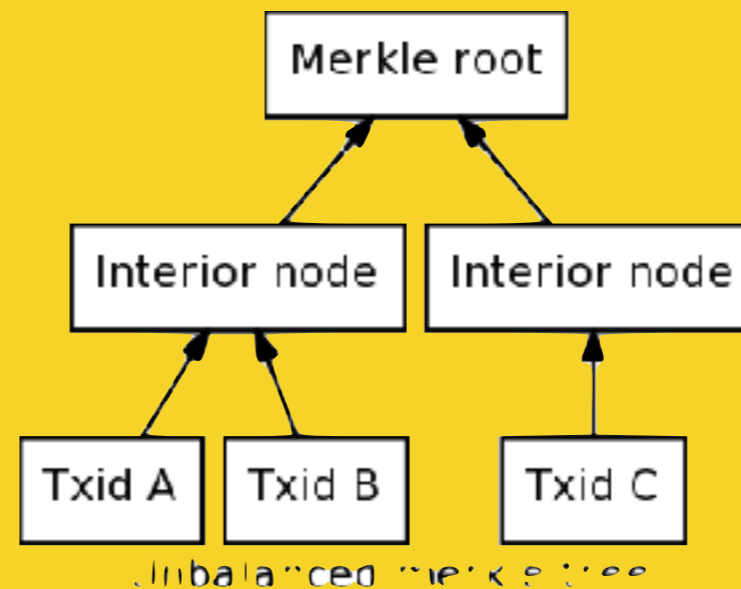


Each block is named by:

$\text{SHA256}(\text{SHA256}(\text{Vers} \parallel \text{Prev} \parallel \text{Merkle} \parallel \text{Time} \parallel \text{Bits} \parallel \text{Nonce}))$

Only blocks with $\text{Name} < D_{\text{time}}$ are valid.

4 Version
32 previousBlockHash
32 MerkleRoot of Transactions
4 Time
4 Bits
4 Nonce



Transactions can be any ledger entry.

In Bitcoin, they represent transfers of coin assets.

Block #443888

Summary

Number Of Transactions	444
Output Total	424.3016726 BTC
Estimated Transaction Volume	85.74330564 BTC
Transaction Fees	0.16513254 BTC
Height	443888 (Main Chain)
Timestamp	2016-12-17 20:29:03
Received Time	2016-12-17 20:29:03
Relayed By	SlushPool
Difficulty	310,153,855,703.43
Bits	402885509
Size	238.131 kB
Weight	952.272 kWU
Version	0x20000002
Nonce	777617094
Block Reward	12.5 BTC

Hashes

Hash	00000000000000000000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc
Previous Block	000000000000000000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214
Next Block(s)	000000000000000000000000000000002cc08d842aa0156b466c300a7bd756448d22ec337d4692c
Merkle Root	87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

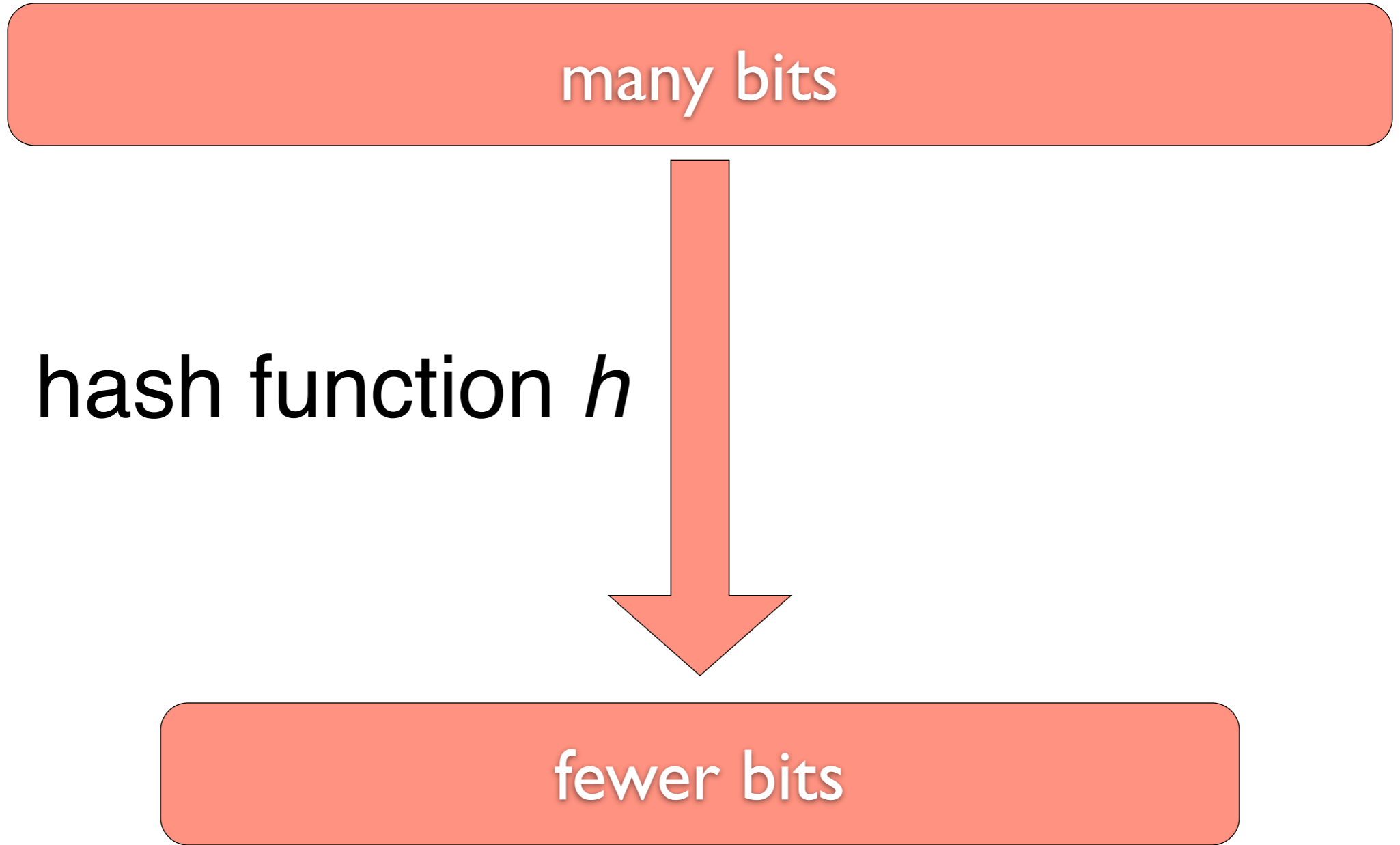
What is a hash function?

goal of a hash function

many bits

hash function h

fewer bits



a hash function is a function

$$h : \{0, 1\}^d \longrightarrow \{0, 1\}^r$$

such that h is easy to evaluate
and $r < d$

useful in data structures

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

Examples

```
ab2017:18f-money$ shasum -a 256 README.md  
6e7407cea997f98b6962a4ac3a2b15fb703209dc74b0ce  
cb566d59bd7a6ba813  README.md
```

Collisions should be rare

Block #443888

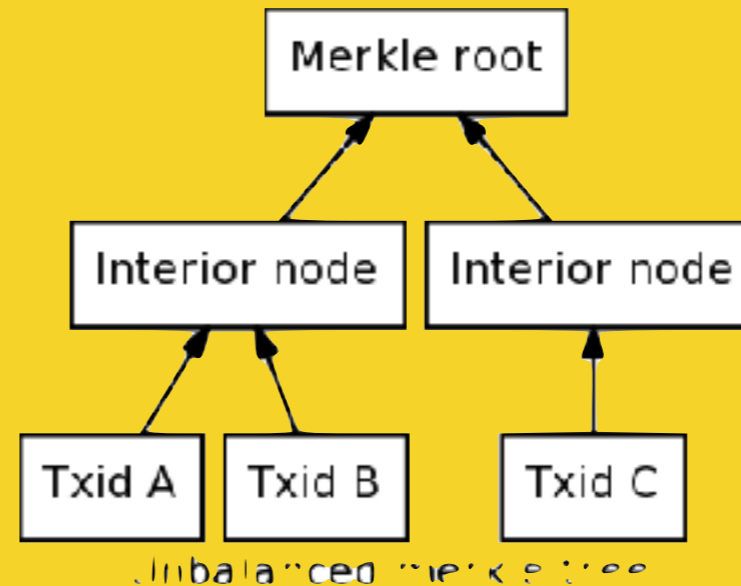
Summary

Number Of Transactions	444
Output Total	424.3016726 BTC
Estimated Transaction Volume	85.74330564 BTC
Transaction Fees	0.16513254 BTC
Height	443888 (Main Chain)
Timestamp	2016-12-17 20:29:03
Received Time	2016-12-17 20:29:03
Relayed By	SlushPool
Difficulty	310,153,855,703.43
Bits	402885509
Size	238.131 kB
Weight	952.272 kWU
Version	0x20000002
Nonce	777617094
Block Reward	12.5 BTC

Hashes

Hash	00000000000000000000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc
Previous Block	000000000000000000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214
Next Block(s)	000000000000000000000000000000002cc08d842aa0156b466c300a7bd756448d22ec337d4692c
Merkle Root	87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

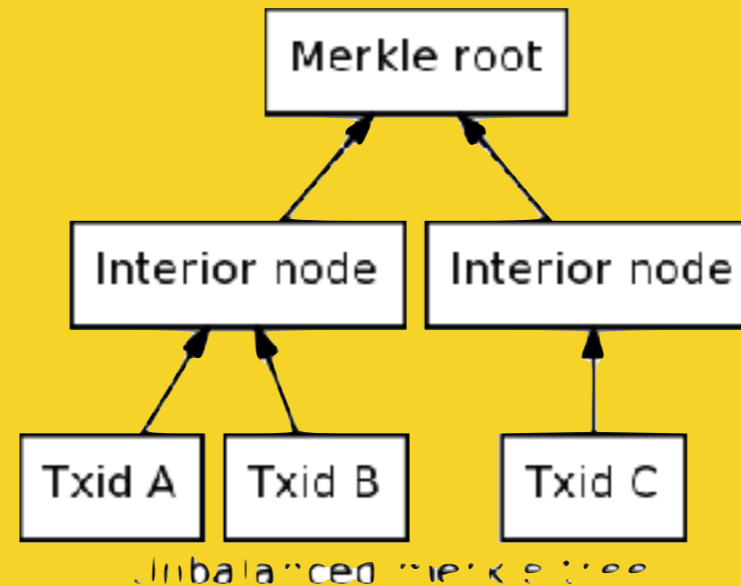
- 4 Version
- 32 previousBlockHash
- 32 MerkleRoot of Transactions
- 4 Time
- 4 Bits
- 4 Nonce



Each block is named by:

SHA256(SHA256(Vers || Prev || Merkle || Time || Bits || Nonce)

4 Version
 32 previousBlockHash
 32 MerkleRoot of Transactions
 4 Time
 4 Bits
 4 Nonce



Each block is named by:

$\text{SHA256}(\text{SHA256}(\text{Vers} \parallel \text{Prev} \parallel \text{Merkle} \parallel \text{Time} \parallel \text{Bits} \parallel \text{Nonce}))$

Only blocks with $\text{Name} < D_{\text{time}}$ are valid.

Block 443888

20000002

0000000000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03

402885509

777617094

Block 443888

20000002

0000000000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214

87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03

1482006543

0x5855A00F

402885509

0x18038B85

777617094

0x2E597EC6

Block 443888

20000002

000000000000000000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214
87f683e898a4f452b14392d90ec55d861b9b6cb20679cf6bb639eb8add2c8ac2

2016-12-17 20:29:03 1482006543 0x5855A00F

402885509 0x18038B85

777617094 0x2E597EC6

02000020

14c2a9b75c44c656d5720f694c32d97aa3354d2d926a8001000000000000000000
c28a2cdd8aeb39b66bcf7906b26c9b1b865dc50ed99243b152f4a498e883f687

0FA05558

858B0318

C67E592E

↓ sha256

99d1364a650f0f7e60803989d0d7bbca9be11c675d1271d075617668a8c8434f

↓ sha256

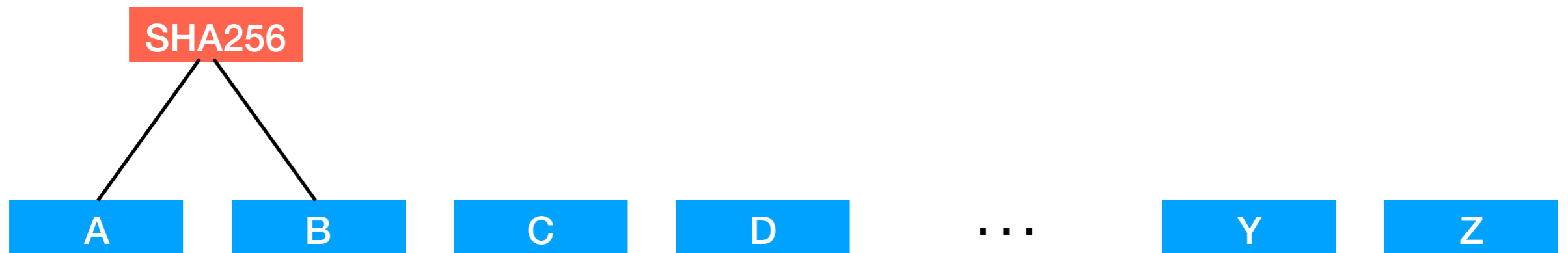
dc6411dcd03843070f92a84f4d4bb3d4c2339b2a0ddc0c0000000000000000000

00000000000000000000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc

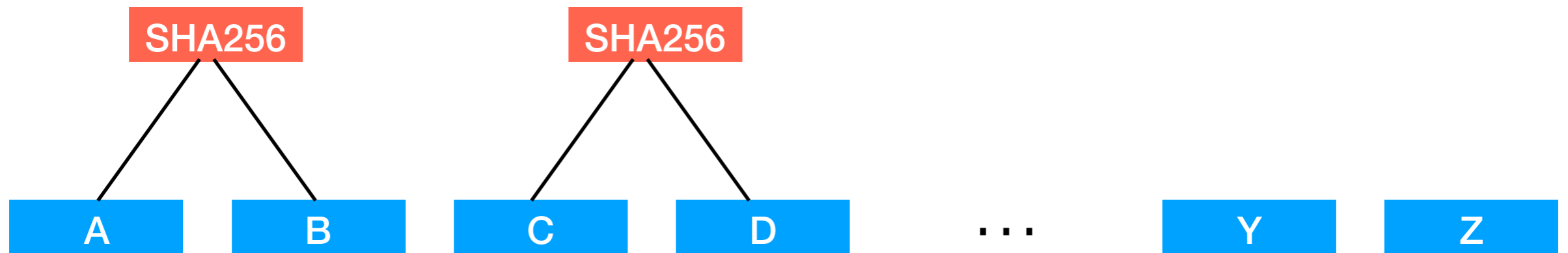
Merkle Tree



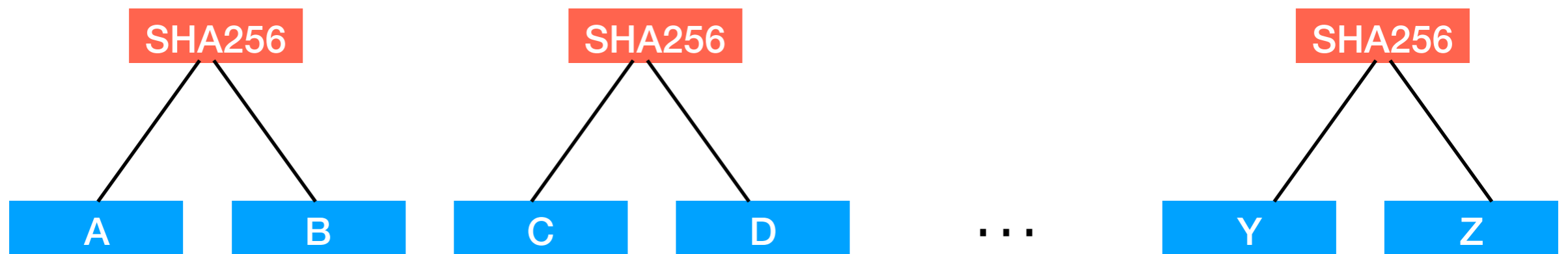
Merkle Tree



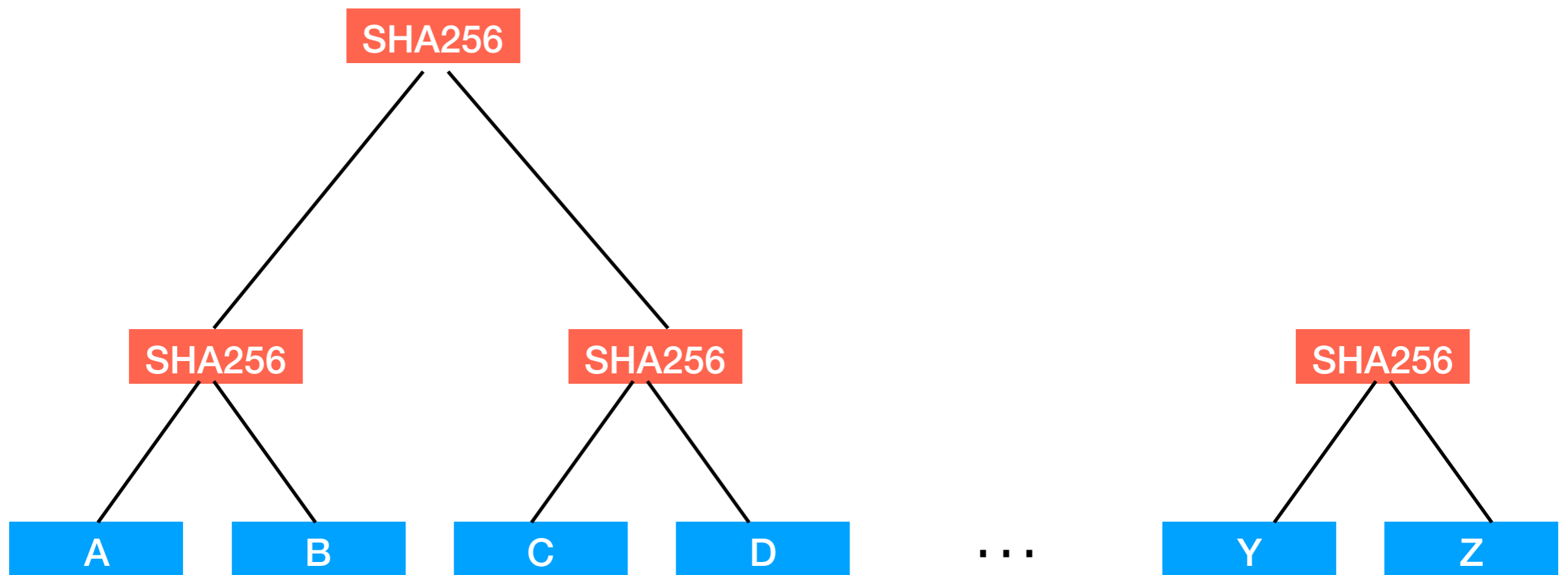
Merkle Tree



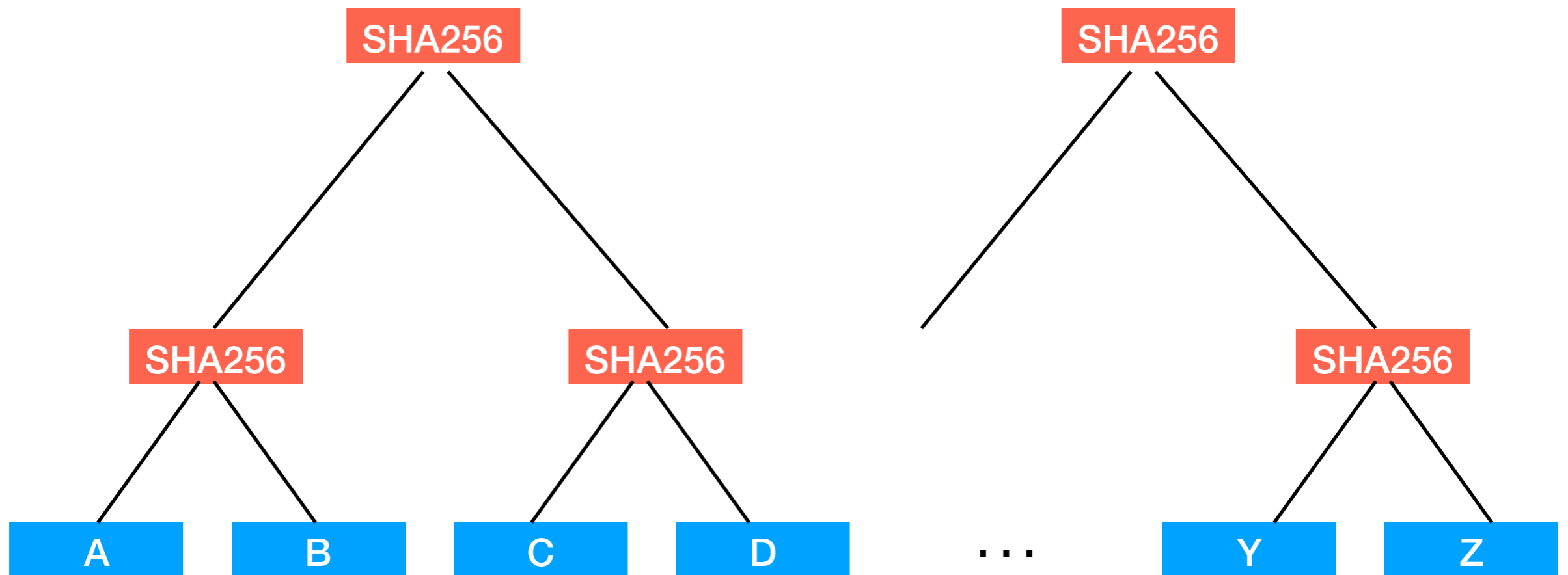
Merkle Tree



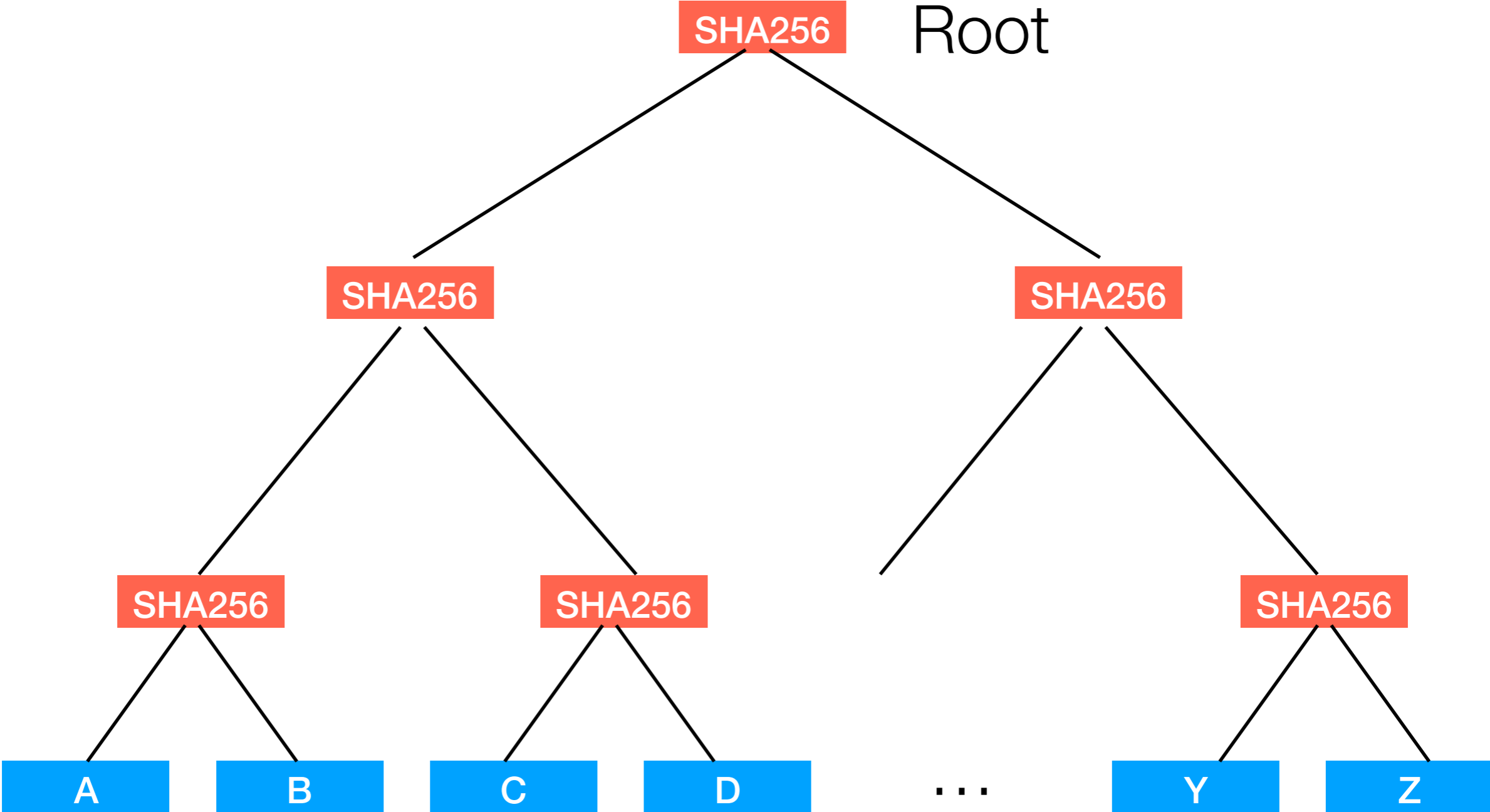
Merkle Tree



Merkle Tree



Merkle Tree



Bitcoin Block

4 Version
3 previousBlockHash
3 MerkleRoot of Transactions
4 Time
4 Bits
4 Nonce

of transactions

Tx1

Tx2

...

Txn

Transactions

List of Inputs

ref to previous output
signature script

List of Outputs

value
spending script

value
spending script

Transactions in a Bitcoin Block

Tx1

4 Version

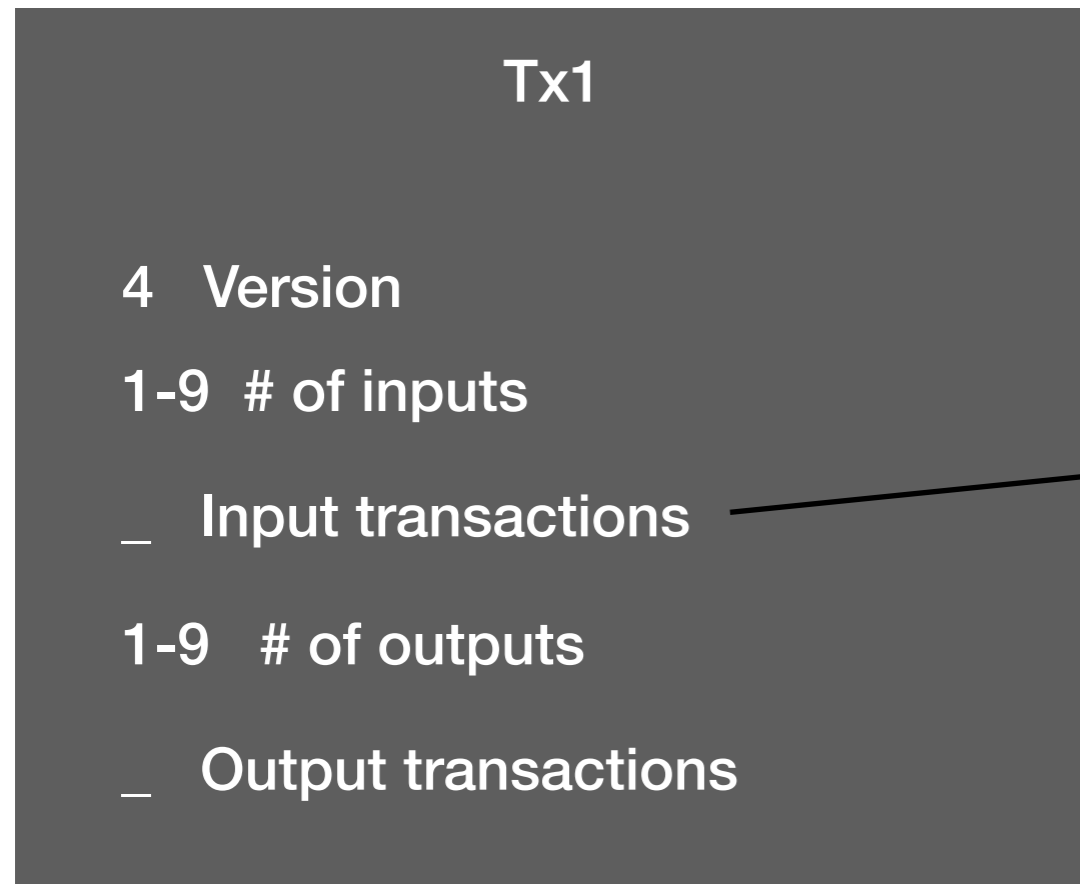
1-9 # of inputs

_ Input transactions

1-9 # of outputs

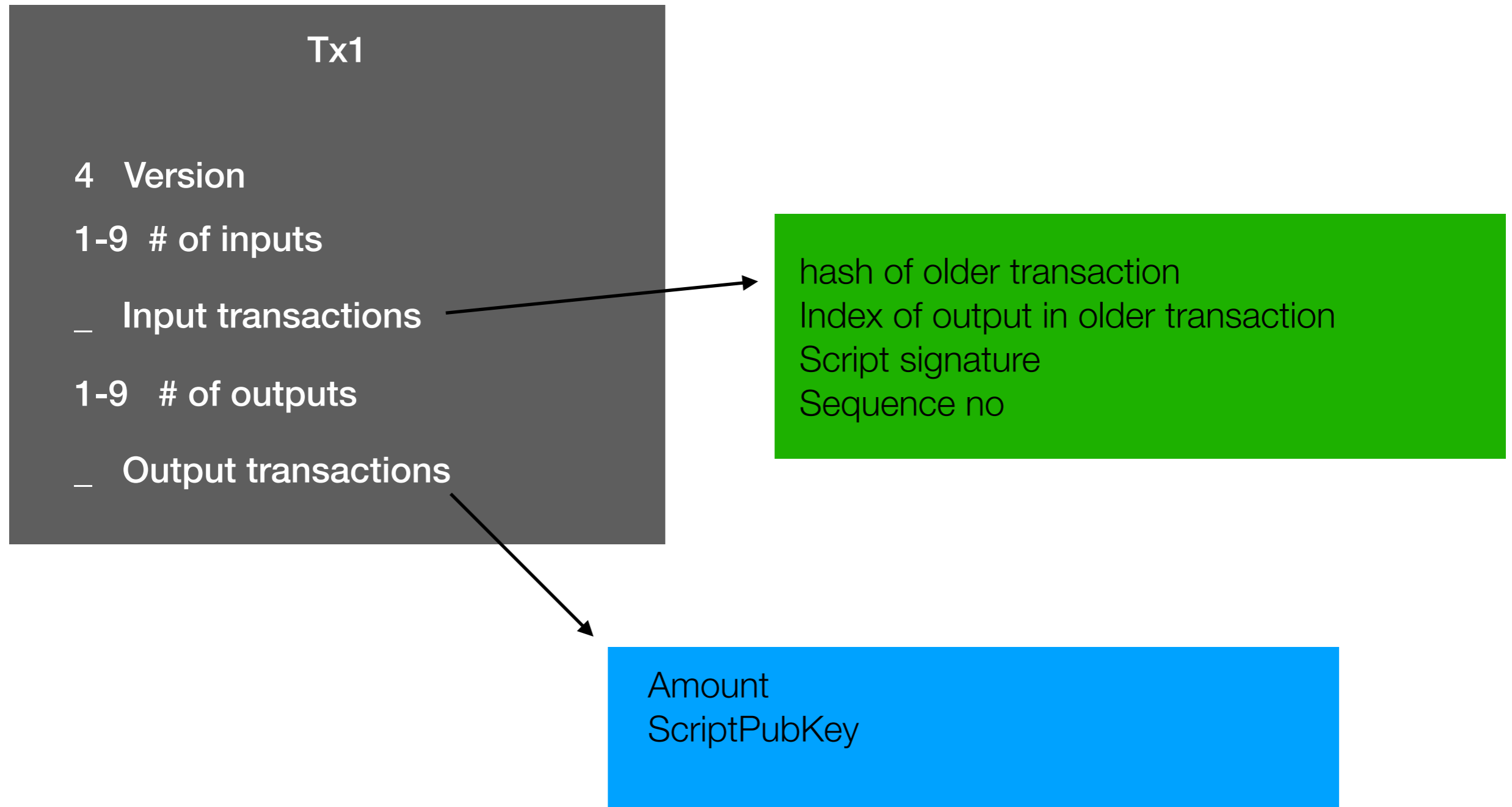
_ Output transactions

Transactions in a Bitcoin Block



hash of older transaction
Index of output in older transaction
Script signature
Sequence no

Transactions in a Bitcoin Block



How do we know if a
transaction is valid?

How do we know if a transaction is valid?

Sum(inputs) > Sum(outputs)

Inputs are not already spent

Inputs are “authorized”



Past tx in earlier blocks

New tx

“Spending witness for previous outputs of transactions”

“Ledger entries of new owners, and their policy on how to spend this coin.”

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
483045022100b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
483045022100b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver

Hash of input

```
01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
483045022100b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000
```

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver	Hash of input
<u>01000000</u> <u>01</u>	<u>0105f03ccf2cf648bd</u>
	<u>81865c608685600f8f16229608e0</u>
	<u>c05b56702943c53429</u> <u>01000000</u> 8b
	483045022100b232d83cc379df6f
	4d6b423871f2e3015085726a0313
	5bae0bcfce5dd44526ed02204081
	1b91eb053adfaa5a63d221da5ea7
	02efc92e98d08d6ca7bbefa1ab85
	7cce014104ef75b5750b34e5e845
	004e29af1e70ac0333095afa6eba
	e4eed9e5610f17b358578700492d
	16bf6fa379e962421f5c38812972
	399a8b3c27adc4532a7ea9957dff
	ffffff02807080b80d000000 <u>1976</u>
	<u>a9141f585f53479b0a2918895ebc</u>
	<u>41e09db4f171fe3888ac80e7c63f</u>
	00000000 <u>1976a9142d04eee9e30a</u>
	<u>e8b732bbf56f0dfa83d5d1af33d9</u>
	<u>88ac00000000</u>

Index of input

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver	Hash of input
<u>01000000</u> 01	<u>0105f03ccf2cf648bd</u>
	<u>81865c608685600f8f16229608e0</u>
	<u>c05b56702943c53429</u> 010000008b
	483045022100b232d83cc379df6f
	4d6b423871f2e3015085726a0313
	5bae0bcfce5dd44526ed02204081
	1b91eb053adfaa5a63d221da5ea7
	02efc92e98d08d6ca7bbefa1ab85
	7cce014104ef75b5750b34e5e845
	004e29af1e70ac0333095afa6eba
	e4eed9e5610f17b358578700492d
	16bf6fa379e962421f5c38812972
	399a8b3c27adc4532a7ea9957dff
	ffffff02807080b80d0000001976
	<u>a9141f585f53479b0a2918895ebc</u>
	<u>41e09db4f171fe3888ac80e7c63f</u>
	00000000 <u>1976a9142d04eee9e30a</u>
	<u>e8b732bbf56f0dfa83d5d1af33d9</u>
	88ac00000000

Index of input

Length

scriptsig

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver	Hash of input
<u>01000000</u> 01	<u>0105f03ccf2cf648bd</u>
	<u>81865c608685600f8f16229608e0</u>
	<u>c05b56702943c53429</u> 010000008b
	483045022100b232d83cc379df6f
	4d6b423871f2e3015085726a0313
	5bae0bcfce5dd44526ed02204081
	1b91eb053adfaa5a63d221da5ea7
	02efc92e98d08d6ca7bbefa1ab85
	7cce014104ef75b5750b34e5e845
	004e29af1e70ac0333095afa6eba
	e4eed9e5610f17b358578700492d
	16bf6fa379e962421f5c38812972
	399a8b3c27adc4532a7ea9957dff
	ffffff02807080b80d0000001976
	<u>a9141f585f53479b0a2918895ebc</u>
	<u>41e09db4f171fe3888ac80e7c63f</u>
	<u>000000001976a9142d04eee9e30a</u>
	<u>e8b732bbf56f0dfa83d5d1af33d9</u>
	88ac00000000

Index of input

Length

scriptsig

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver	Hash of input
0100000001	0105f03ccf2cf648bd
81865c608685600f8f16229608e0	
c05b56702943c53429	010000008b
483045022100b232d83cc379df6f	
4d6b423871f2e3015085726a0313	
5bae0bcfce5dd44526ed02204081	
1b91eb053adfaa5a63d221da5ea7	
02efc92e98d08d6ca7bbefa1ab85	
7cce014104ef75b5750b34e5e845	
004e29af1e70ac0333095afa6eba	
e4eed9e5610f17b358578700492d	
16bf6fa379e962421f5c38812972	
399a8b3c27adc4532a7ea9957dff	
ffffff02	807080b80d0000001976
a9141f585f53479b0a2918895ebc	
41e09db4f171fe3888ac	80e7c63f
00000000	1976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9	
88ac	00000000

Index of input

Length

scriptsig

1st out

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver	Hash of input		
01000000	010105f03ccf2cf648bd	Index of input	
81865c608685600f8f16229608e0			
c05b56702943c53429	010000008b		
483045022100b232d83cc379df6f		Length	
4d6b423871f2e3015085726a0313			
5bae0bcfce5dd44526ed02204081		scriptsig	
1b91eb053adfaa5a63d221da5ea7			
02efc92e98d08d6ca7bbefa1ab85			
7cce014104ef75b5750b34e5e845			
004e29af1e70ac0333095afa6eba			
e4eed9e5610f17b358578700492d			
16bf6fa379e962421f5c38812972			
399a8b3c27adc4532a7ea9957dff			
ffffff02	807080b80d0000001976		1st out
a9141f585f53479b0a2918895ebc			
41e09db4f171fe3888ac	80e7c63f	2nd out	
00000000	1976a9142d04eee9e30a		
e8b732bbf56f0dfa83d5d1af33d9			
88ac	00000000		

Example Input Transaction

Tx

4 Version

1-9 # of inputs

_ Input

1-9 # of outputs

_ Output

Recall an input is:

hash of older transaction

Index of output in older transaction

Script signature

Sequence no

Ver	Hash of input		
01000000	010105f03ccf2cf648bd	Index of input	
81865c608685600f8f16229608e0			
c05b56702943c53429	010000008b		
483045022100b232d83cc379df6f		Length	
4d6b423871f2e3015085726a0313			
5bae0bcfce5dd44526ed02204081		scriptsig	
1b91eb053adfaa5a63d221da5ea7			
02efc92e98d08d6ca7bbefa1ab85			
7cce014104ef75b5750b34e5e845			
004e29af1e70ac0333095afa6eba			
e4eed9e5610f17b358578700492d			
16bf6fa379e962421f5c38812972			
399a8b3c27adc4532a7ea9957dff			
ffffff02	807080b80d0000001976		1st out
a9141f585f53479b0a2918895ebc			
41e09db4f171fe3888ac	80e7c63f	2nd out	
00000000	1976a9142d04eee9e30a		
e8b732bbf56f0dfa83d5d1af33d9			
88ac	00000000	locktime	

value
spending script

ref to prev output
signature script

Spending Script

A program, P , that when executed after executing the signature script, returns “Valid”

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG



Duplicate
top value
on the
stack

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG



Duplicate
top value
on the
stack



Hash top
value on
stack

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG



Duplicate
top value
on the
stack



Hash top
value on
stack



push this
constant
onto stack

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG



Duplicate
top value
on the
stack



Hash top
value on
stack



push this
constant
onto stack



check
equality of
top two
stack
values

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG



Duplicate
top value
on the
stack



Hash top
value on
stack



push this
constant
onto stack



check
equality of
top two
stack
values



check
whether
next two
values are
pk,sig for
the tx

The diagram illustrates a transaction structure. It consists of two main gray rectangular blocks. The left block contains a blue box with the text 'value' and 'dup hash160 [h(pk)] eqverify checksig'. The right block contains a green box with the text 'ref to prev output' and '<pk> <signature>'. A black arrow points from the green box to the blue box. To the right of the green box, a portion of another blue box is visible, containing the letters 'V' and 's'.

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

Spending Script

A program, P , that when executed after executing the signature script, returns “Valid”

01000000010105f03ccf2cf648bd
81865c608685600f8f16229608e0
c05b56702943c53429010000008b
483045022100b232d83cc379df6f
4d6b423871f2e3015085726a0313
5bae0bcfce5dd44526ed02204081
1b91eb053adfaa5a63d221da5ea7
02efc92e98d08d6ca7bbefa1ab85
7cce014104ef75b5750b34e5e845
004e29af1e70ac0333095afa6eba
e4eed9e5610f17b358578700492d
16bf6fa379e962421f5c38812972
399a8b3c27adc4532a7ea9957dff
ffffffff02807080b80d0000001976
a9141f585f53479b0a2918895ebc
41e09db4f171fe3888ac80e7c63f
000000001976a9142d04eee9e30a
e8b732bbf56f0dfa83d5d1af33d9
88ac00000000

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

483045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc3435022100c6
cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d0148044ded81d4fb1601da
e9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73883328d9965c5cd17dceb93212
e193add48d4895dea0f35c1eccba

Then run this program

dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```


value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502  
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
```

```
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73  
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

044ded81d4fb1...ecccba
3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502  
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01  
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73  
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

044ded81d4fb1...ecccba

044ded81d4fb1...ecccba

3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502  
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
```

```
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73  
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

1f585f53479b0a2918895ebc41e09db4f171fe38

044ded81d4fb1...ecccba

3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502  
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
```

```
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73  
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

1f585f53479b0a2918895ebc41e09db4f171fe38

1f585f53479b0a2918895ebc41e09db4f171fe38

044ded81d4fb1...ecccba

3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

1f585f53479b0a2918895ebc41e09db4f171fe38

1f585f53479b0a2918895ebc41e09db4f171fe38

044ded81d4fb1...ecccba

3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

044ded81d4fb1...ecccba

3045022058582...c07d01

value

dup hash160 [h(pk)] eqverify checksig

ref to prev output

<pk> <signature>

First run this program

```
PUSH3045022058582c05485b1274f3b9e11f68dda5535d93e24667d48ad247ae8a75b3fc343502
2100c6cb8028e20882af2870ff5f12cf33483c3c6193168e785cbcf74bb197e9c07d01
PUSH044ded81d4fb1601dae9b57df4a0988cc9b4a9df5dae0f0c6e17d2196b424a6d50fbd80e73
883328d9965c5cd17dceb93212e193addd48d4895dea0f35c1ecccba
```

Then run this program

```
dup hash160 PUSH1f585f53479b0a2918895ebc41e09db4f171fe38 eqverify checksig
```

044ded81d4fb1...ecccba

3045022058582...c07d01

OK

Standard spending script

DUP HASH160 [H(PK)] EQVERIFY CHECKSIG



Duplicate
top value
on the
stack



Hash top
value on
stack



push this
constant
onto stack



check
equality of
top two
stack
values



check
whether
next two
values are
pk,sig for
the tx

```
"vout_sz": 2,  
"confirmations": 9,  
"confidence": 1,  
"inputs": [  
  {  
    "prev_hash":  
"f7f380ed4cc8f54982cc2cc04cb372558e62770c5b9bff575161f637bd3ad183",  
    "output_index": 1,  
    "script":  
"4830450221009f7768bf1d2322b757d37384377410f30a5e19d0f6e810d8aae8f4700  
f82fd6f0220111ff9684afc84f160a4842cf113487098e84ccab92e3740317b3575f6152  
b070121023a24f09e3b1c840946748d6da88e9aa687b9c08e547664c3ec16c0eab3f  
505fc",  
    "output_value": 33311400,  
    "sequence": 4294967295,  
    "addresses": [ "1PxTVHpG3JagK3oogWeLhUNFYVfgkRLP2b"],  
  }  
],  
"outputs": [  
  {  
    "value": 32000000, DUP HASH160 c29e48f3c4745986acc9c9c30c23d15f939d842e EQ CHECK  
    "script": "76a914c29e48f3c4745986acc9c9c30c23d15f939d842e88ac",  
    "addresses": [  
      "1Jk3i3m78bkNMKKyVBmVb1tLvnaQJ8kJCT"  
    ],  
  },  
  {  
    "value": 311400,  
    "script": "76a914fbcfc189b757194aa237130b0deb09698040c6fa88ac",  
    "addresses": [  

```

Bitcoin address

1Jk3i3m78bkNMKKyVBmVb1tLvnaQJ8kJCT

a redundant “base-58” encoding of (a hash of) your public key:

DUP HASH160 **c29e48f3c4745986acc9c9c30c23d15f939d842e** EQ CHECKSIG

1. $A = \text{Ripemd160}(\text{SHA256}(pk))$

2. Compute $\text{SHA256}(\text{SHA256}(00A))$

c46f8f04db15c58a03027e23528c141c3df329db3cca1339f2a8c6fea790350f

3. Copy first 4 bytes to end

c29e48f3c4745986acc9c9c30c23d15f939d842e c46f8f04

4. Base-58 encode

1Jk3i3m78bkNMKKyVBmVb1tLvnaQJ8kJCT

How to spend

1. Form a valid transaction tx using address
2. Broadcast your tx to the bitcoin network
3. Wait for a miner to include it in a block

How to mine

1. Listen for new {blocks, txs}
2. Organize *valid* txs into a new pre-block
3. Hash pre-block, while changing nonce/
time/txs in pre-block in order to find a
valid block
4. Broadcast new valid blocks to peers.

L7

abhi shelat
17f-money

Name:

What is a blockchain:

What is a bitcoin transaction: