DIALOGUE WITH THE FED

Beyond Today's Financial Headlines

Blockchain, Cryptocurrencies and Central Banks

David Andolfatto
Vice President, Research
Federal Reserve Bank of St. Louis

August 29, 2018

The views expressed here are those of the speakers and do not necessarily represent the views of the Federal Reserve Bank of St. Louis or of the Federal Reserve System.

FEDERAL RESERVE BANK of ST. LOUIS

CENTRAL TO AMERICA'S ECONOMY®

Outline

- Blockchain + Cryptocurrencies + Central Banks
  - Common Theme: Database Management
- Demystifying Blockchain (communal recordkeeping)
  - Why the blockchain should be familiar to you
  - Primitive blockchains in moneyless societies
- Delegated vs. Communal Recordkeeping Systems
  - A case for central bank digital currency (delegated)
  - A case for cryptocurrencies (communal)
- Summary and Conclusion

Blockchain + Cryptocurrencies + Central Banks

Common Theme: Database Management

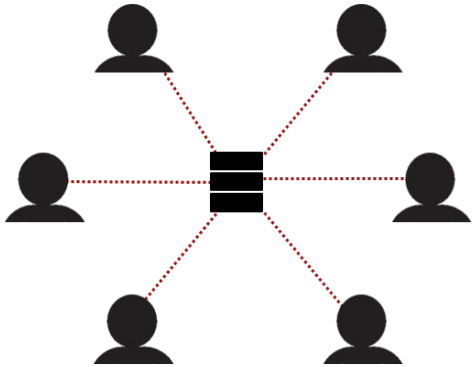
- Information relating to credit/work histories, consumer reports, buy/sell records, service records, diplomas, licenses, etc.
  - Valued in a society where honesty and trust are lacking.
  - Reputation/status constitutes a form of currency
    - reputation loss is a form of communal punishment
    - this incentivizes good behavior.
- Problem: obvious incentive to counterfeit histories (“evil”).
- Wanted: an honest, secure, easily-accessible, low-cost database of individual behavioral histories.
- Objective: eliminate discordant records, auditing costs, legal disputes; promote fair and efficient outcomes

Key Question

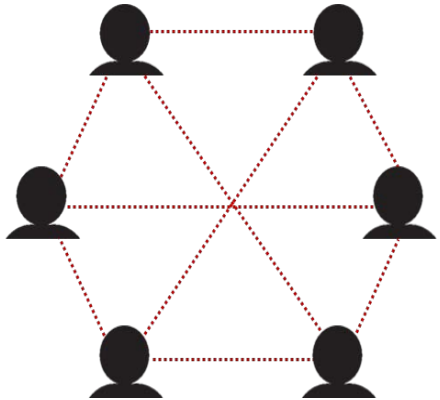
- How are members of a community wanting to share and manage a database to do so when they do not fully trust each other (owing to aforementioned evil)?

Key Question (cont.)

- Two basic approaches to the problem:
  1. Delegate recordkeeping to 3rd party, a central authority; trust (but audit) → central database.
  2. Recordkeeping a communal effort; all eyes on each other → distributed database.



Centralized Server

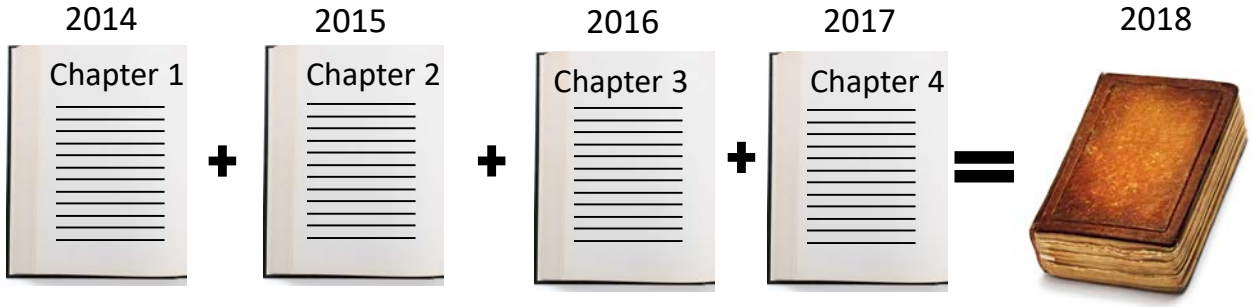


Decentralized Network

Demystifying Blockchain

Demystifying Blockchain

- Consider a history textbook published in 2016 about events that happened in 2014 (Chapter 1) and 2015 (Chapter 2).

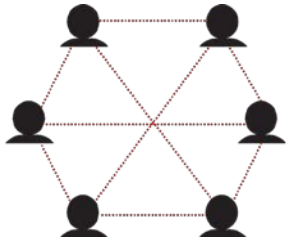


- History as time-stamped blocks of information (chapters) in an ever-expanding history textbook (blockchain).
- Who gets to read this history?
- Who gets to write it?

Thinkstock / Devonyu, Thinkstock / Vladimirs

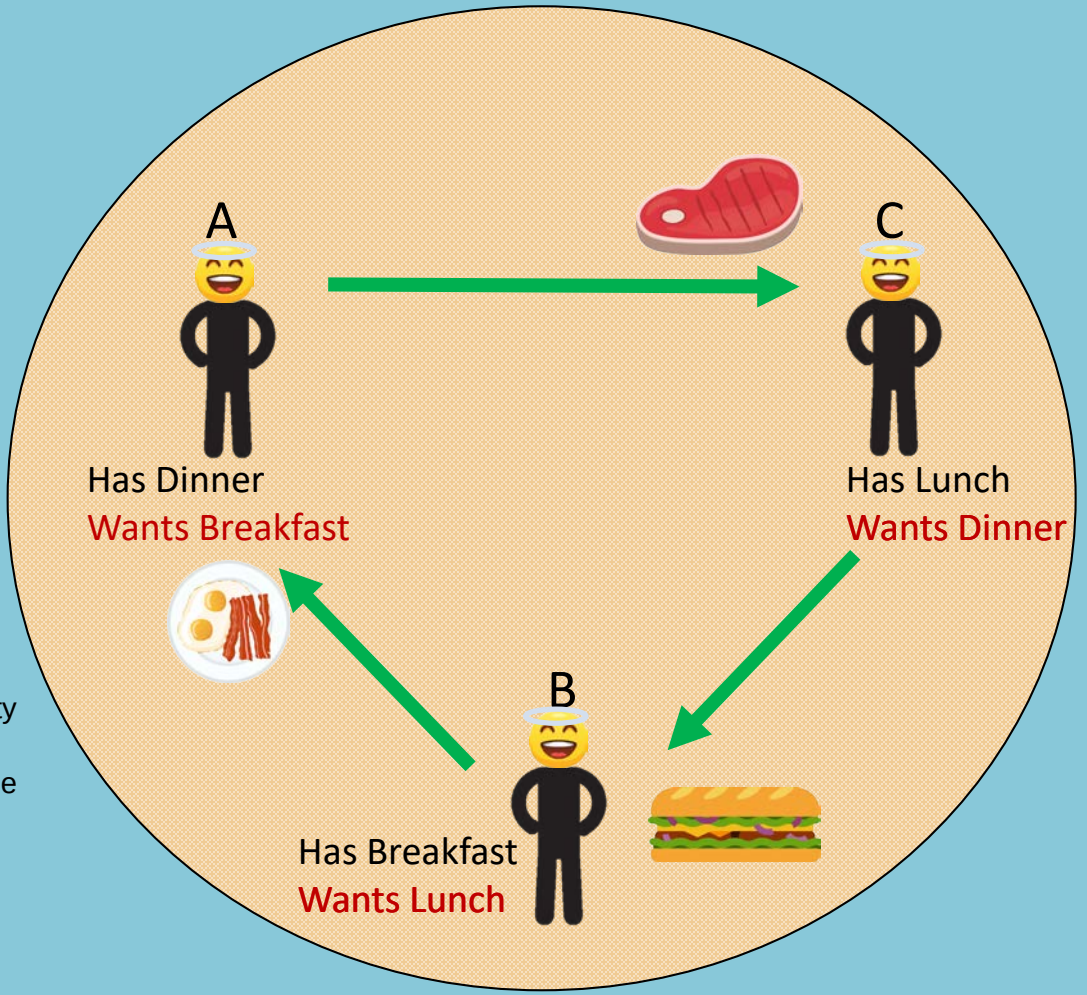
Primitive Blockchains in Moneyless Societies

- Small, close-knit communities (friends, family, neighbors, hunter-gatherer societies) do not use money/barter.
- How is economic cooperation sustained when some/most/all people are inherently noncooperative?
- Through a virtual database of individual behavioral histories (living in a network of brains) updated via communal consensus mechanism (gossip).
  - Sounds like a blockchain!



A World Free of Evil

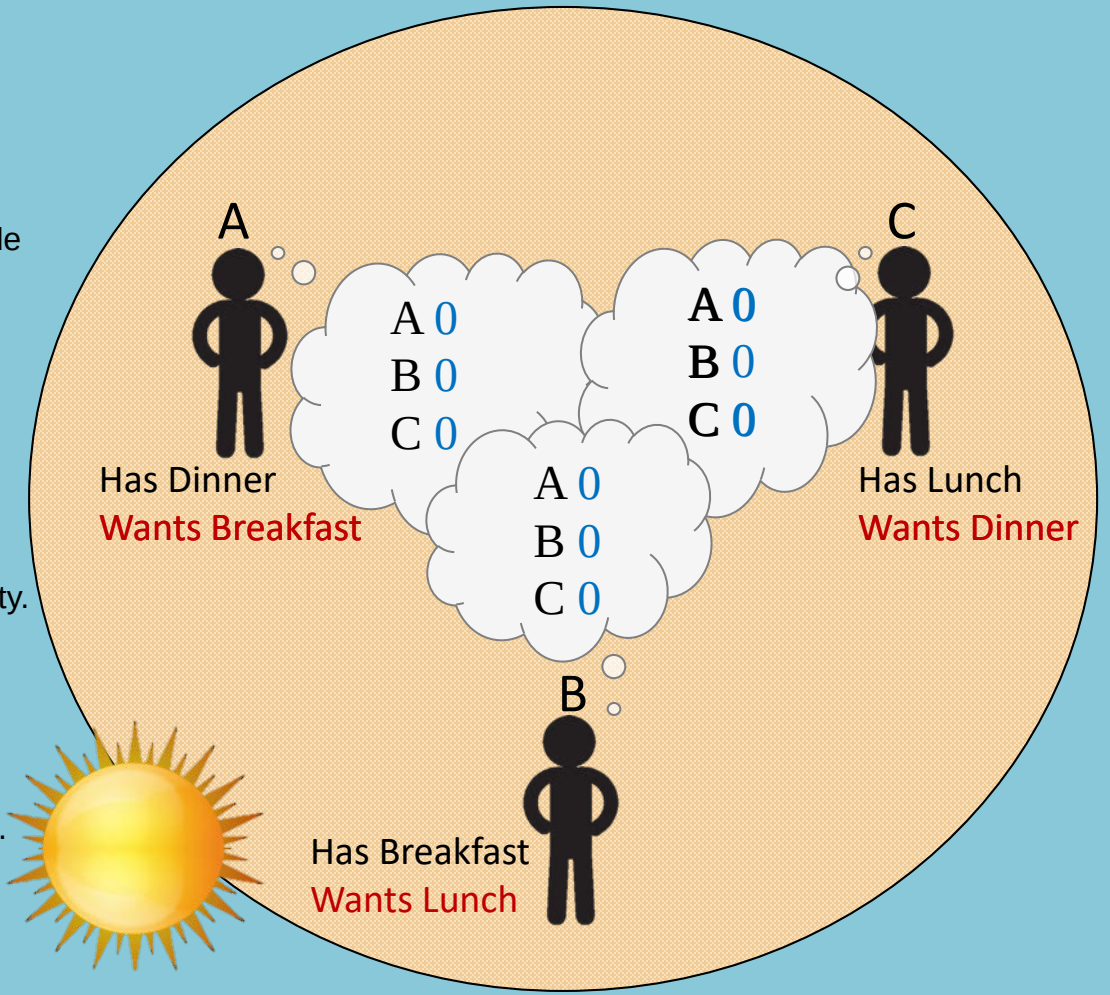
- Imagine a world free of evil.
  - Everyone is trustworthy, honest.
- Three people live on a small island:
  - Adam (A) specializes in producing dinner, but prefers to eat breakfast.
  - Betty (B) specializes in producing breakfast, but prefers to eat lunch.
  - Charlie (C) specializes in producing lunch, but prefers to eat dinner.
  - Each person knows each other's preferences.
- Multilateral trade takes place.
  - Morning: Betty makes breakfast and gives it to Adam because it's the right thing to do.
  - Afternoon: Charlie makes lunch and gives it to Betty because it's the right thing to do.
  - Evening: Adam makes dinner and gives it to Charlie because it's the right thing to do.
- End of the day: everyone eats their favorite meal and is happy.



Thinkstock / lefym Turkin

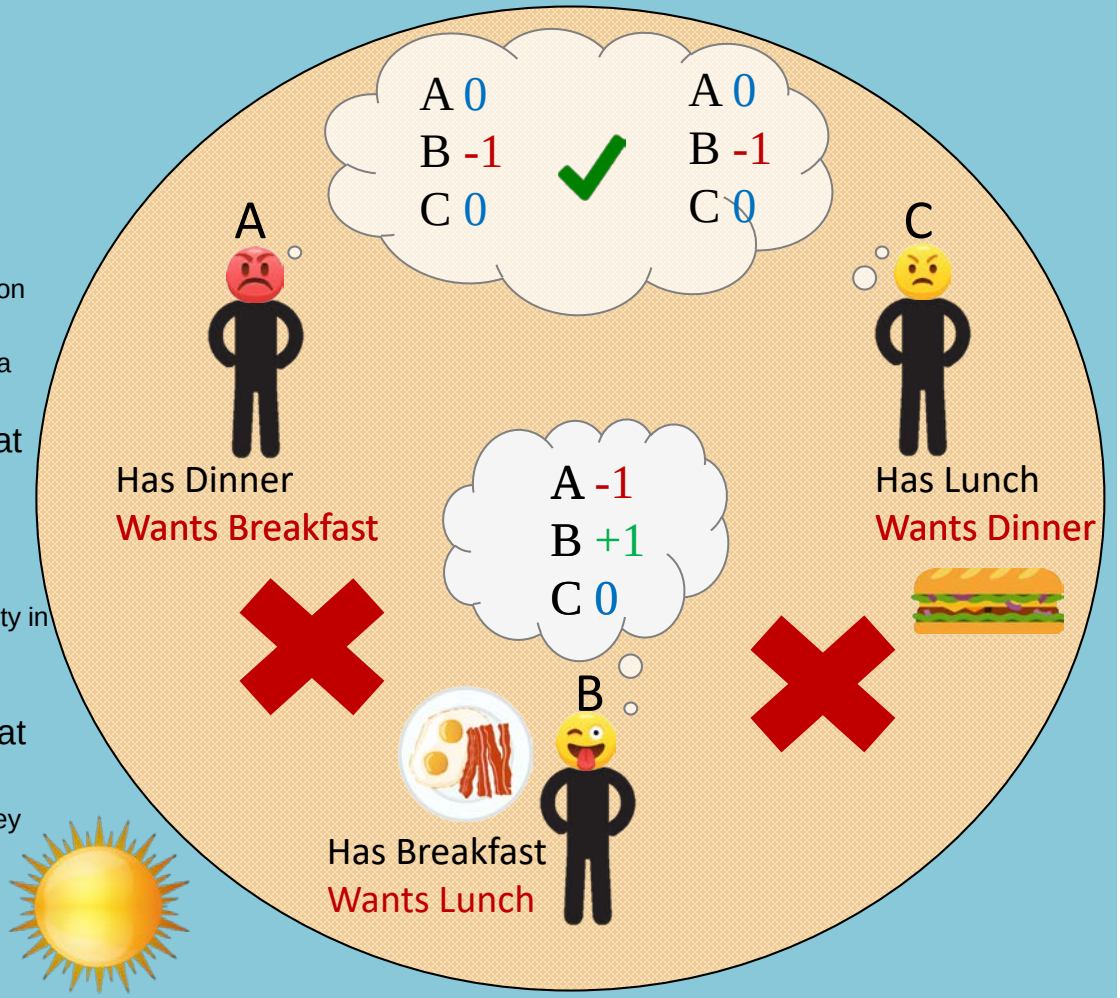
Primitive Blockchain

- In reality, people aren't trustworthy.
  - In this example, the *right* thing to do is to trade meals so that everyone gets their favorite.
  - Any one of them can choose **not** do the right thing, though.
- Knowing that their peers aren't trustworthy, each person keeps score.
  - One earns points by giving to the community, and loses points by taking from the community.
- This is a primitive blockchain.
  - There is no central authority keeping track of everyone's actions.
  - Every member of the community keeps track.
  - It's a decentralized network of people.



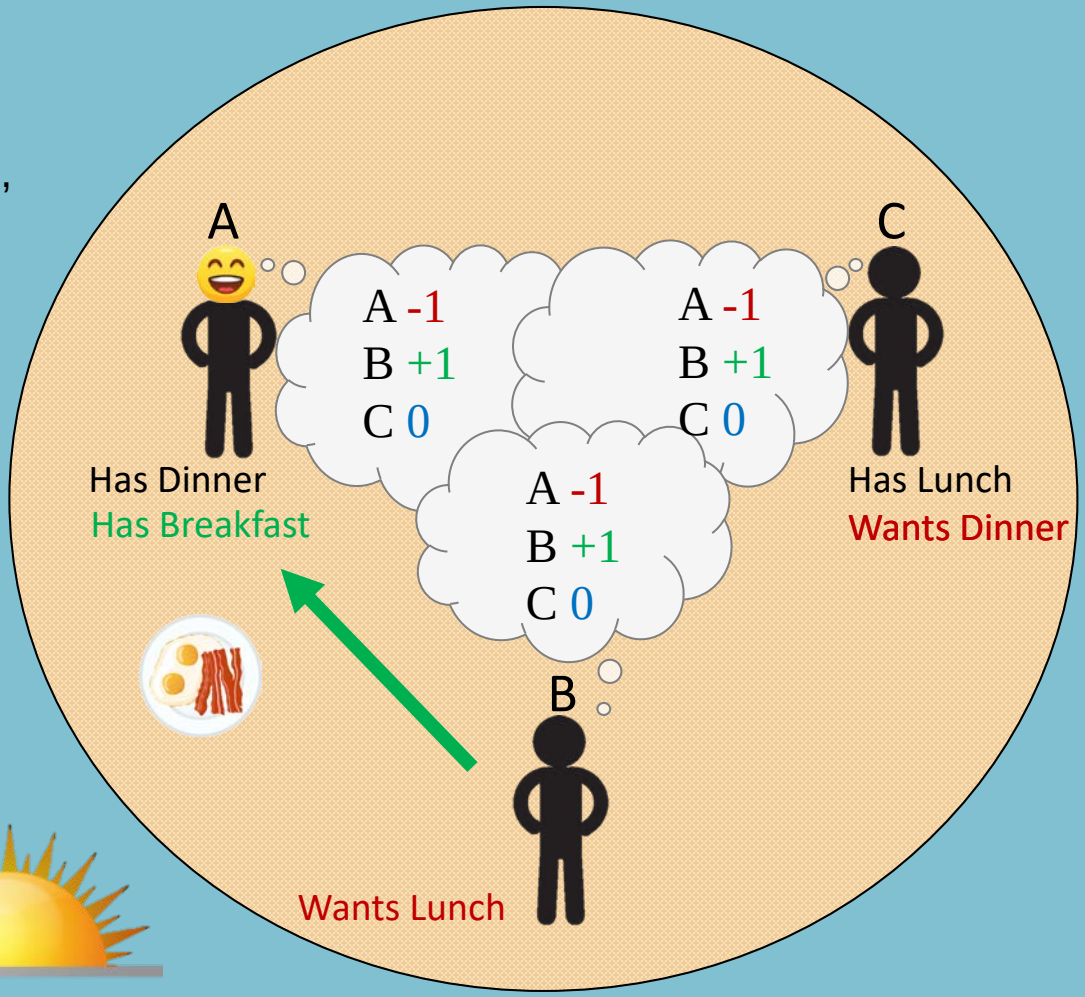
Primitive Blockchain

- This scorekeeping leads to cooperation.
- In the morning, Betty decides to eat breakfast instead of giving it to Adam.
  - Adam and Charlie both see this and dock her a point on their scorecards for selfishness.
  - Betty lies and gives herself a point while taking away a point from Adam.
- Adam and Charlie talk to each other about what happens.
  - They reach a consensus that Betty did not cooperate.
  - Betty's lies can't fool such a small community
  - As a consequence, Charlie does not give lunch to Betty in the afternoon.
- Betty ends up consuming breakfast instead of lunch, which is bad for her, as she prefers to eat lunch.
  - Everyone is thus encouraged to cooperate, or else they deprive themselves of their favorite meal.



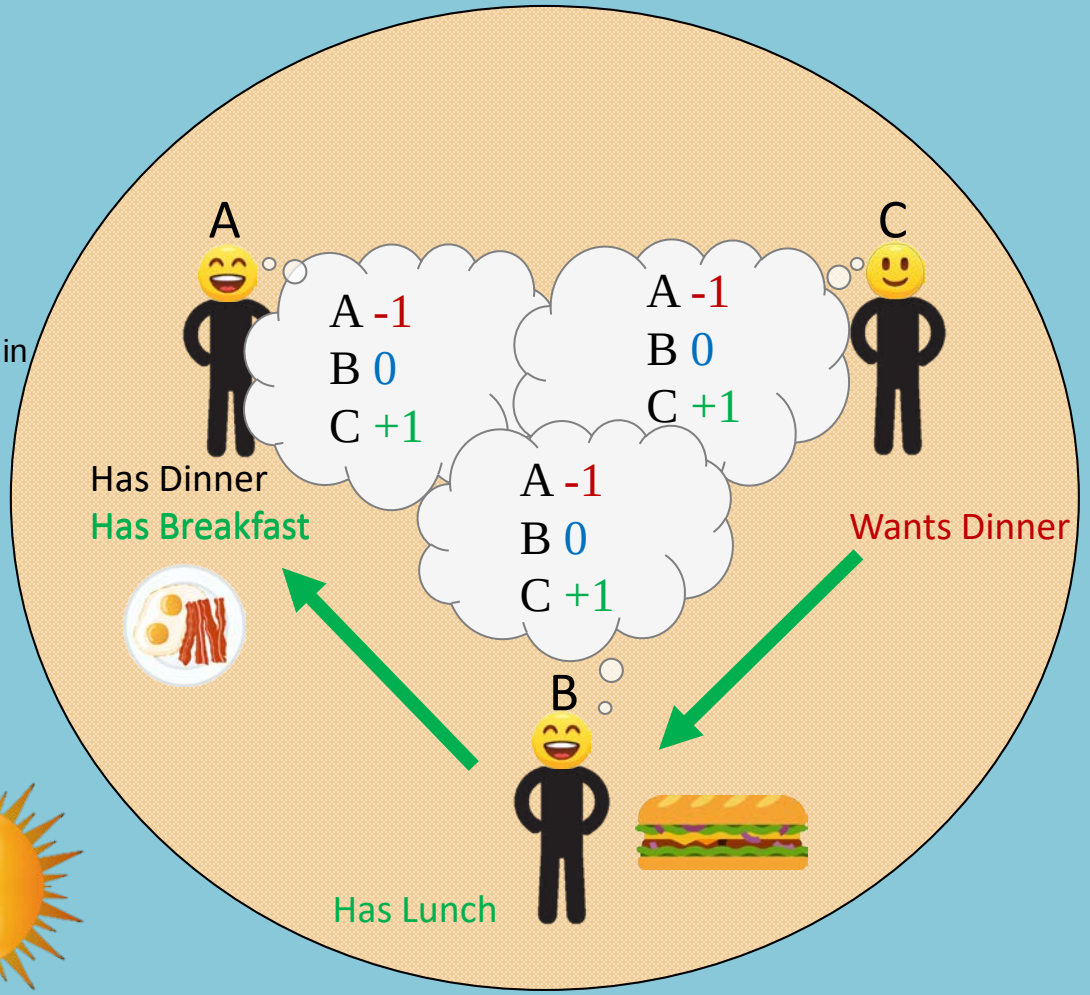
Primitive Blockchain

- Because Betty would rather have lunch, she cooperates.
  - She gives breakfast to Adam.
- Everyone sees Betty's actions and adjusts points accordingly.
  - Betty gets a point for giving, while Adam loses a point for taking.



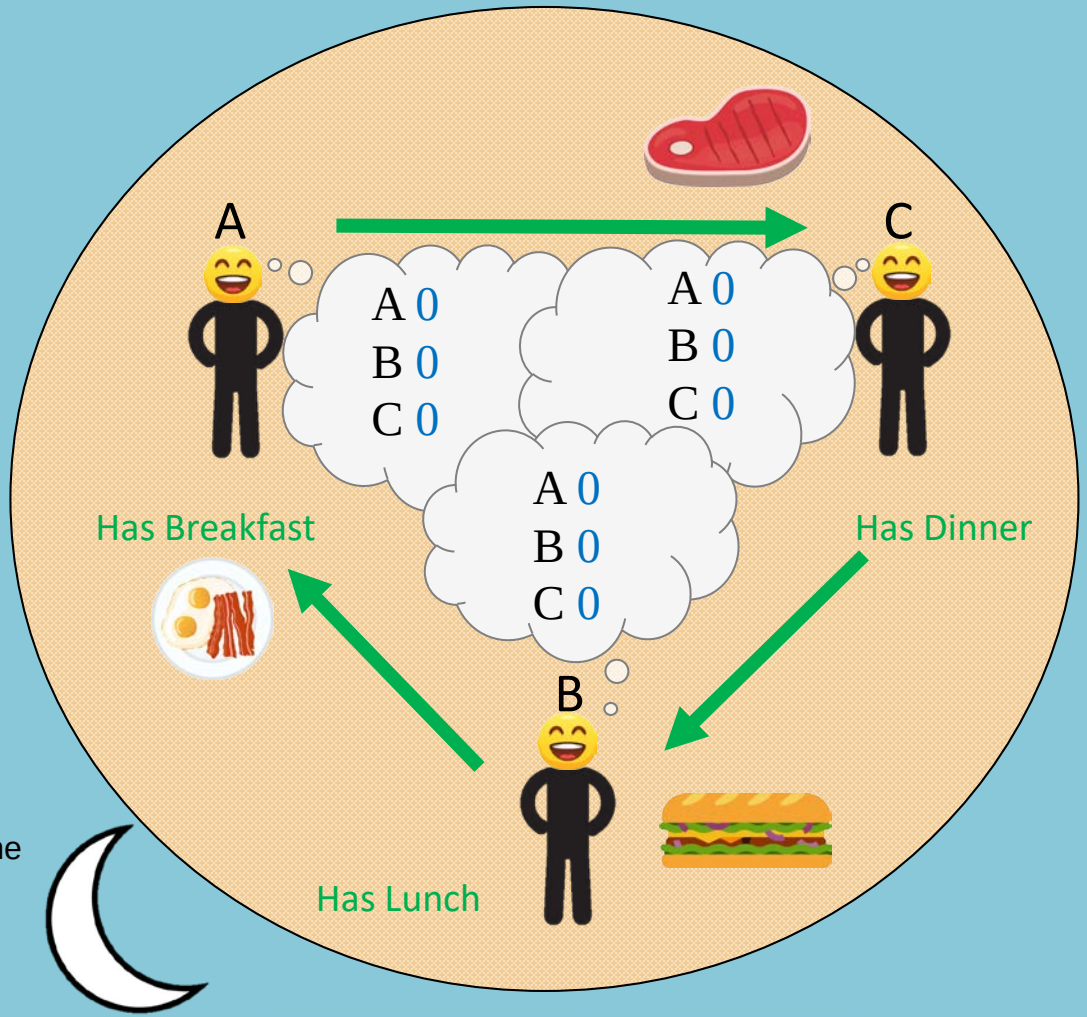
Primitive Blockchain

- Because Betty cooperated in the morning, Charlie gives her lunch in the afternoon.
  - In effect, Betty “spends” the point she earned in the morning to get lunch.
- Everyone sees the trade and adjusts points accordingly.
  - Charlie gets a point for giving, while Betty loses a point for taking.



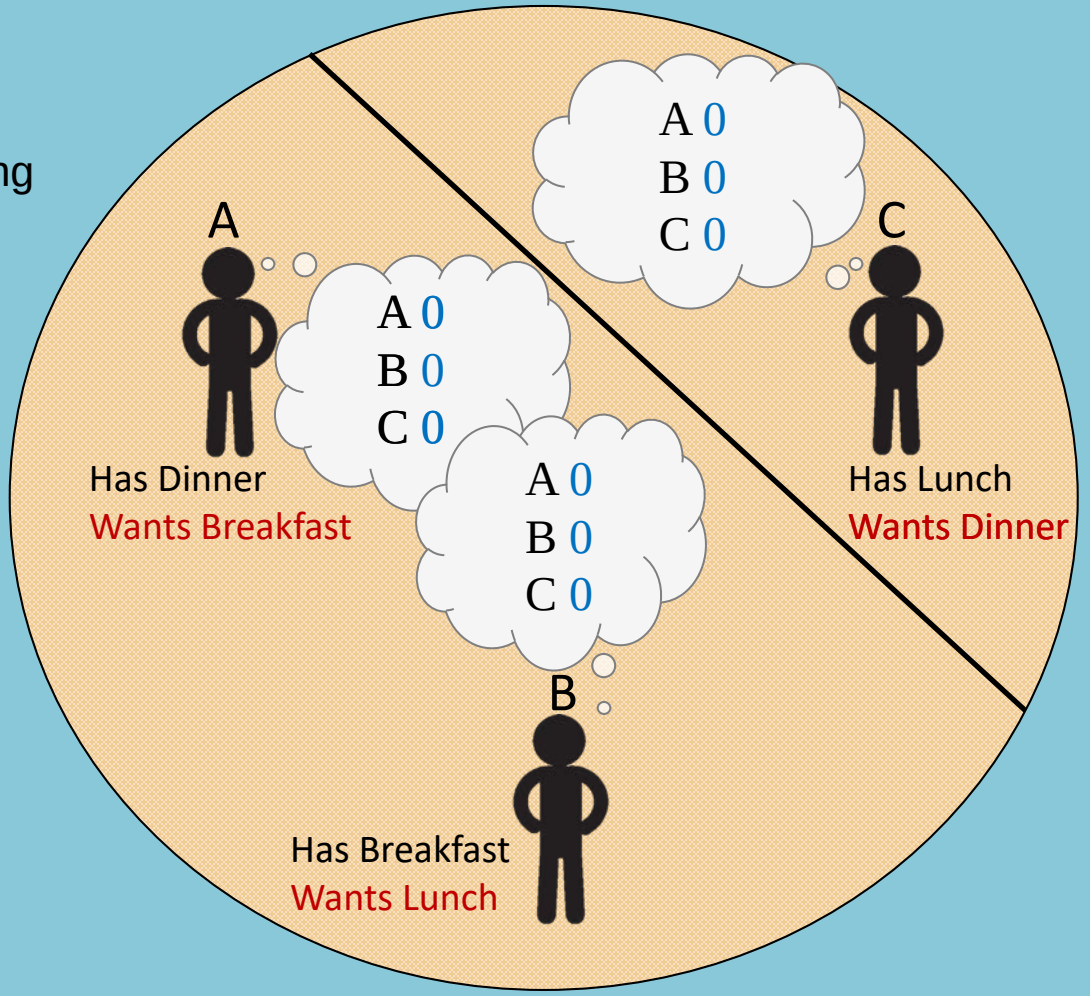
Primitive Blockchain

- Finally, in the evening, Adam gives Charlie dinner.
  - Adam owed the community after consuming breakfast, and Charlie “spends” the point he earned at lunch.
- Everyone sees the trade and adjusts points accordingly.
  - Adam gets a point for giving, while Charlie loses a point for taking.
  - This moves every score back to zero.
- End of the day: Everyone eats their favorite meal and is happy.
- This is the blockchain at work.
  - Decentralized recordkeeping by everyone in the community leads to cooperation.



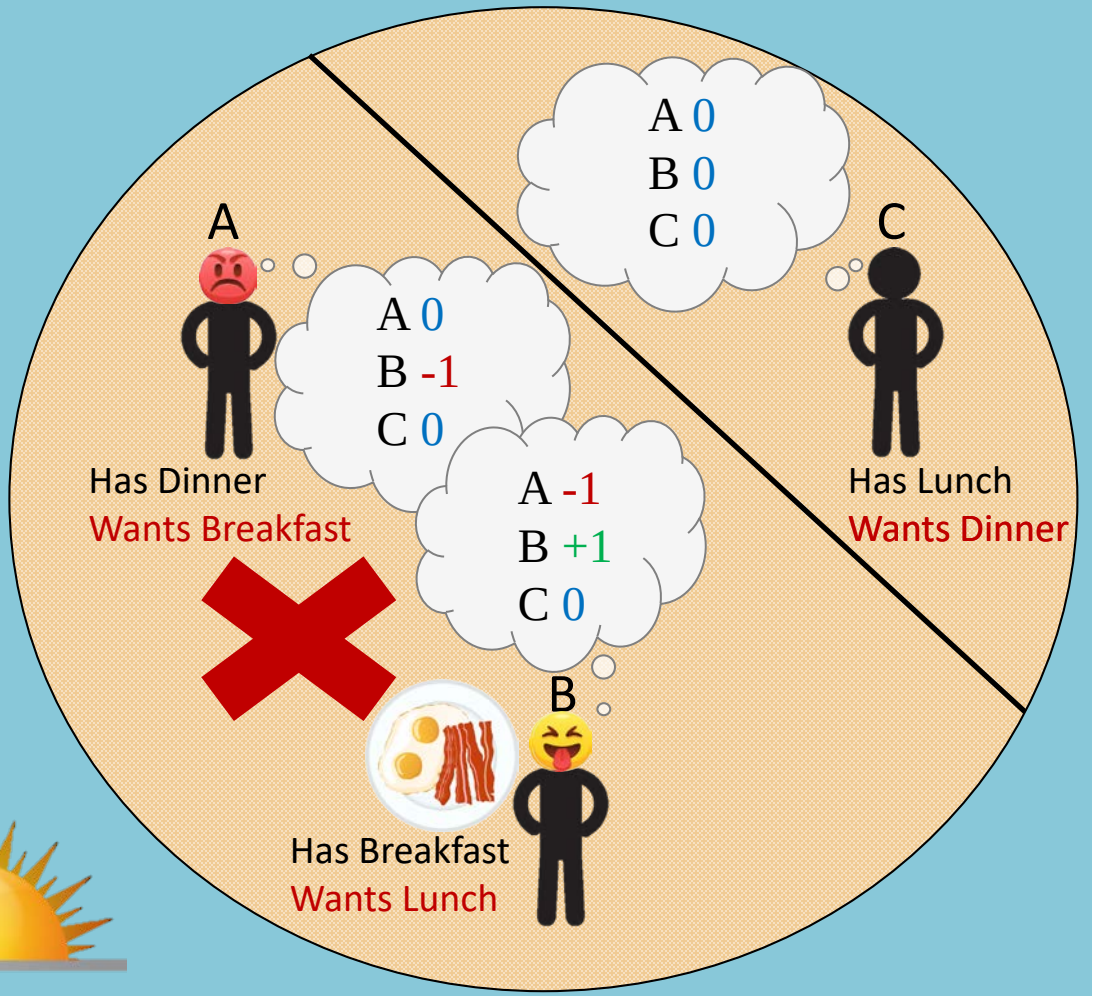
Primitive Blockchain (Limitation)

- What if not everyone can see everything that happens?
  - Imagine that Charlie spends the morning off producing lunch, so he can't see the others.
- This happens in large communities.
- When not everyone can keep track of everybody's history of actions, this primitive blockchain does *not* work.



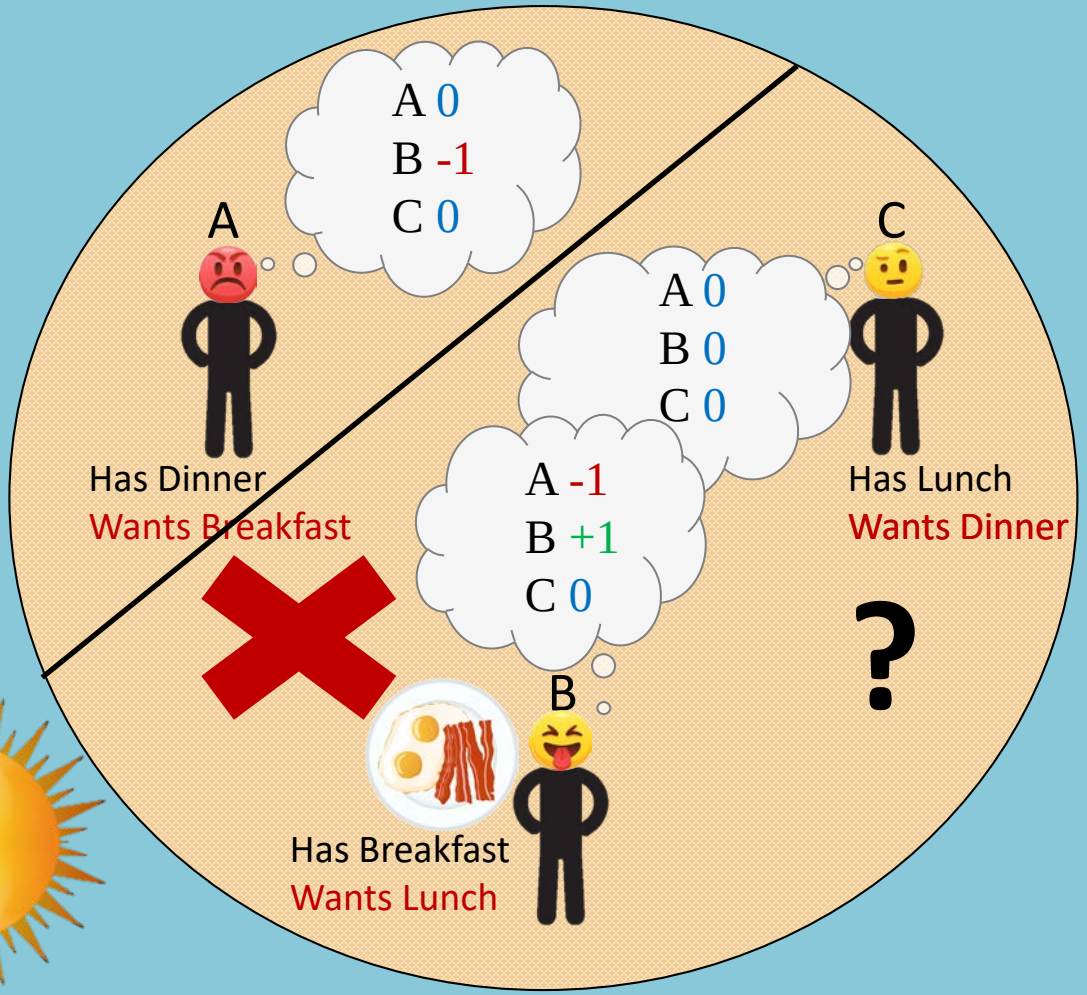
Primitive Blockchain (Limitation)

- As in the earlier scenario, Betty decides to eat breakfast herself instead of giving it to Adam.
- The scores don't adjust equally.
  - Adam docks Betty a point for not cooperating.
  - Betty lies and changes the score as if she gave breakfast to Adam.
  - Charlie doesn't see the trade, so his score is unchanged.



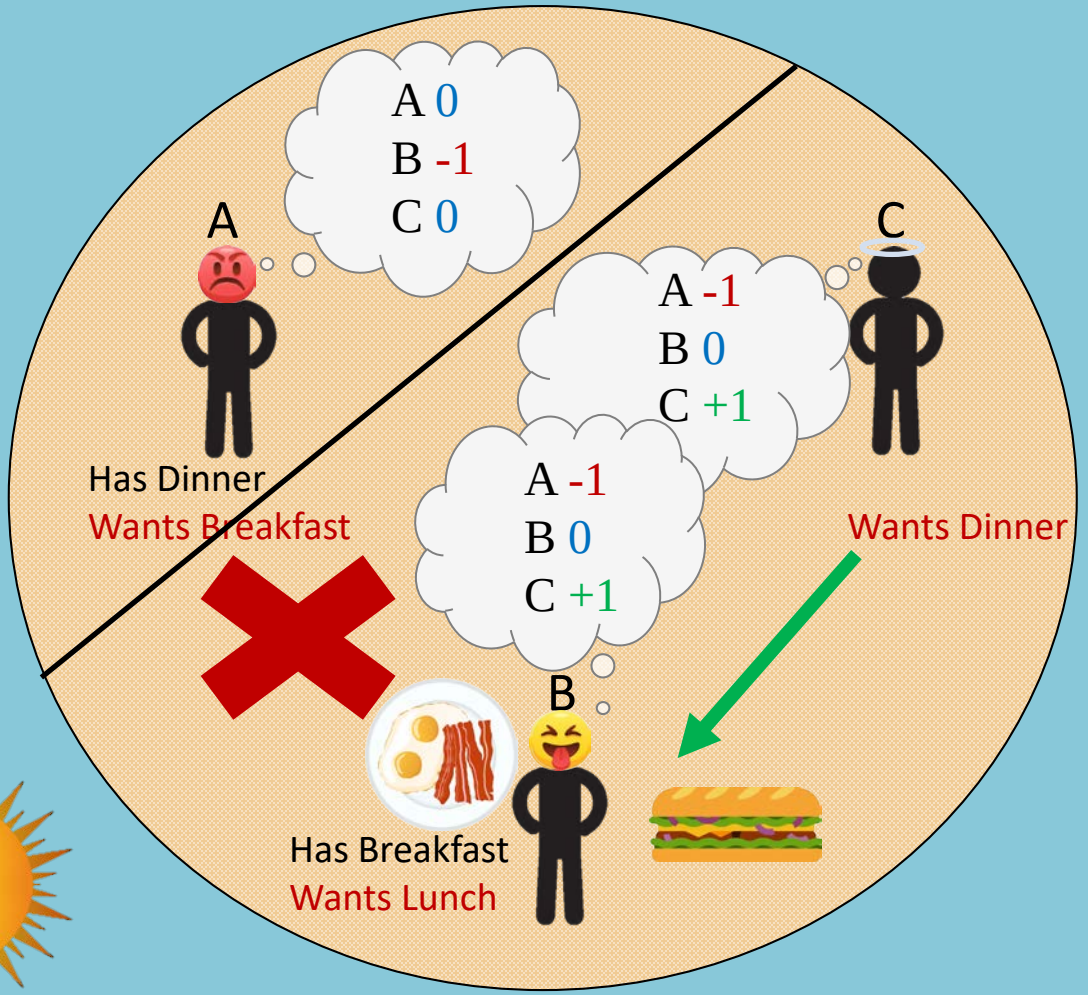
Primitive Blockchain (Limitation)

- In the afternoon, Adam goes off to make dinner and can't see what happens.
- Betty claims that she cooperated at breakfast, but Charlie doesn't know.
  - If Charlie doesn't believe her and thinks she didn't cooperate earlier, he won't give her lunch.
  - In this case, trade breaks down, and everyone is stuck with their least favorite meal.



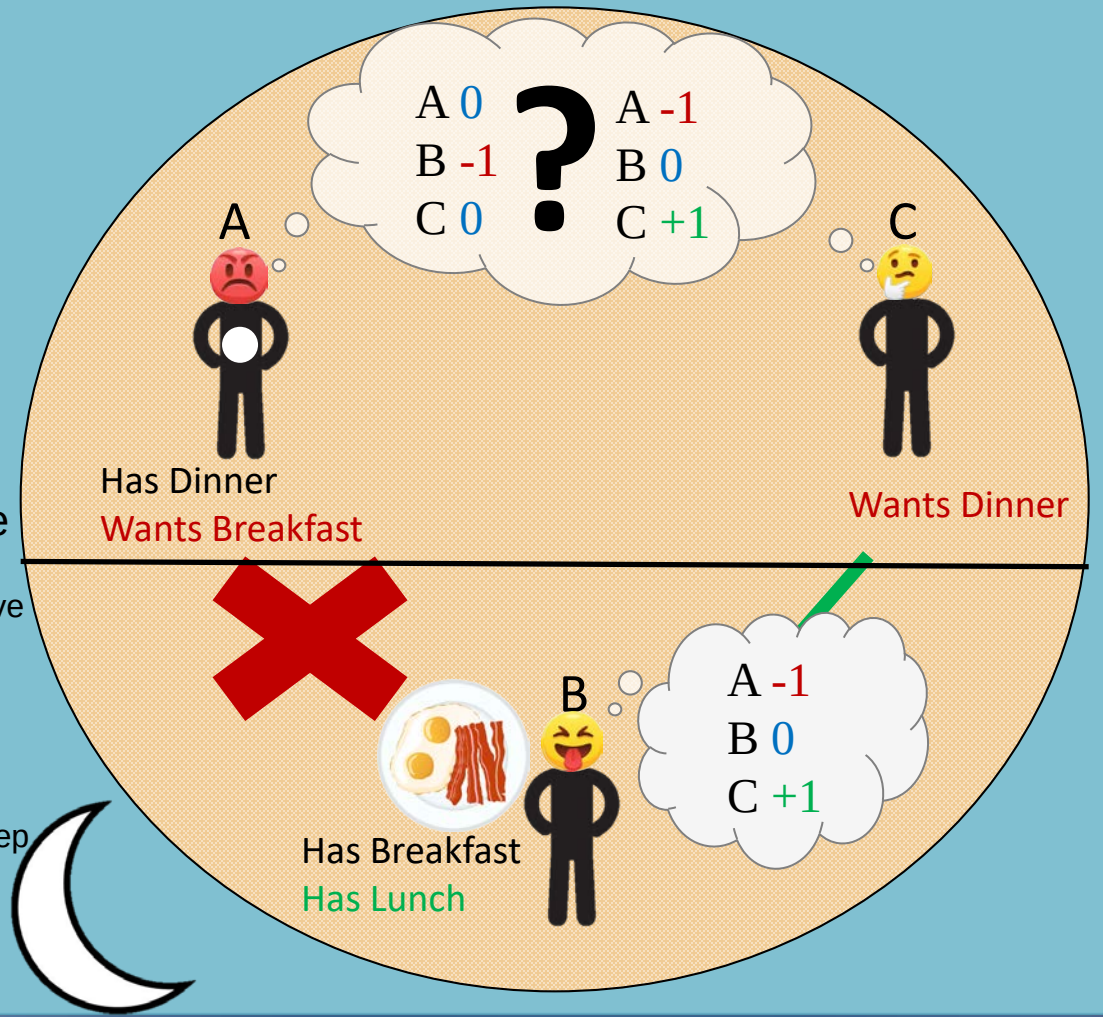
Primitive Blockchain (Limitation)

- But what if Charlie believes Betty?
  - He adjusts his scorecard to match Betty's.
- In this case, he sends lunch to Betty.
  - Now, Betty gets to eat both breakfast and lunch.
  - Both adjust their scores accordingly.
  - Adam is off making dinner, so he can't see what happens..



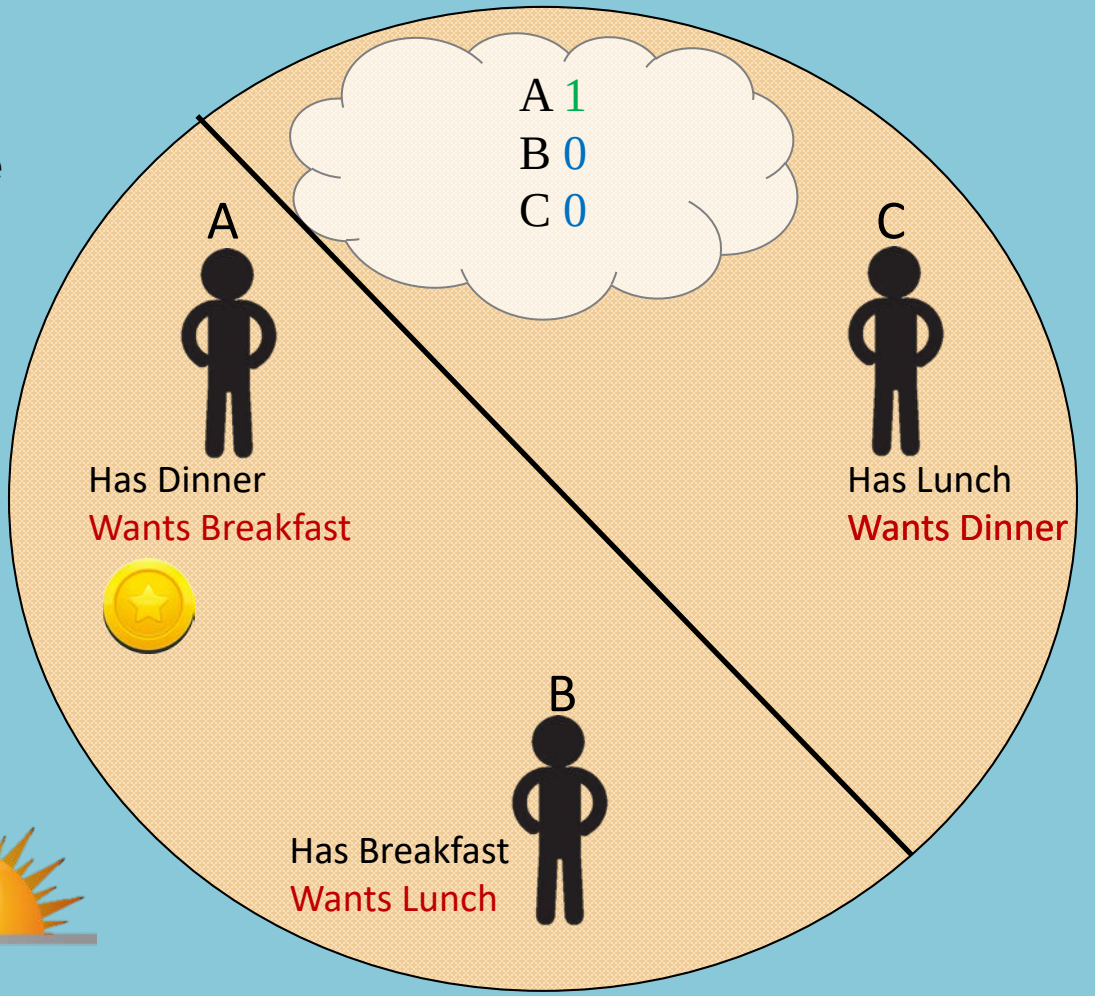
Primitive Blockchain (Limitation)

- In the evening, Betty goes to bed so that she can get up to make breakfast.
- Adam and Charlie don't agree about what happened today; there is no consensus.
  - Adam's scorecard shows that he didn't get breakfast this morning.
  - Charlie's scorecard is based on his belief that Betty did give Adam breakfast in the morning.
- Without consensus about history, trade breaks down.
  - If Adam gives dinner to Charlie, Adam will have eaten nothing today.
  - If Adam keeps dinner for himself, Charlie will have eaten nothing.
- As such, the primitive blockchain doesn't scale.
  - In communities in which not everyone can keep track of everything, the blockchain does not induce cooperation.



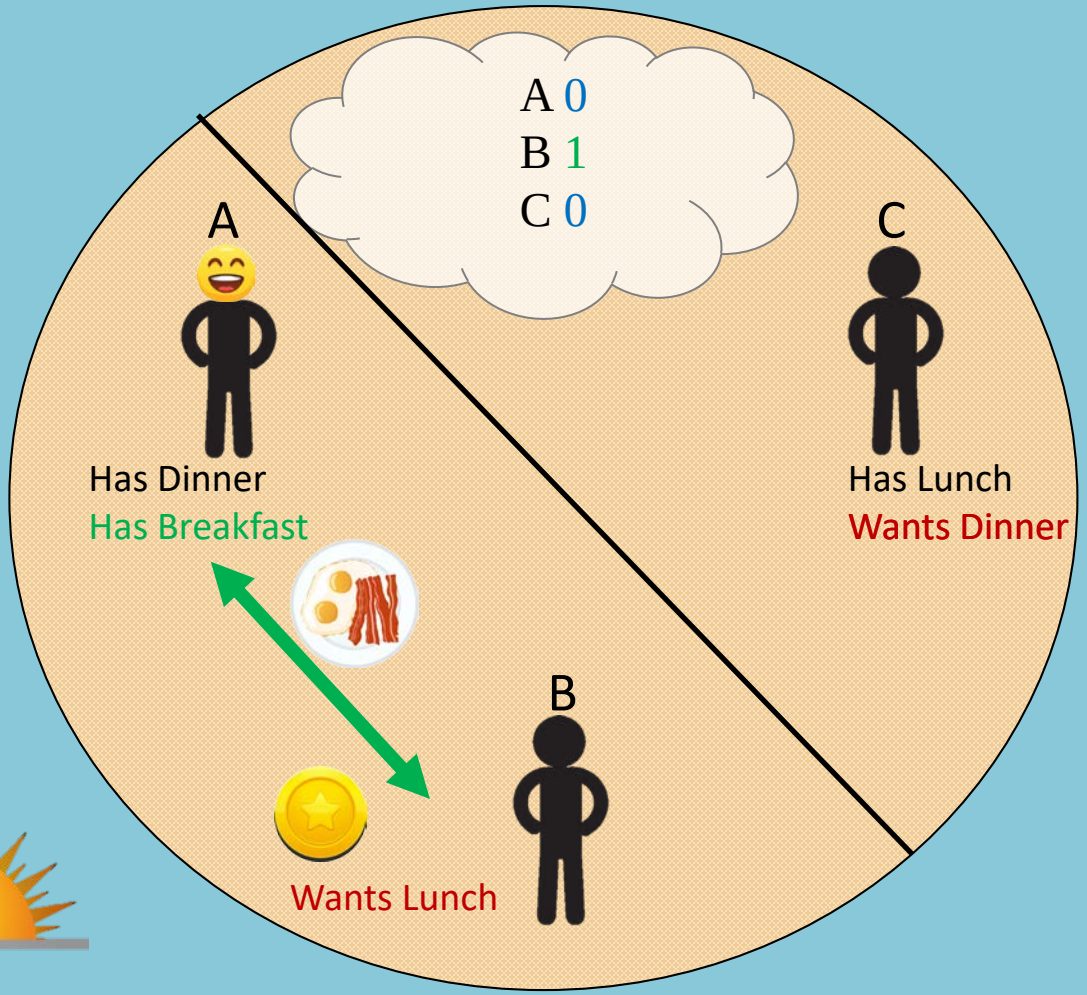
Physical Money

- To combat the problems outlined in the previous scenarios, the society invents physical money.
- Assume the following:
  - The token can't be stolen.
  - The token can't be counterfeited.
- There is still a scorecard, implicitly
  - But each person doesn't care
  - All that matters is whether or not they receive a token for their efforts



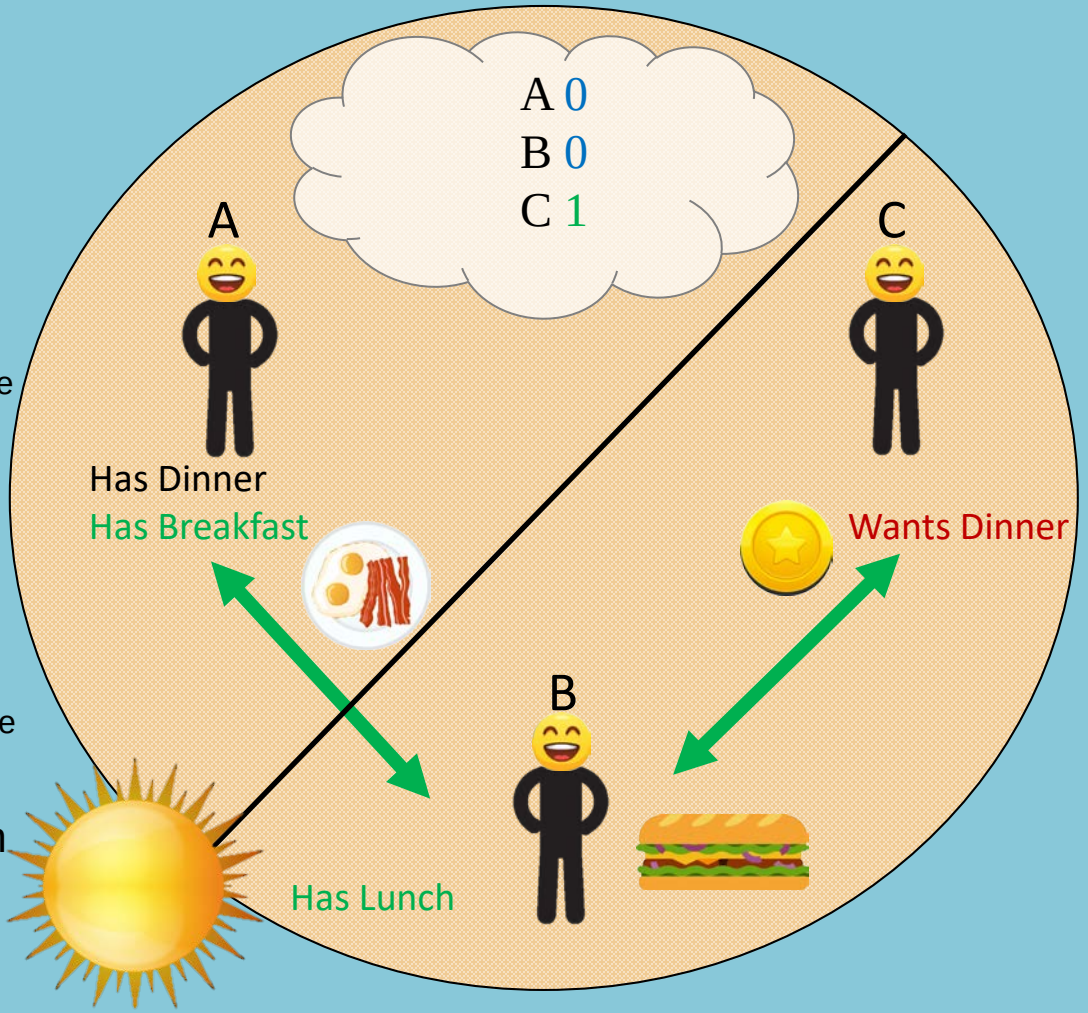
Physical Money

- As before, Charlie spends the morning away and can't see the rest of the island's actions.
- In the morning, Betty gives breakfast to Adam.
  - In return, Adam sends over the token.
  - The overall score updates, reflecting the fact that Betty now has the token.



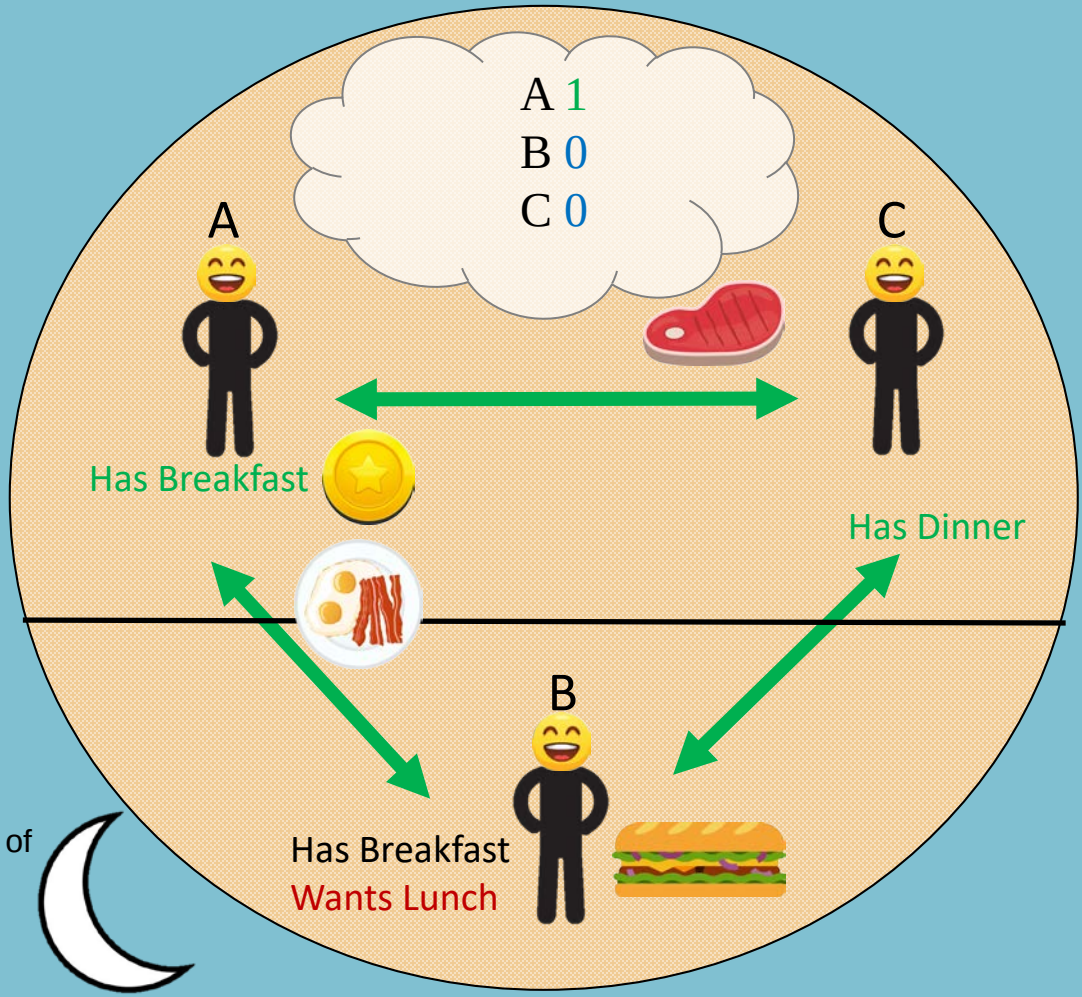
Physical Money

- Now, Adam is away.
- Money is a signal about the history of people's actions.
  - It proves that Betty gave Adam breakfast in the morning.
  - Charlie knows that Betty cooperated because she shows him the token that she earned.
- The token encourages cooperation
  - If Betty didn't give breakfast to Adam, she wouldn't have the token and thus, would not be able to get lunch.
- Betty spends the token on lunch, which Charlie provides to her.



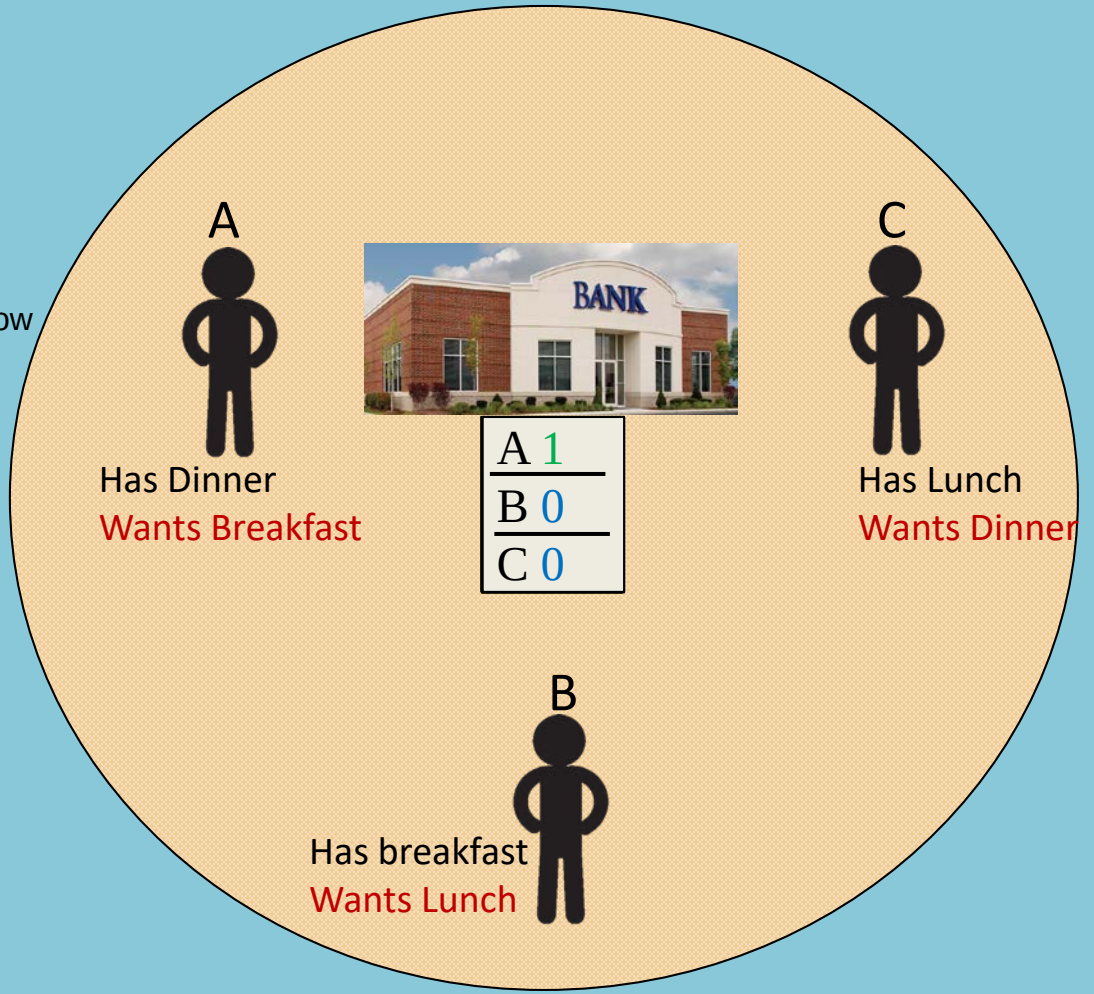
Physical Money

- The same thing occurs at night.
- Charlie's token signals that he cooperated in the afternoon by giving lunch to Betty.
- Charlies spends the token on dinner, which Adam provides.
- Now, Adam has the token.
- End of the day: everyone eats their favorite meal and is happy.
  - This is *not* blockchain at work.
  - The token serves as a proof of history in lieu of communal recordkeeping.



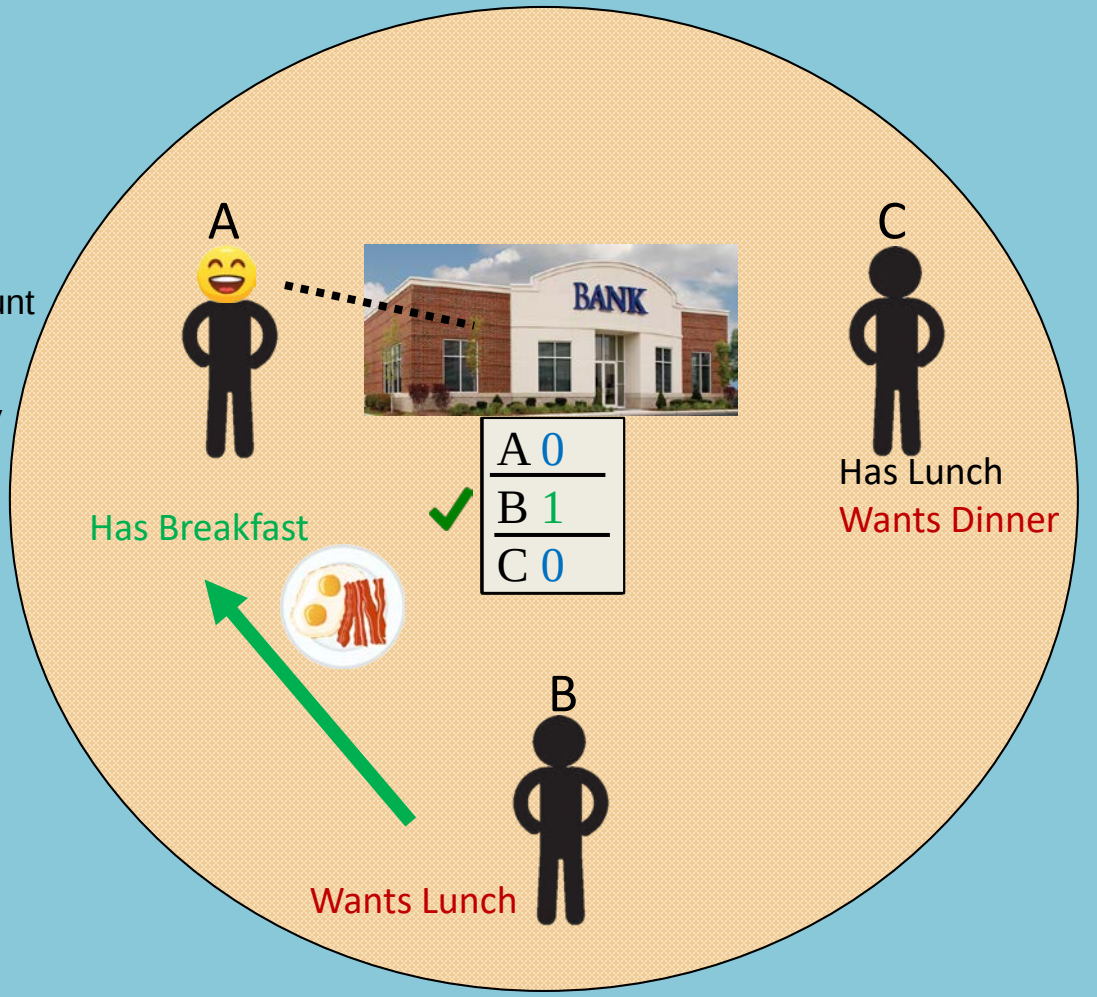
Digital Money (Central Ledger)

- Physical money is cumbersome.
  - What if it gets stolen or lost?
  - Before every trade, you have to physically show it to prove you have money to spend.
- Digital money is easier to use.
- It's also easier to steal or counterfeit.
  - The community entrusts a central authority, the bank, to keep track of it.



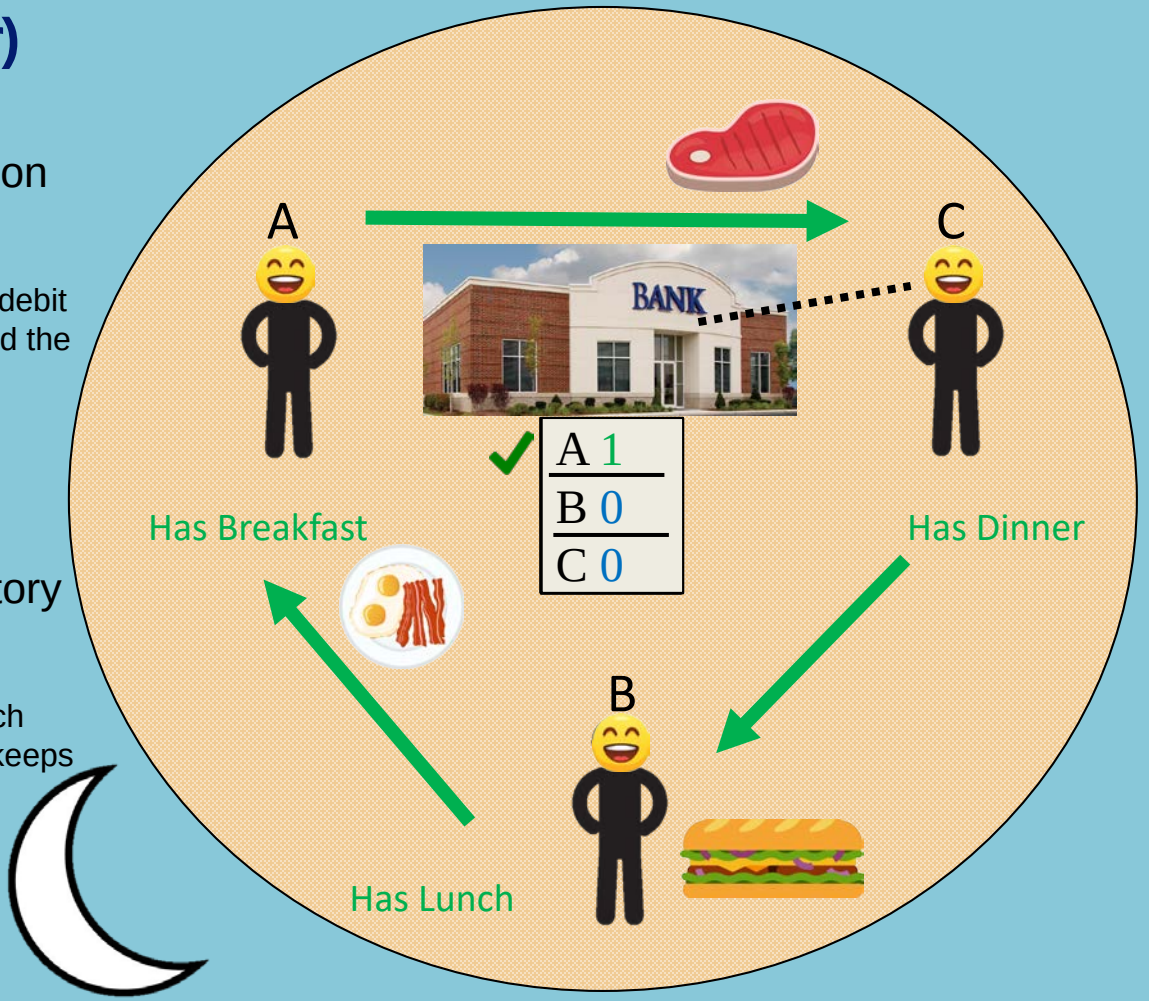
Digital Money (Central Ledger)

- In the morning, Adam swipes his debit card.
  - Adam is telling the bank to debit his account and credit Betty's.
  - The bank verifies that he has money, so Betty sends him breakfast.
- Digital money still encourages cooperation.
  - If Betty does not cooperate, Adam won't send her money.
  - She then would have nothing to spend in the afternoon and wouldn't get lunch.



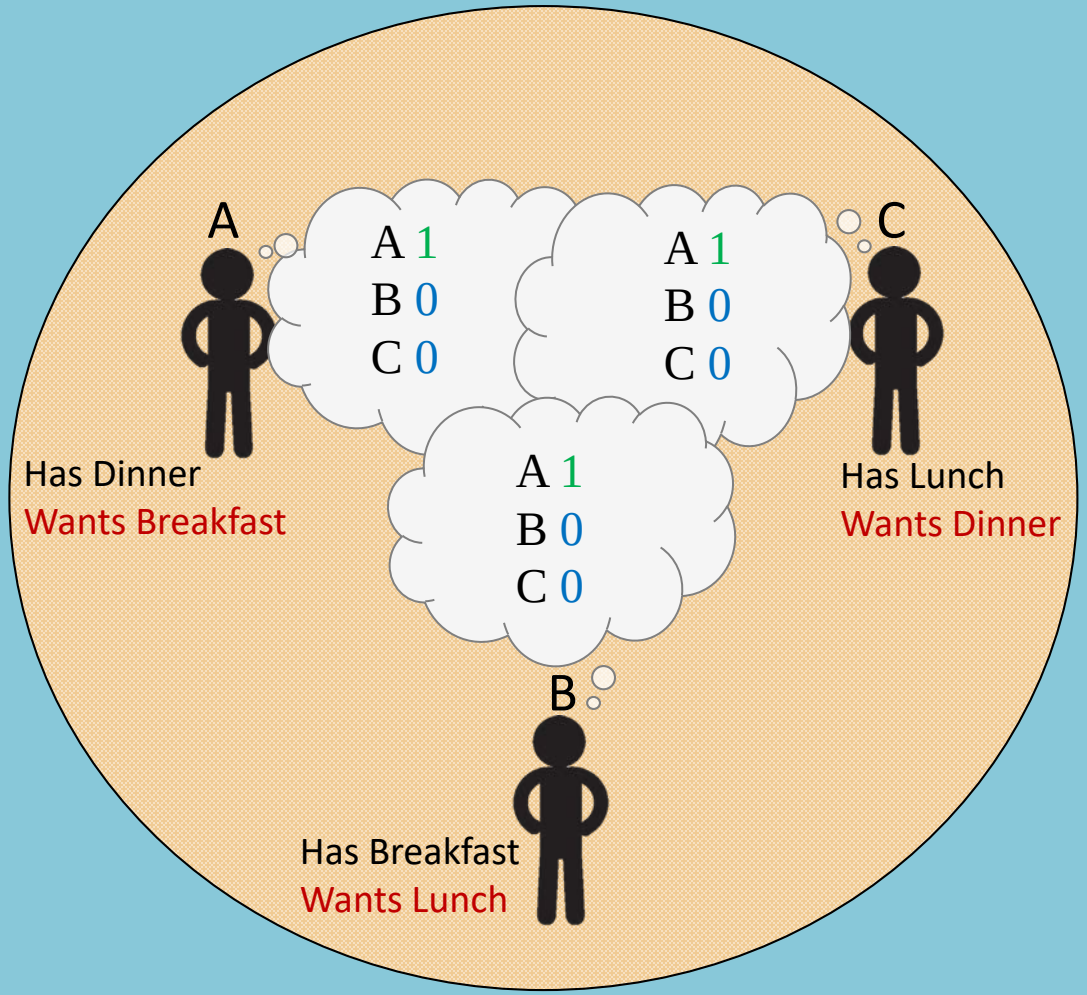
Digital Money (Central Ledger)

- A similar trade occurs in the afternoon and evening.
  - The consumer of each meal swipes their debit card, the bank verifies the transaction, and the trade takes place.
- End of the day: everyone eats their favorite meal and is happy.
- Money is still a signal about the history of actions.
  - Instead of showing physical money to each other to prove what happened, the bank keeps track via digital money.



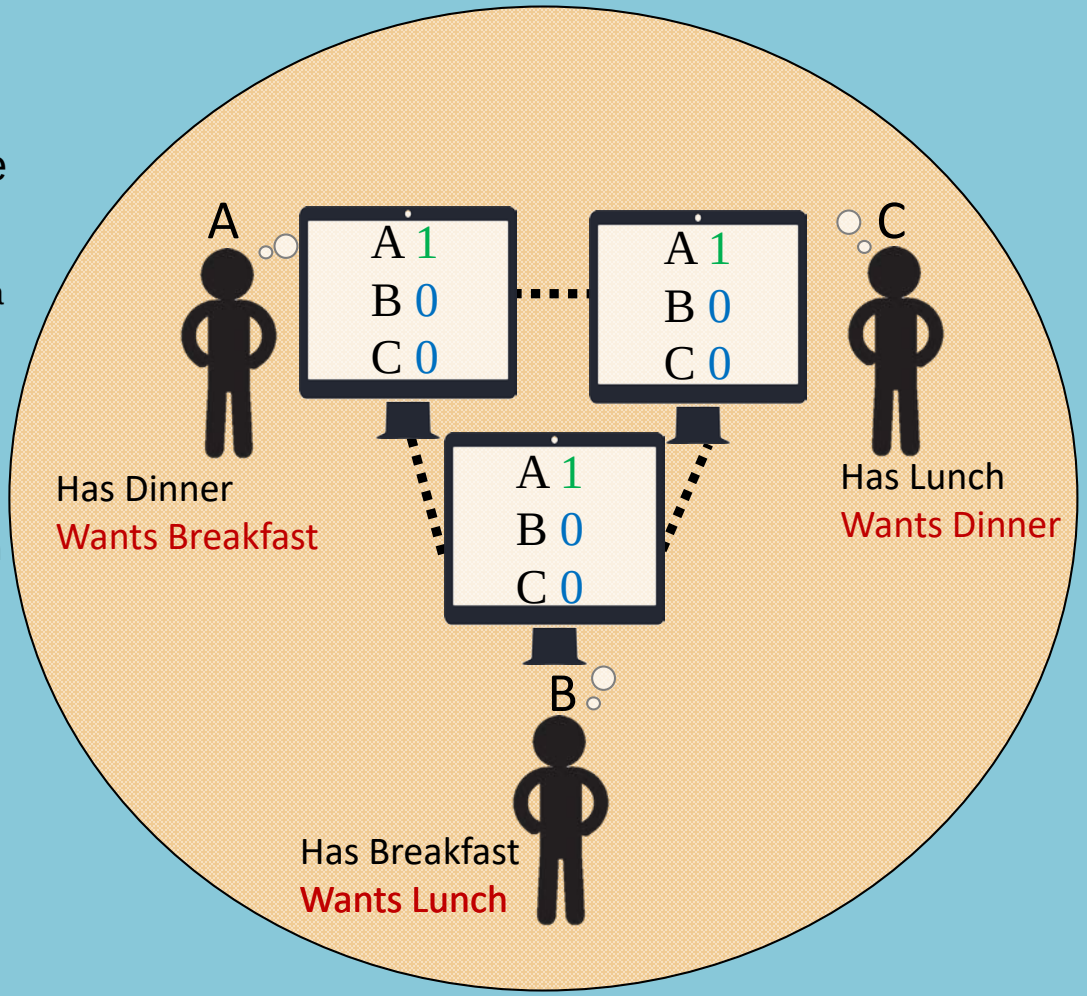
Cryptocurrency

- What if there are no banks in this community?
- What if people don't trust the bank?
- One option is to revert back to the primitive blockchain.
  - However, we know that this blockchain has limitations.



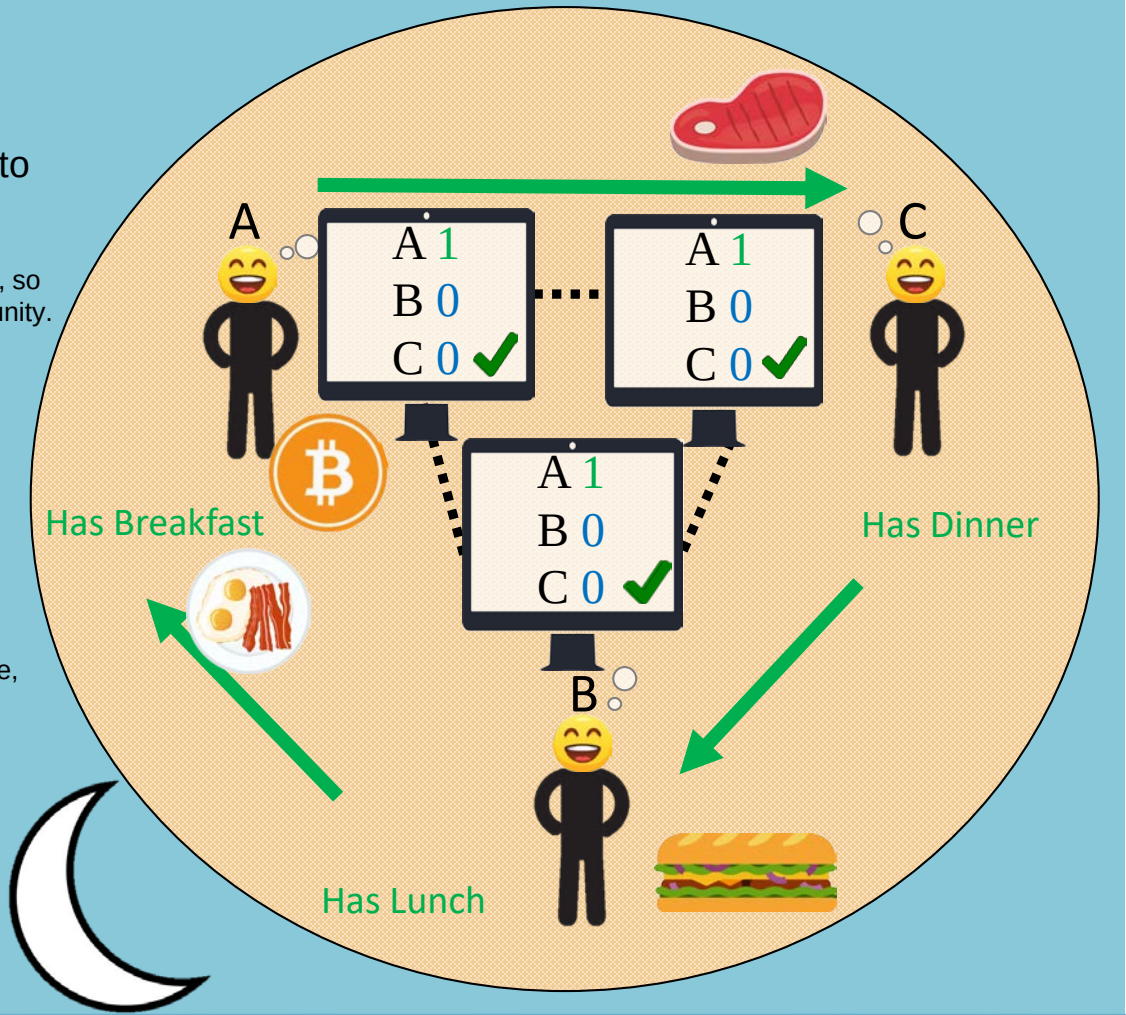
Cryptocurrency

- Thanks to technological progress, there is another option: cryptocurrency.
  - This digital money operates independently of a central authority
  - Instead of our brains keeping track of what happens, computers on a shared network do the work
  - Instead of having to talk to each other to reach consensus, the network uses math and game theory to verify actions.
- This is a modern blockchain.
  - It's a communal, technology-based recordkeeping system.

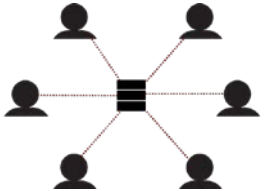
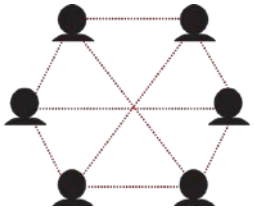


Cryptocurrency

- For each trade, the consumer pays bitcoin to the producer.
  - The trade takes place on a shared computer network, so action is recorded and verified throughout the community.
- Bitcoin induces cooperation.
  - If somebody doesn't cooperate, they won't have the bitcoin to buy their favorite meal.
- The modern blockchain works for larger communities, too.
  - The human brain can't keep track of that many people, but computers can.
- Bitcoin is literally a revolution.
  - It's the same concept as the primitive blockchain.
  - The only difference is that it's based on technology.



Modern Blockchain

- Works in much the same way as “primitive blockchain,” but now on a **global scale** thanks to technological advancements in data storage, communications, cryptography and game theory.
  - Human brains replaced with computer servers.
  - Vocal communications replaced with electronic messaging.
  - Security storage and messaging via cryptography.
  - Consensus via technology, math, and game theory.
- But these technological advancements are also available for non-consensus based database management systems.
- When to choose  vs.  ?

Delegated vs. Communal Recordkeeping Systems

Central Bank Digital Currency (CBDC)

- Central banks already issue digital money (reserves).
  - Note: Private banks issue digital money too (deposit accounts)
- What is meant by CBDC?
  1. Central bank accounts for all (not just depository institutions).
  2. Central bank digital tokens (permissionless bearer instruments, like central bank paper money).
- Option 2 seems unlikely because of *know-your-customer* (KYC) and *anti-money-laundering* (AML) concerns.
- Option 1 (or some variant) seems promising.

How Would CBDC Work?

- *Fedwire* a real-time-gross-settlement (RTGS) payment service operated by Fed for large financial institutions.
  - Cheap, efficient, and secure (550K TX/day, $3T/day).
  - Why not ***Fedwire4All***?
- Technologically feasible for anyone to open online interest-bearing accounts with the Federal Reserve.
  - U.S. Treasury already does this: www.treasurydirect.gov
- CBDC: No-frills account, no overdraft privileges, fully-insured, no minimum balances, zero (or low) user cost.

A Case for Central Bank Digital Currency

- Relative to cryptocurrencies, trusted intermediary inherently more efficient than consensus-based record-keeping.
- Public good aspect to payment services (similar to public roadways, sidewalks, etc.) → role for state money.
  - Eliminate “tollgates upon the highway of commerce.” (Carter Glass, 1913)
  - Level the playing field for small businesses (economically/politically smart)
  - Promote financial inclusion (economically/politically smart)
- Move cash management operations of large firms out of the shadow bank sector (promote financial stability).
- New monetary/fiscal policy tools: interest on CBDC and “helicopter” transfers of money.

A Case for Cryptocurrencies

- Circumvent unavailable/archaic/costly bank network.
  - Globally, correspondent banking system can be slow/costly.
  - Billions of people worldwide presently unbanked; U.S. 7% households unbanked (roughly 15 million adults).
  - Cryptocurrencies offer permissionless access and use; consumer interface similar to online banking.
  - Bitcoin as a global digital (vehicle) currency?
- Distrust of central authorities.
  - Centralized databases imply concentrations of power.
  - Will personal information be kept secure/not be misused?
  - Can central banks be trusted to manage money supply?

Competitive Coexistence

- Options: (1) CBDC; (2) private banks; (3) cryptocurrencies.
  - These are not mutually exclusive alternatives
  - Innovation should be encouraged in all three spheres.
- CBDC offers public option as baseline service for all (online version of U.S. Postal Savings System 1911-67).
- Private banks compete by offering “full service” accounts together with regular lending services.
- Cryptocurrencies likely to serve niche roles and provide a check on irresponsible central (and private) bank policies.

Summary and Conclusions

Summary

- Technological advances in data storage, communications, security, continue to transform the money and payments system (database management systems, generally).
- Blockchain: What's old is new again? Many promising applications (though money not likely one of them).
- Payment system as a public good? Central banks may have comparative advantage in providing uniform, low-cost, widely-accessible medium of exchange in the form of CBDC.
    - Leveling playing field, promoting financial inclusion, makes economic and political sense, via CBDC or some variant.

Concluding Thoughts

- This is not the first or last word on the subject.
- Evaluating cryptocurrencies and banks from perspective of alternative database management systems useful.
- Need to respect different perspectives on the subject.
- Seek common ground, compromise where we can.
- Coexistence both possible and desirable!

Thank you!

- Additional information available on my blog, *Macromania*
  - http://andolfatto.blogspot.com/
- Follow me on Twitter: @dandolfa
- Email: David.Andolfatto@stls.frb.org

Connect With Us

STLOUISFED.ORG

Blogs and Publications
News and views about the economy and the Fed

Federal Reserve Economic Data (FRED)
Thousands of data series, millions of users

From the President
Key policy views, speeches, presentations and media interviews of President Bullard

Community Development
Promoting financial stability of families, neighborhoods

Economic Education Resources
For every stage of life

SOCIAL MEDIA

ECONOMY MUSEUM

INSIDE THE ECONOMY. MUSEUM
AT THE FEDERAL RESERVE BANK OF ST. LOUIS