Games and Economic Behavior 153 (2025) 1–9

Contents lists available at ScienceDirect

Games and Economic Behavior

journal homepage: www.elsevier.com/locate/geb

No trade under verifiable information ☆

Spyros Galanis

Department of Economics, University of Durham, United Kingdom

ARTICLE INFO

JEL classification:
D82
D83
D84
G14
G41

Keywords:
No trade
Blockchain
Oracles
Agreeing to disagree
Information aggregation

ABSTRACT

No trade theorems examine conditions under which agents cannot agree to disagree on the value of a security which pays according to some state of nature, thus preventing any mutual agreement to trade. A large literature has examined conditions which imply no trade, such as relaxing the common prior and common knowledge assumptions, as well as allowing for agents who are boundedly rational or ambiguity averse. We contribute to this literature by examining conditions on the private information of agents that reveals, or verifies, the true value of the security. We argue that these conditions can offer insights in three different settings: insider trading, the connection of low liquidity in markets with no trade, and trading using public blockchains and oracles.

1. Introduction

Contrary to common belief, asymmetric information by itself is insufficient to account for the high trading volumes observed in financial markets. Aumann (1976) first showed that if agents share a common prior, then it cannot be common knowledge that they disagree on the probability they assign to an event. Milgrom and Stokey (1982) use this result to show that if an allocation is ex ante Pareto efficient, then new asymmetric information will not lead to trade if agents are risk averse and hold concordant beliefs. There is now a large literature examining conditions that generate no trade, such as relaxing the common prior or common knowledge assumptions, or having agents who are boundedly rational or ambiguity averse.

The current paper contributes to this literature by examining a different set of conditions that lead to no trade, specifically examining how agents' private information can reveal or verify the true value of the security being traded. To provide an example, suppose that it is common knowledge that agent i always knows the true state and therefore the true value of the traded security. Then, no other agent would be willing to accept a buy or a sell order and there would be no trade, irrespective of whether the common prior assumption holds. The reason is that it cannot be common knowledge that we disagree on the value of the security, when it is common knowledge that agent i knows its value. Hence, accepting a trade 'must' be wrong if you are not agent i. Is it possible to further weaken this condition regarding the verifiability of the security's value while still implying no trade? For example, we could require that the conjunction of everyone's knowledge verifies the true value of the security. Alternatively, what if there is an agent who always knows whether the value of the security is above or below a certain threshold? Are these conditions necessary or sufficient to preclude trade? To motivate these questions, we provide three examples.

☆ I would like to thank Arzé Karam, Jan Christoph Schlegel, an anonymous referee, and participants at the EC24 Workshop on Blockchains and Decentralized Finance at Yale, for useful comments. I would like to acknowledge financial support from the Economic and Social Research Council (ES/V004425/1). The previous title of this paper was "No Trade in a Blockchain".

E-mail address: spyros.galanis@durham.ac.uk.

https://doi.org/10.1016/j.geb.2025.05.007
Received 13 September 2023

Available online 30 May 2025

The first is insider trading. The UK Criminal Justice Act 1993 states in Section 52 that 'An individual who has information as an insider is guilty of insider dealing if [...] he deals in securities that are price-affected securities in relation to the information'. This clause can be interpreted to mean that insider trading occurs when the insider possesses private information significant enough to affect the price—or underlying value—of the security. Put differently, the insider knows whether the value of the security lies above or below a certain threshold.

Suppose that agents bet on the financial performance of a company, by trading a derivative on the price of its share. If an employee has insider information which always reveals the true value of the company, it is straightforward that she should not be allowed to trade. The reason is not that she can make huge profits by 'taking advantage' of other agents; it is because, if agents are rational, they will understand that this possibility exists and there will be no trade. A no trade result is detrimental in this case because the price of the derivative may not be sufficiently close to its true value, hence the market would fail in aggregating information. However, what if the employee's knowledge is not enough to verify the true value of the company, but only whether it is above a certain threshold? By understanding the conditions on verifiability that result in no trade, we can determine under which conditions we should allow insiders to participate in a financial market.

The second example links low liquidity with no trade. In 1998, the Long-Term Capital Management (LTCM) hedge fund was facing collapse due to the Russian debt default. The resulting fire sales and the costly disruptions for the world financial markets led the Federal Reserve Bank of New York to hold meetings to recapitalise LTCM. Cai (2003) documents how market makers in the bonds futures market made huge profits using privileged information on customer order flow. What happens to trading if it becomes common knowledge that market insiders know which assets are distressed and therefore have a low value? If this leads to a no trade result, then the liquidity of the market will dry up, exacerbating the price impact of the insiders and the distressed sellers. Cai (2003) shows, in fact, that market liquidity was very low during this episode.[1]

The third example is trading on the blockchain. A public blockchain enables a decentralised trading environment, where completing a transaction does not require a third party which custodies the agents' assets, verifies their ownership, or executes the transaction. All transactions are public and trades are executed algorithmically using *smart contracts*, when pre-specified events occur. For example, paying an option on a real-world asset requires the reporting of its value within the blockchain, so that the smart contract can be executed. In practice, the verification and reporting of real-world events to the blockchain is performed by *oracles*.[2] However, because users of the blockchain are anonymous, nothing stops oracles from participating in the trade, especially when they know it is going to be favourable for them.[3] Will this 'insider trading' make trading on the blockchain inherently undesirable?

We examine conditions on the verifiability of securities (that is, revealing their true value) using three different environments. In all settings, there are finitely many states and agents, equipped with asymmetric information and different priors. Security X pays a dividend according to the state of nature. Trades are agreed in the interim stage, after agents receive their private information but before the true state is revealed. The first environment is static and follows Aumann (1976). We say that there is common knowledge trade at some state if the agents' expected values of the security are common knowledge but different. The second environment is dynamic with infinitely many periods, following Geanakoplos and Polemarchakis (1982). In each period, one agent announces (truthfully) his expected value of the security. All other agents update their information based on the announcement and form a new expected value. In the next period, another agent announces his expected value, and so on. We say that agents cannot disagree forever if they eventually agree on the expected value of the security. The third environment is also dynamic and follows Ostrovsky (2012). Agents are myopic and payoffs are determined using market scoring rules, which are most often used in prediction markets. We say that there is information aggregation if the price of the security always converges to its true value.

What conditions on the private information of agents lead to no trade and information aggregation? On one extreme, we say that the security is *verifiable* if, for each state, there is some agent who knows its value in the interim stage, when the trade is agreed. This condition is strong and it implies that there cannot be common knowledge trade. On the other extreme, the security is *collectively verifiable* if the conjunction of the knowledge of all agents reveals its true value. In this case, it is possible that no-one knows the value of the security, when the trade is agreed. We show by example that collective verifiability does not lead to no trade.

Our main results involve two intermediate properties. We say that the security is *maxmin verifiable* if there exists a agent who knows whether the maximum (or minimum) has occurred, among all values of the security that it is common knowledge that are possible. It is *threshold verifiable* if there is a threshold x within those values and a agent who knows at some state whether the security's value is strictly above or below x. Even though maxmin verifiability is significantly weaker than verifiability, we show that it is sufficient for no trade. Our main result, Theorem 1, shows that threshold verifiability is necessary and sufficient for no common knowledge trade. In a dynamic setting, however, a security that is threshold or maxmin verifiable at time t, may not be at time $t+1$. This means that these two properties are not sufficient for no trade or information aggregation, unless we assume that they hold at a distant time t^*, when agents have stopped updating their announcements.

[1] Brunnermeier (2001) provides an overview of the literature on asymmetric information and stock market crashes, whereas Brunnermeier and Pedersen (2005) construct a model of predatory trading with distressed sellers. Karam and Bogoev (2023) provide an empirical investigation of the connection between low liquidity and momentum trading.

[2] Garratt and Monnet (2022) show that oracles are unavoidable, because the truthful reporting about the realisation of publicly observed events cannot be implemented as a unique equilibrium in a completely decentralized environment.

[3] More accurately, they are pseudonymous, because the history of transactions is public and can be linked to the unique addresses.

1.1. Related literature

Several papers (Morris (1994), Feinberg (2000), Samet (1998), Bonanno and Nehring (1999), Halpern (2002), Ng (2003)) characterize the existence of a common prior with respect to the condition that there does not exist a mutually beneficial trade that is common knowledge at all states. Geanakoplos (1989) showed that trade can still occur with common priors if agents are boundedly rational and make information processing errors. These results were extended in an environment with unawareness by Galanis (2013, 2018), Heifetz et al. (2013) and Meier and Schipper (2014). The current paper differs from this literature because it imposes conditions on the private information of agents, rather than on priors or bounded rationality.

Ostrovsky (2012) and Chen et al. (2012) show that in a market with either myopic or strategic agents, *separable* securities are both necessary and sufficient for information aggregation. Their models are based on market scoring rules (Hanson (2003, 2007)), hence their results are directly applicable to prediction markets (Wolfers and Zitzewitz (2004)). Similar approaches can be found in Dimitrov and Sami (2008), Galanis and Kotronis (2021), Galanis et al. (2024) and Galanis and Mikhalishchev (2025), where the focus is on examining whether information gets aggregated under various assumptions regarding preferences and the signal structure, such as unawareness, ambiguity aversion, and costly information acquisition. These papers identify classes of securities which ensure that information is aggregated. In the current model, our results apply to all securities, but the conditions on private information are imposed at a distant time t^* where all information updating has concluded.

The advantage of the market scoring rules (MSR) over more well-known market mechanisms, such as the continuous double auction, is that an agent can make her prediction/trade without waiting for another agent to take the opposite side, or submit a limit order and wait for it to be filled. This feature makes it an attractive mechanism for markets with relatively few participants who do not trade daily, or in markets with automated market makers. Automated market makers (AMMs) are widely used in Decentralized Finance, see Schlegel et al. (2022) for an axiomatization of the logarithmic MSR. For more on the connection between prediction markets and AMMs, see Frongillo and Waggoner (2017), Othman and Sandholm (2011), Abernethy et al. (2013), and Abernethy and Frongillo (2012).

There is a growing literature on the economics of blockchain and cryptocurrencies. Biais et al. (2019) provides a game-theoretic analysis of the proof-of-work protocol, which is in Bitcoin used by the miners, who maintain and update the ledger. Athey et al. (2016) and Böhme et al. (2015) describe several empirical facts about the usage of Bitcoin, whereas Chen et al. (2019) examines the desirable properties of the proof-of-work protocol. Easley et al. (2019) explains the emergence of transaction fees in Bitcoin using a game-theoretic analysis. Budish (2018) argues that the payments to miners, for maintaining the blockchain, must be large relative to the one-off benefits of attacking it, thus making the blockchain vulnerable to attacks once it becomes valuable. Schilling and Uhlig (2019) discusses the monetary policy implications when cryptocurrencies compete with traditional currencies, backed by a central bank. Hinzen et al. (2019) argues that the proof-of-work protocol is inherently unable to sustain a large volume of transactions. The reason is that a rise in transaction demand leads to an increase in block fees, attracting more miners and exacerbating network latency, thus delaying payment confirmation and making the payment platform less attractive for users. Abadi and Brunnermeier (2018) examines when record-keeping is better organised through a blockchain, instead of a traditional centralised intermediary.

In the current paper we assume that oracles do not act strategically and cannot lie about their reports, when they verify the value of the security. The issue of eliciting truthful reports in a strategic environment was first studied by Prelec (2004) (Bayesian Truth Serum) and Miller et al. (2005) (peer-prediction mechanisms). In general, these mechanisms work by randomly pairing two agents and paying them according to how close their reports are. See Jurca and Faltings (2006), Witkowski and Parkes (2012a,b) for various extensions. Goel et al. (2019) uses the peer-prediction mechanism of Radanovic et al. (2016), in order to study truthful reporting of oracles in a blockchain.

The paper is organised as follows. Section 2 presents the basic model. Section 3 examines the three trading environments and presents the results on no trade.

2. Model

Let I be a finite set of n agents. Uncertainty is described by a finite set of states Ω. Agent i's private information is represented by partition Π_i and prior p_i that has full support on Ω. We do not assume a common prior, so we allow $p_i \neq p_j$ for some $i, j \in I$.

Agent i knows event E at ω if $\Pi_i(\omega) \subseteq E$. This means that in all states that he considers possible at ω, E is true. Define $\Pi_i(F) = \bigcup_{\omega' \in F} \Pi_i(\omega')$ to be the set of all states that i thinks are possible, if the true state is in F. Using this notation, we can say that $\Pi_j(\Pi_i(\omega))$ is the set of states that, at ω, agent i thinks that j considers possible. If $\Pi_j(\Pi_i(\omega)) \subseteq F$, then we say that i knows that j knows F. An event E is common knowledge at ω if $\Pi_{i_n}(\Pi_{i_{n-1}} \dots (\Pi_{i_1}(\omega))) \subseteq E$, for any sequence of agents $i_1, \dots, i_n$.[4]

Let $C(\omega)$ be the set of states that are reachable from ω. Formally, $C(\omega)$ is the union of sets $\Pi_{i_n}(\Pi_{i_{n-1}} \dots (\Pi_{i_1}(\omega)))$, for any sequence of agents $i_1, \dots, i_n$. Say that an event E' is self-evident if, whenever it occurs, everyone knows it. Formally, for all $\omega' \in E'$ and $i \in I$, we have $\Pi_i(\omega') \subseteq E'$. Then, $C(\omega)$ can be described as the smallest self-evident event that contains ω.[5] Aumann (1976) showed that an event E is common knowledge at ω if and only if $C(\omega) \subseteq E$.

[4] These notions are explained further in Geanakoplos (1992).

[5] The partition generated by C is called the finest common coarsening of the partitions of all agents.

A security is a function $X : \Omega \to \mathbb{R}$, where $X(\omega)$ is the security's payoff at state ω. Let $X(C(\omega)) = \bigcup_{\omega' \in C(\omega)} X(\omega')$ be the collection of all values of security X that can be realised in states reachable from ω. Intuitively, these are the values of X such that some agent i_1 thinks that i_2 thinks that ...some i_n considers possible. Alternatively, $X(C(\omega))$ is the smallest set of the security's values that it is common knowledge at ω that agents consider possible. Let $\max X(C(\omega))$ be the maximum and $\min X(C(\omega))$ the minimum of these values.

When a state ω occurs, agent i receives private information $\Pi_i(\omega)$ and updates his prior p_i. His expectation of X at ω is therefore $e_i(\omega) \equiv \sum_{\omega' \in \Pi_i(\omega)} X(\omega') \frac{\pi_i(\omega')}{\pi_i(\Pi_i(\omega))}$. The event "Agent i's expectation of X is e_i" consists of all states ω such that $e_i(\omega) = e_i$.

2.1. Verifiability

We introduce four properties on the private information of agents that verify the value of security X and in the next section we examine their implications for trade. Note that we allow for different priors. Under a common prior, there would be no trade so verifiability would not have any implications.

Definition 1. Security X is verifiable if, for each $\omega \in \Omega$, there exists $i \in I$ such that $\Pi_i(\omega) \subseteq X^{-1}(k)$, for some $k \in \mathbb{R}$.

Verifiability specifies that, at each state, there exists at least one agent who knows the true value of the security. This is a strong property that implies no common knowledge trade. Maxmin verifiability, which is weaker, specifies that among all the values of X that it is common knowledge that they are possible, there is a agent who knows either the highest or lowest value of X, when it is true. For example, consider a security which is linked to the value of a new oil well. The possible values are between zero and some positive number, depending on how much oil can be extracted. An expert can determine the range of values by running tests if given access to the well, however if there is no oil at all then she will be able to verify this. Hence, if the expert is also a agent in the market, maxmin verifiability is satisfied, because when one extreme value is true, at least one agent knows it.

Another example involves scientists engaged in the development of a breakthrough drug, either within a pharmaceutical firm or a regulatory authority overseeing its approval. While the success of the drug remains uncertain, the firm's valuation is constrained within a certain range, sustained by ongoing research efforts and investment. However, once the drug is either demonstrably successful or on the verge of regulatory approval, it becomes apparent that the firm's value will approach its maximum. If these scientists are permitted to participate in trading before the company's announcement, the condition of maxmin verifiability is fulfilled.

Finally, a catastrophe bond (CAT bond) provides high yields to investors who buy it but the entire principal is lost if a specific disaster, such as a hurricane, occurs before it matures. The issuance of CAT bonds is premised on the violation of maxmin verifiability, so that it is common knowledge that no scientist could predict with probability 1 that a hurricane of a certain magnitude will occur.[6]

Definition 2. Security X is maxmin verifiable at ω if there exist $i \in I$ and $\omega' \in C(\omega)$ such that $\Pi_i(\omega') \subseteq X^{-1}(k)$, where $k \in \{\max X(C(\omega)), \min X(C(\omega))\}$.

This is a significant weakening of verifiability because only one value is verified, not all. Moreover, it is possible that the true value $X(\omega)$ is different from both $\max X(C(\omega))$ and $\min X(C(\omega))$. Nevertheless, we show that this property is still strong enough to preclude common knowledge trade. The following property is weaker than maxmin verifiability.

Definition 3. Security X is threshold verifiable at ω if, whenever $X(C(\omega))$ is not constant, there exist $i \in I$ and $\omega', \omega'' \in C(\omega)$ such that $\max_{\omega_0 \in \Pi_i(\omega')} X(\omega_0) < x < \min_{\omega_0 \in \Pi_i(\omega'')} X(\omega_0)$, for some $x \in \mathbb{R}$.

If security X is threshold verifiable, there are two cases. First, $X(C(\omega))$ is constant, so its unique value is common knowledge at ω. Second, $X(C(\omega))$ is not constant but there is a threshold x and a agent who knows at some state whether the value of the security is strictly above or below x. It is important to emphasise that the agent knows whether the value is above or below the threshold at *some* state, not at all states. Theorem 1 shows that threshold verifiability is necessary and sufficient for no common knowledge trade.

Examples for threshold verifiability are similar to the ones for maxmin verifiability, but the requirements are weaker. A scientist working in a pharmaceutical company knows whether its value is below or above a threshold, as he has inside information on how well the new drugs perform in tests. Similarly, an oil expert knows whether the value of the well will be above or below a threshold, depending on the outcome of the tests she conducts.

The final property specifies that the value of the security is verified only when all agents share their private information.

Definition 4. Security X is collectively verifiable if, for each $\omega \in \Omega$, $\bigcap_{i \in I} \Pi_i(\omega) \subseteq X^{-1}(k)$, for some $k \in \mathbb{R}$.

[6] The maturity of CAT bonds is usually between 1 and 5 years. Longer maturities are probably infeasible as scientists would accurately predict that a catastrophic event will occur with probability close to 1, hence maxmin verifiability is satisfied and such bonds would not be traded.

Collective verifiability is the minimum requirement which allows agents to agree a trade now and reveal their private information at a later date, so that the trade is settled and payments are made. We show with an example that this property is not strong enough to preclude common knowledge trade.

3. Trading environments

We explore three different trading environments. The first is static, whereas the other two are dynamic.

3.1. We cannot agree to disagree

We say that there is common knowledge trade at ω if the agents' expectations about the value of X are common knowledge at ω, but different. This is interpreted as agreeing to trade with each other, fully taking into account that the others are also willing to do so. For example, if $e_i > e_j$, then agent i is willing to buy some units of X from j. See Section 3.4, where we extend trading to a collection of securities $\{X_i\}_{i\in I}$ with $\sum_{i\in I} X_i = 0$. Recall that Aumann (1976) shows that common knowledge trade is impossible with a common prior, however in this setting priors can be different.

Definition 5. There is common knowledge trade at ω if the event "agent i's expectation of X is e_i, for each $i \in I$" is common knowledge at ω, yet $e_i \neq e_j$ for some $i, j \in I$.

The following theorem shows that threshold verifiability is necessary and sufficient to preclude any common knowledge trade. To prove necessity, we make the additional assumption that the security pays differently across states, so that $X(\omega) \neq X(\omega')$ for all $\omega, \omega' \in \Omega$. This precludes the uninteresting case where the intersection of the security's values that each agent considers possible across states, $\bigcap_{\omega'\in C(\omega)} [\min_{\omega_0\in\Pi_i(\omega')} X(\omega_0), \max_{\omega_0\in\Pi_i(\omega')} X(\omega_0)]$, is a singleton and the same for all agents, so that there is no common knowledge trade for any set of priors.

Theorem 1. *Security X is threshold verifiable at ω if and only if there is no common knowledge trade at ω, for any set of priors.*

Proof. Suppose X is threshold verifiable at ω. If $X(C(\omega))$ is constant, everyone knows the security's value and there is no common knowledge trade. If $X(C(\omega))$ is not constant, there exist $i \in I$ and $\omega', \omega'' \in C(\omega)$ such that $\max_{\omega_0\in\Pi_i(\omega')} X(\omega_0) < \min_{\omega_0\in\Pi_i(\omega'')} X(\omega_0)$. This implies that for any prior p_i, i's expected value of X at ω' is different from i's expected value of X at ω''. Because they are different, expected values cannot be common knowledge at ω, hence there is no common knowledge trade at ω.

Conversely, suppose that X is not threshold verifiable at ω, hence $X(C(\omega))$ is not constant. We will show that there is common knowledge trade at ω for some set of priors. The negation of threshold verifiability implies that for each $i \in I$ we have $\bigcap_{\omega'\in C(\omega)} [m_i^{\omega'}, M_i^{\omega'}] \neq \emptyset$, where $m_i^{\omega'} = \min_{\omega_0\in\Pi_i(\omega')} X(\omega_0)$ is the minimum and $M_i^{\omega'} = \min_{\omega_0\in\Pi_i(\omega')} X(\omega_0)$ is the maximum value of X given i's partition cell at ω'. We need to show that there is common knowledge trade at ω for some set of priors $\{p_i\}_{i\in I}$. For each $i \in I$, pick $k_i \in \bigcap_{\omega'\in C(\omega)} [m_i^{\omega'}, M_i^{\omega'}] \neq \emptyset$. Because X pays differently at each state, so that $X(\omega') \neq X(\omega'')$ for all $\omega', \omega'' \in \Omega$, we have that $\bigcap_{\omega'\in C(\omega)} [m_i^{\omega'}, M_i^{\omega'}]$ is not a singleton. This implies that we can choose k_i such that $k_i \in (m_i^{\omega'}, M_i^{\omega'})$ and we can find $i, j \in I$ such that $k_i \neq k_j$.

We interpret k_i as i's expected value of X, which is constant for all $\omega' \in C(\omega)$. Using the following procedure, we construct, for each $i \in I$, a prior p_i that generates k_i as the expected value of X, given each partition cell $\Pi_i(\omega')$, $\omega' \in C(\omega)$. Given $\omega' \in C(\omega)$, we have that $k_i \in (m_i^{\omega'}, M_i^{\omega'})$. This implies that we can find a posterior $p_i^{\omega'}$ with full support on $\Pi_i(\omega')$, such that $E_{p_i^{\omega'}}[X] = k_i$. This is true for all partition cells within $C(\omega)$. Let $\mathcal{P}_\omega^i$ be the collection of these generated posteriors. By assigning positive weights $\pi(\omega')$ to posteriors $p_i^{\omega'} \in \mathcal{P}_\omega^i$ that add up to 1, we construct the prior $p_i = \sum_{p_i^{\omega'}\in\mathcal{P}_\omega^i} \pi(\omega') p_i^{\omega'}$ for agent i. Note that there are infinitely many such priors. Each k_i is constant across all partition cells in $C(\omega)$, hence the expected values of X are common knowledge. Because $k_i \neq k_j$ for some $i, j \in I$, there is common knowledge trade ω. □

The theorem specifies that if threshold verifiability fails, then there is common knowledge trade for some set of priors. However, the proof provides a stronger result, that there is common knowledge trade for infinitely many sets of priors. To provide some intuition, note that if threshold verifiability fails at ω, then for each $i \in I$ we have $\bigcap_{\omega'\in C(\omega)} [m_i^{\omega'}, M_i^{\omega'}] \neq \emptyset$, where $m_i^{\omega'} = \min_{\omega_0\in\Pi_i(\omega')} X(\omega_0)$ is the minimum and $M_i^{\omega'} = \min_{\omega_0\in\Pi_i(\omega')} X(\omega_0)$ is the maximum value of X given i's partition cell at ω'. For each $i \in I$, we can pick $k_i \in \bigcap_{\omega'\in C(\omega)} [m_i^{\omega'}, M_i^{\omega'}] \neq \emptyset$, which is interpreted as agent i's expected value of X, constant across all his partition cells. If $k_i \neq k_j$ for at least two agents, then there is common knowledge trade. We can find infinitely many such vectors $\{k_i\}_{i\in I}$ by choosing different

points in the intervals $\bigcap_{\omega' \in C(\omega)} [m_i^{\omega'}, M_i^{\omega'}] \neq \emptyset, i \in I$. Moreover, each such vector $\{k_i\}_{i \in I}$ can be generated by infinitely many sets of priors, as we describe in the proof.

Note that maxmin verifiability implies no common knowledge trade, as it is stronger than threshold verifiability. The following example shows that if the security is collectively verifiable, then there can be common knowledge trade.

Example 1. Let the state space be $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4\}$ and consider two agents. Agent 1's partition is $\Pi_1 = \{\{\omega_1, \omega_2\}, \{\omega_3, \omega_4\}\}$, whereas 2's partition is $\Pi_2 = \{\{\omega_1, \omega_3\}, \{\omega_2, \omega_4\}\}$. Agent 1's prior is $p_1 = \{1/6, 1/3, 1/3, 1/6\}$ and agent 2's is $p_2 = \{1/3, 1/6, 1/6, 1/3\}$. The security is $X(\omega_1) = X(\omega_4) = 1$ and $X(\omega_2) = X(\omega_3) = -1$. It is collectively verifiable because at each state, the agents' collectively know the value of X. However, at any state ω it is common knowledge that 1's expectation of X is $-1/3$, whereas 2's expectation is $1/3$. This means that there is common knowledge trade, where 2 buys the security from 1.

3.2. We cannot disagree forever

We now analyse a dynamic trading environment, based on Geanakoplos and Polemarchakis (1982). In every period, one agent announces his expected value of the security X. Each announcement reveals some information to the other agents, who then update their own posterior beliefs. Geanakoplos and Polemarchakis (1982) show that if the agents share a common prior, they will eventually agree on their expected value of X. If priors are different, however, agents may disagree forever.

Formally, there are infinitely many periods $t = 0, 1, 2, \ldots$. At period $t = 0$ and state ω, agent i's partition cell is denoted $\Pi_i^0(\omega)$ and the public information created by the announcement is $C^0(\omega) = \Omega$. Agents make announcements sequentially. At period t, agent j announces his expected value of security X, according to his prior p_j and partition cell $\Pi_j^{t-1}(\omega) = \Pi_j^0(\omega) \cap C^{t-1}(\omega)$, which is formulated by his initial private information Π_j^0 and the public information $C^{t-1}(\omega)$ that has been revealed by all previous announcements. The public information, created by j's announcement e_t at period t, is defined as $C^t(\omega) = \{\omega' \in C^{t-1}(\omega) : \sum_{\omega'' \in \Pi_j^{t-1}(\omega')} X(\omega'') \frac{p_j(\omega'')}{p_j(\Pi_j^{t-1}(\omega'))} = e_t\}$, the set of states which are consistent with all announcements up to t.

After each announcement, all other agents update their own information, by excluding any states that would not result in agent j making this announcement. Because the state space is finite, this process of updating of information will eventually stop. Suppose that this happens in period t^*. This means that each agent j will make the same announcement e_j at all states in $C^{t^*}(\omega)$.[7] If they agree on their announcements, we say that they cannot disagree forever.

Definition 6. Agents cannot disagree forever at ω if at t^* we have $e_i = e_j$ for all $i, j \in I$.

Is threshold verifiability of X at $t = 0$ and ω, or even maxmin verifiability, sufficient for no disagreement? We show by example that it is not.

Example 2. Let the state space be $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$ and consider two agents. Agent 1's partition is $\Pi_1 = \{\{\omega_1, \omega_2\}, \{\omega_3, \omega_4\}, \{\omega_5\}\}$, whereas 2's partition is $\Pi_2 = \{\{\omega_1, \omega_3\}, \{\omega_2, \omega_4, \omega_5\}\}$. Agent 1's prior is $p_1 = \{1/12, 1/6, 1/6, 1/2, 1/2\}$ and agent 2's is $p_2 = \{1/6, 1/12, 1/12, 1/6, 1/2\}$. The security is $X(\omega_1) = X(\omega_4) = 1$, $X(\omega_2) = X(\omega_3) = -1$ and $X(\omega_5) = 5$. The security is maxmin, and therefore partially, verifiable because at any state ω, $C(\omega) = \Omega$ and agent 1 knows the maximum value of X at ω_5.

From Theorem 1, we know that there is no common knowledge trade at $t = 0$. However, it is straightforward to show that there can be disagreement and trade in a dynamic setting. If the true state is $\omega \neq \omega_5$, agent 1 does not announce 5, which informs agent 2 that the state is not ω_5. By excluding state ω_5, the partitions and the posteriors are updated so that the example becomes identical to Example 1. Then, agent 1 announces 1/3 and agent 2 announces -1/3, so that there is no more updating and there is common knowledge trade and disagreement forever.

Disagreement and trade are possible because maxmin verifiability in period t does not imply maxmin verifiability at $t + 1$. The reason is that even if the maximum (or minimum) value of $X(C^t(\omega))$ is verified, this may not be true for $X(C^{t+1}(\omega))$. In Example 2, the maximum value 5 is verified at $t = 0$ but at $t = 1$ neither the maximum 1, nor the minimum -1, are verified. In contrast, a common prior at t continues to be common at $t + 1$, as long as all agents use Bayes' rule, hence the result of Geanakoplos and Polemarchakis (1982), that agents cannot disagree forever. In order to preclude trade in our environment, we need threshold verifiability at period t^*, which is the period after which there is no more updating of information by anyone. Because at t^* the announcement of each agent is constant in $C^{t^*}(\omega)$, threshold verifiability implies that $X(C^{t^*}(\omega))$ is constant. We therefore have the following Corollary.

Corollary 1. *If at ω and t^* security X is threshold verifiable, then agents cannot disagree forever at ω.*

[7] If he was not making the same announcement, then at some $t > t^*$ the public information $C^{t^*}(\omega)$ would further shrink, contradicting that the updating of information has stopped.

3.3. Information aggregation

The question of no trade is closely related to the question of whether a security can aggregate information, so that the price always converges to its true value. In this section we model trading using the market scoring rule, which is also used in prediction markets. Trading is organised as follows. At $t = 0$, nature selects a state $\omega \in \Omega$ and the uninformed market maker makes a prediction y_0 about the value of security $X : \Omega \to \mathbb{R}$. At $t = 1$, agent 1 makes a revised prediction y_1, at $t = 2$ agent t_2 makes his prediction, and so on. At $t = n + 1$, agent 1 makes another prediction y_{n+1}. Each prediction y_k is required to be within the set $Y = [\min_{\omega\in\Omega} X(\omega), \max_{\omega\in\Omega} X(\omega)]$.

The agents' payoffs are computed using a scoring rule, $s(y, x^*)$, where x^* is the true value of the security and y is a prediction. A scoring rule is *proper* if, for any probability measure p and any random variable X, the expectation of s is maximised at $y = E_p[X]$. It is *strictly proper* if y is unique. We focus on continuous strictly proper scoring rules. Examples are the quadratic, where $s(y, x) = -(x - y)^2$, and the logarithmic, where $s(y, x) = (x - a)ln(y - a) + (b - x)ln(b - y)$ with $a < \min_{\omega\in\Omega} X(\omega), b > \max_{\omega\in\Omega} X(\omega)$. A agent's payoff from announcing y_t at t, is $s(y_t, x^*) - s(y_{t-1}, x^*)$, where y_{t-1} is the previous announcement and x^* is the true value of the security.

We assume that each agent is myopic, so that he cares only about the current payoff, when making an announcement. Because scoring rules are strictly proper and agents are myopic, their announcement will always be their expected value of X. Hence, this model is closely related to the model of the previous section. We say that information gets aggregated if the agents' predictions converge to the true value of the security, $X(\omega)$.

Definition 7. Information gets aggregated at ω if sequence $\{y_k\}_{k=1}^{\infty}$ converges in probability to random variable $X(\omega)$.

Ostrovsky (2012) and Chen et al. (2012) show that, with common priors, information gets aggregated at all states if and only if the security is separable.[8] This means that if the security is not separable, it is possible that agents agree on its expected value, but this is different from its true value at ω.

In the previous section, we showed that threshold verifiability at t^* is strong enough to imply agreement. Moreover, it implies that $X(C^{t^*}(\omega))$ is constant. Because there is only one value of X that is possible, it must be the correct one and we have information aggregation. It is important to note that this result holds for all securities, not just the separable ones.

Corollary 2. *If security X is threshold verifiable at t^* and ω, then there is information aggregation at ω.*

3.4. Multiple securities

In the current model, only one security, X, is traded. In this section, we discuss how trading can be generalised to multiple securities, $\{X_i\}_{i\in I}$, one for each agent, so that $\sum_{i\in I} X_i = 0$. First, we fix the set of priors and show that common knowledge trade with X implies common knowledge trade with $\{X_i\}_{i\in I}$. Suppose, without loss of generality, that the only common knowledge event is the whole state space Ω. Then, our definition of common knowledge trade with X is that each agent i's expected value given each of his partition cells is e_i, yet $e_i \neq e_j$ for at least two agents. If $e_i > e_j$, then Agent i is willing to buy the security from Agent j at some intermediate price $e_i > p > e_j$. We can model this trade by having two new securities, $X_i = X - \mathbf{p}$ and $X_j = -X + \mathbf{p}$, where $\mathbf{p}$ is the security that pays p at all states, so we have $X_i + X_j = \mathbf{0}$. Both agents have strictly positive expected value from their respective securities, and this trade is feasible because the two securities add up to 0 at all states.

The two approaches are complementary. We can view X as the 'fundamental' asset which pays according to the state (e.g. the value of the oil well), whereas securities X_i, X_j denote the actual trade that has been agreed. With n agents, where n is even, we can order $e_1 > e_2 > \ldots > e_n > 0$. By setting p such that $e_{n/2} > p > e_{n/2+1}$, we can define $X_i = X - \mathbf{p}$ for $i \leq n/2$ and $X_i = -X + \mathbf{p}$ otherwise. We then have common knowledge trade with multiple securities. The converse is not necessarily true. To see this, suppose that $\{X_i\}_{i\in I}$ satisfy common knowledge trade with multiple securities. We can define $X = \sum_{j\in I} \lambda_j X_i$, so we need to find $\lambda = \{\lambda_1, \ldots, \lambda_n\}$ such that $\sum_{j\in I} \lambda_j E_{p_i}[X_j|\Pi_i(\omega)] = e_i$, for all $\omega \in \Omega$ and $i, j \in I$. As there are many more equations than unknowns, the system may not have a solution.

We now allow for all possible priors and extend our analysis to multiple securities. We say that a collection $\{X_i\}_{i\in I}$ of securities is tradable if they add up to zero at all states, $\sum_{i\in I} X_i = 0$, so that the trade is feasible, and every Agent i's maximum value of X_i given each of his partition cells is strictly positive. If the last condition was not satisfied for some partition cell, then the expectation of X_i would be negative for all priors, hence Agent i would not agree to participate in the trade.

Definition 8. Securities $\{X_i\}_{i\in I}$ are tradable if $\sum_{i\in I} X_i = 0$ and $\max_{\omega_0\in\Pi_i(\omega)} X(\omega_0) > 0$, for all $i \in I$ and $\omega \in \Omega$.

We say that there is common knowledge trade given a collection of tradable securities if it is common knowledge that each Agent i's expected value of X_i is $e_i > 0$.

[8] Ostrovsky (2012) characterises this class of separable securities, which includes the Arrow-Debreu securities.

Definition 9. There is common knowledge trade at ω (with tradable securities $\{X_i\}_{i\in I}$) if the event "agent i's expectation of X_i is $e_i > 0$, for all $i \in I$" is common knowledge at ω.

Note that e_i in this definition denotes the expected profits of Agent i, whereas e_i in the original definition denotes i's expected value of X. Samet (1998) uses a weaker definition, which only requires that the expectations are strictly positive. He shows that there is a common prior that generates a given collection of posterior beliefs, one for each agent and his partition cells, if and only if there is no common knowledge trade with multiple securities.

We extend threshold verifiability in a similar way.

Definition 10. Tradable securities $\{X_i\}_{i\in I}$ are threshold verifiable at ω if, whenever $X_i(C(\omega))$ is not constant for some $i \in I$, there exist $i \in I$ and $\omega', \omega'' \in C(\omega)$ such that $\max_{\omega_0 \in \Pi_i(\omega')} X_i(\omega_0) < x < \min_{\omega_0 \in \Pi_i(\omega'')} X_i(\omega_0)$, for some $x \in \mathbb{R}$.

We finally have the following Proposition, which is an extension of Theorem 1. The proof is almost identical so it is omitted.[9]

Proposition 1. *Tradable securities $\{X_i\}_{i\in I}$ are threshold verifiable at ω if and only if there is no common knowledge trade at ω, for any set of priors.*

Declaration of competing interest

I would like to confirm that there are no declarations of interest.

Data availability

No data was used for the research described in the article.

References

Abadi, J., Brunnermeier, M., 2018. Blockchain economics. Technical report. National Bureau of Economic Research.

Abernethy, J., Chen, Y., Vaughan, J.W., 2013. Efficient market making via convex optimization, and a connection to online learning. ACM Trans. Econ. Comput. 1 (2), 1–39.

Abernethy, J.D., Frongillo, R.M., 2012. A characterization of scoring rules for linear properties. In: Conference on Learning Theory. In: JMLR Workshop and Conference Proceedings, pp. 27.1–27.13.

Athey, S., Parashkevov, I., Sarukkai, V., Xia, J., 2016. Bitcoin pricing, adoption, and usage: theory and evidence. Mimeo.

Aumann, R., 1976. Agreeing to disagree. Ann. Stat. 4, 1236–1239.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C., 2019. The blockchain folk theorem. Rev. Financ. Stud. 32 (5), 1662–1715.

Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: economics, technology, and governance. J. Econ. Perspect. 29 (2), 213–238.

Bonanno, G., Nehring, K., 1999. How to make sense of the common prior assumption under incomplete information. Int. J. Game Theory 28 (3), 409–434.

Brunnermeier, M.K., 2001. Asset Pricing Under Asymmetric Information: Bubbles, Crashes, Technical Analysis, and Herding. OUP, Oxford.

Brunnermeier, M.K., Pedersen, L.H., 2005. Predatory trading. J. Finance 60 (4), 1825–1863.

Budish, E., 2018. The economic limits of bitcoin and the blockchain. Technical report. National Bureau of Economic Research.

Cai, F., 2003. Was there front running during the ltcm crisis? Available at SSRN 385560.

Chen, X., Papadimitriou, C., Roughgarden, T., 2019. An axiomatic approach to block rewards. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, pp. 124–131.

Chen, Y., Ruberry, M., Vaughan, J.W., 2012. Designing informative securities. arXiv preprint. arXiv:1210.4837.

Dimitrov, S., Sami, R., 2008. Non-myopic strategies in prediction markets. In: Proceedings of the 9th ACM Conference on Electronic Commerce, pp. 200–209.

Easley, D., O'Hara, M., Basu, S., 2019. From mining to markets: the evolution of bitcoin transaction fees. J. Financ. Econ. 134 (1), 91–109.

Feinberg, Y., 2000. Characterizing common priors in the form of posteriors. J. Econ. Theory 91 (2), 127–179.

Frongillo, R., Waggoner, B., 2017. An axiomatic study of scoring rule markets. arXiv preprint. arXiv:1709.10065.

Galanis, S., 2013. Unawareness of theorems. Econ. Theory 52 (1), 41–73.

Galanis, S., 2018. Speculation under unawareness. Games Econ. Behav. 109, 598–615.

Galanis, S., Ioannou, C.A., Kotronis, S., 2024. Information aggregation under ambiguity: theory and experimental evidence. Rev. Econ. Stud. 91 (6), 3423–3467.

Galanis, S., Kotronis, S., 2021. Updating awareness and information aggregation. B.E. J. Theor. Econ. 21, 613–635.

Galanis, S., Mikhalishchev, S., 2025. Information aggregation with costly information acquisition. Mimeo.

Garratt, R., Monnet, C., 2022. An impossibility theorem on truthful reporting in fully decentralized systems. Available at SSRN 4017963.

Geanakoplos, J., 1989. Game theory without partitions, and applications to speculation and consensus. Cowles Foundation Discussion Paper, No. 914.

Geanakoplos, J., 1992. Common knowledge. J. Econ. Perspect. 6 (4), 53–82.

Geanakoplos, J., Polemarchakis, H., 1982. We can't disagree forever. J. Econ. Theory 28, 192–200.

Goel, N., Filos-Ratsikas, A., Faltings, B., 2019. Decentralized oracles via peer-prediction in the presence of lying incentives. Mimeo.

Halpern, J.Y., 2002. Characterizing the common prior assumption. J. Econ. Theory 106 (2), 316–355.

Hanson, R., 2003. Combinatorial information market design. Inf. Syst. Front. 5 (1), 107–119.

Hanson, R., 2007. Logarithmic market scoring rules for modular combinatorial information aggregation. J. Predict. Mark. 1 (1), 3–15.

Heifetz, A., Meier, M., Schipper, B.C., 2013. Unawareness, beliefs, and speculative trade. Games Econ. Behav. 77, 100–121.

[9] Note that we do not require that each X_i pays differently across states, as in the proof of Theorem 1. The reason is that $e_i = e_j$ is allowed here, as they are the expected profits, not the agents' expected value of X.

Hinzen, F.J., John, K., Saleh, F., 2019. Proof-of-work's limited adoption problem. NYU Stern School of Business.
Jurca, R., Faltings, B., 2006. Robust incentive-compatible feedback payments. In: Agent-Mediated Electronic Commerce. Automated Negotiation and Strategy Design for Electronic Markets. Springer, pp. 204–218.
Karam, A., Bogoev, D., 2023. Intraday momentum trading and liquidity crises. Working paper.
Meier, M., Schipper, B.C., 2014. Speculative trade under unawareness: the infinite case. Econ. Theory Bull. 2 (2), 147–160.
Milgrom, P., Stokey, N., 1982. Information, trade, and common knowledge. J. Econ. Theory 26, 17–27.
Miller, N., Resnick, P., Zeckhauser, R., 2005. Eliciting informative feedback: the peer-prediction method. Manag. Sci. 51 (9), 1359–1373.
Morris, S., 1994. Trade with heterogeneous prior beliefs and asymmetric information. Econometrica 62 (6), 1327–1347.
Ng, M.-C., 2003. On the duality between prior beliefs and trading demands. J. Econ. Theory 109, 39–51.
Ostrovsky, M., 2012. Information aggregation in dynamic markets with strategic traders. Econometrica 80 (6), 2595–2647.
Othman, A., Sandholm, T., 2011. Liquidity-sensitive automated market makers via homogeneous risk measures. In: International Workshop on Internet and Network Economics. Springer, pp. 314–325.
Prelec, D., 2004. A Bayesian truth serum for subjective data. Science 306 (5695), 462–466.
Radanovic, G., Faltings, B., Jurca, R., 2016. Incentives for effort in crowdsourcing using the peer truth serum. ACM Trans. Intell. Syst. Technol. 7 (4), 48.
Samet, D., 1998. Common priors and separation of convex sets. Games Econ. Behav. 24, 172–174.
Schilling, L., Uhlig, H., 2019. Some simple bitcoin economics. J. Monet. Econ. 106, 16–26.
Schlegel, J.C., Kwaśnicki, M., Mamageishvili, A., 2022. Axioms for constant function market makers. Available at SSRN.
Witkowski, J., Parkes, D.C., 2012a. Peer prediction without a common prior. In: Proceedings of the 13th ACM Conference on Electronic Commerce. ACM, pp. 964–981.
Witkowski, J., Parkes, D.C., 2012b. A robust Bayesian truth serum for small populations. In: Twenty-Sixth AAAI Conference on Artificial Intelligence.
Wolfers, J., Zitzewitz, E., 2004. Prediction markets. J. Econ. Perspect. 18 (2), 107–126.