14.462
Spring, 2020

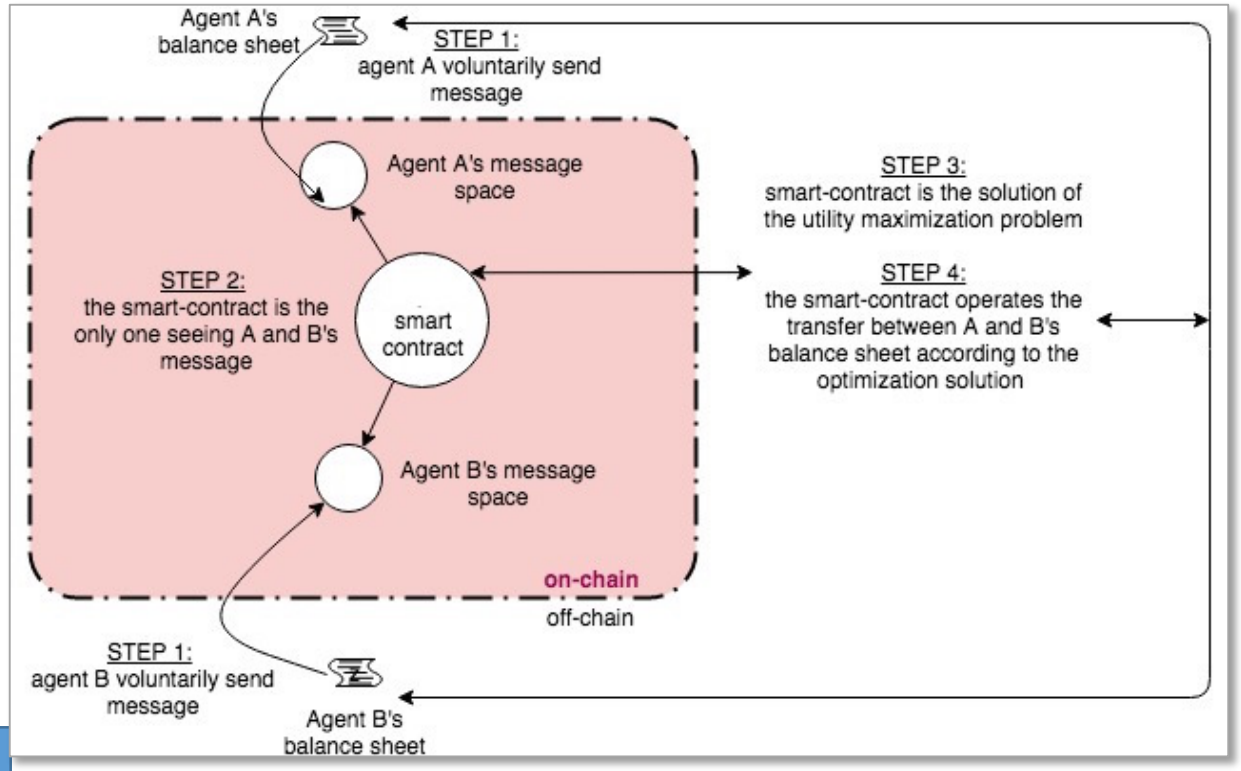
Encryption and Validation Protocols vs. Smart Contracts and Mechanism Design (Lecture 4)

Robert M. Townsend

Elizabeth & James Killian Professor of Economics, MIT

Massachusetts Institute of Technology

Hybrids: On- and Off-Chain, Quasi-Private



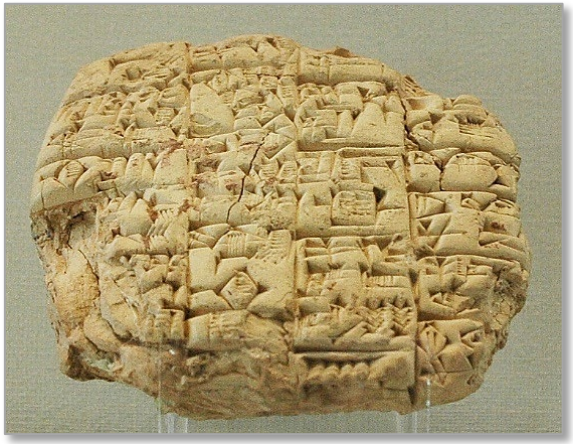
Nicholas Zhang (2019)

No planner, but then Compiling and verify code on-chain is incredible costly.
Solution is do some things off-chain-
Entire documents can be encrypted off-chain and accessed as reliable
Messages, states in contract can be separate from ledgers for transfer of value
Multiparty computation, share partial information, know system is functioning properly
But in practice, mpc technology is still limited, hence quasi private, not going to extremes

Encryption Through History: Mesopotamia Tokens

(Fig. 1) Tokens from Tepe Gawra, present day Iraq, ca. 4000 BC.
. cone, sphere, and flat disk are three measures of cereals: small, larger ,largest.
. tetrahedron is a unit of work (one man/one day?).

(Fig. 2) Tokens from Tello, ancient Girsu, present day Iraq, ca. 3300 BC.
Starting above from left to right : 1 length of textile, one jar of oil, – ? –, one measure of wheat.
Continuing below from right to left: one ram, one length of rope, 1 ingot of metal, 1 garment.

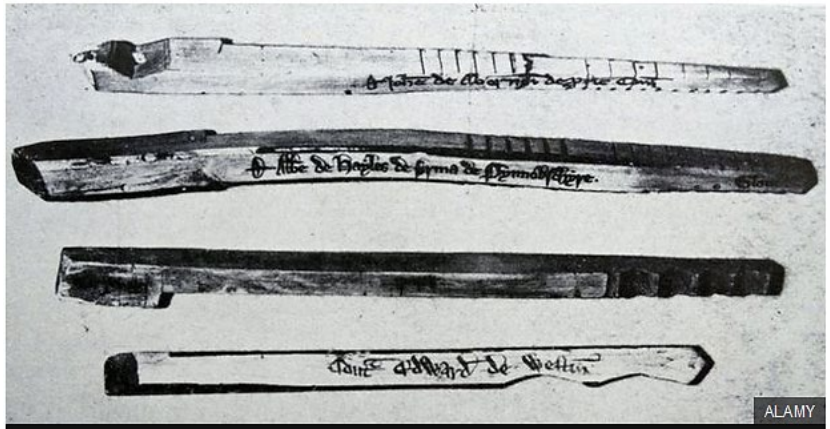


(Fig. 3)

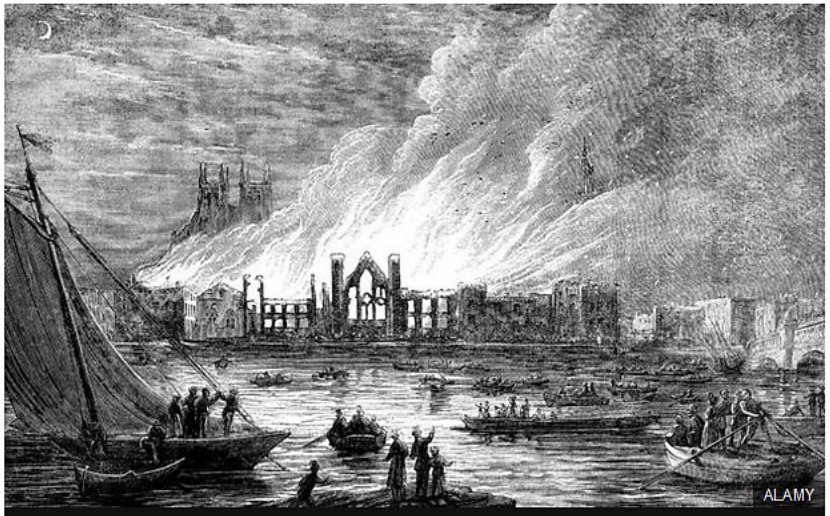
- Mesopotamia: Tokens put in clay envelopes for shipping goods as a manifest
  - Sealed – so tampering with one, the actual or the other, the message, would be obvious
  - If the sender and receiver of the shipment trusted each other, they could be sure there was no tampering by not-trusted parties in between. Tampering of the invoice or theft of the shipment that took place in between would be evident
    - Writing on envelopes is developed, as an ultimate message system

Tally Sticks: Medieval England

- The stick would be split in half, down its length from one end to the other, debtor vs. creditor
- Because willow has a natural and distinctive grain, the two halves would match only each other
- The original borrower was trusted to repay, while the tally stick provided a trustless record of the promise to original lender and then to third parties, a record to the borrower that the holder was presenting the original claim (no double presentation of debt).
- PS: decision to convert to paper and burn the sticks, fire destroyed the houses of parliament



Some of the old wooden tally sticks used by the UK Exchequer until 1826



A decision to burn the obsolete tally sticks in 1834 nearly destroyed the Palace of Westminster

Contemporary, Private and Public Keys, Yet the Double-Spend Problem Emerges

- Public and private keys ensure no one can transact on someone else's ID, impersonating a node.
- Because the message or transaction can only be created with the key combination, it is known the spender wishes to unlock and spend the coin.
- This brings commitment to the transaction, so it cannot be undone or reneged upon later.
- Double spending would be possible if two messages from a given node were able to spend the same coin. With internet latency, hard to know which transaction came first and should be valid, as time stamps are not necessarily chronological
- Solutions in CS: based on Distributed Computing

Which Brings Us to Consensus Protocols

- Validators in a network must achieve consensus, approve next block of transactions (block chain)
- Bitcoin and Ethereum use Proof of Work (PoW) in which nodes in a network compete with computing power to solve cryptographic math puzzles and reach consensus- effectively randomizing who validates
- Practical Byzantine Fault Toleration (PBFT) chooses a leader in round-robin fashion
  - Nodes need to agree on a "membership list" of nodes to select from, picked by the company
  - Centralized consensus is achieved when over 66% of the nodes agree
- Proof of Stake (PoS): The selected validators that suggest the next block for approval are chosen at random, followed by multi-round voting mechanisms with weights based on coin ownership
- Federated Byzantine Agreement (FBA): Each entity names others it trusts, trust networks need not overlap
  - Stellar's FBA is free entry or open membership into validation
- Issues with these protocols is subject of next section

A Bit More on Bitcoin

- One potential problem is that nodes as bad actors could violate the protocol and propose the latest version of the ledger that they would like to become immutable, e.g., knowingly containing the second of the double-spend transactions, while the first was already used to acquire something else. To thwart this, under the Bitcoin system, it is again as if one node were selected at random to certify a current new candidate ledger. There are thus two keys to Bitcoin. One, this certification requires time and energy. A proof-of-work algorithm requires a selectable amount of work to find the random number that, when added to the set of transactions, creates the hash. Difficulty is controlled. The discovered random number is then added to the bottom of the block as the proof of puzzle solved, a certification of work done that all can confirm easily. The work, costly use of electricity and equipment, limits entry into validation. The second key to Bitcoin, and, a premise of computer science more generally, is that most nodes are honest so the de facto randomly-selected miner is likely to be honest and follow the protocol.
- Temporary multiplicity or fraud is possible if another branch containing new blocks is created. But the conventional protocol is that the longest interim chain is considered to be the valid one. To reinforce this, and not incidentally, here Satoshi Nakamoto put some economics into the design of the computer science protocol. Miners have incentives to mine the longest chain, as they are rewarded in Bitcoin only if the block of transactions they validate becomes, eventually, part of the immutable history. To repeat in crude terms: validators now have pecuniary interests in the outcomes they are validating.

Morris and Shin (1997) "Approximate Common Knowledge and Co-ordination: Recent Lessons from Game Theory"

Halpern and Moses (1990)

Two divisions of an army, each commanded by a general, are camped on two hilltops overlooking a valley. In the valley awaits the enemy. The commanding general of the first division has received a highly accurate intelligence report informing him of the state of readiness of the enemy. It is clear that if the enemy is unprepared and both divisions attack the enemy simultaneously at dawn, they will win the battle, while if *either* the enemy is prepared *or* only one division attacks it will be defeated. If the first division general is informed that the enemy is unprepared, he will want to coordinate a simultaneous attack. But the generals can communicate only by means of messengers and, unfortunately, it is possible that a messenger will get lost or, worse yet, be captured by the enemy.

probabilistic version of the co-ordinated attack problem

Suppose now that with probability $\delta > 0$ the enemy is prepared, while with probability $1 - \delta$ the enemy is unprepared. Recall that the first division general knows which of these two contingencies is true, while the second division general does not. We will consider the same communication protocol outlined above, except

now we assume that each messenger gets lost with independent probability $\varepsilon > 0$. We will be focusing on the case where ε is small and in particular is smaller than δ. We will make the unrealistic assumption that there is no upper bound on the

a message will be lost eventually). Now the environment can be described by a *state space* as in Table I.

Thus state (n, m) refers to a situation where the first division general has sent n messages (but does not know whether his last message arrived or not), while the second division general has sent m messages (and similarly does not know whether his last message arrived or not). Note that the infinite sum of the probabilities is

Table I. The naive communication protocal state space.

State	Enemy's preparedness	Probability
$(0, 0)$	Prepared	δ
$(1, 0)$	Unprepared	$(1-\delta)\varepsilon$
$(1, 1)$	Unprepared	$(1-\delta)(1-\varepsilon)\varepsilon$
$(2, 1)$	Unprepared	$(1-\delta)(1-\varepsilon)^2\varepsilon$
...	...	...

Suppose that a successful attack has a payoff of 1 for the generals, while an attack that is unsuccessful (either because the enemy is prepared or only one division attacks) has a payoff of $-M$, where M is a very large number. Both generals not attacking has a payoff of 0. These payoffs capture the qualitative feature underlying

Theorem:

- If the communication system is sufficiently reliable, then the optimal action protocol has co-ordinated attack almost always occurring when the enemy is unprepared.

The optimal action protocol, given the naive communication protocol and ε sufficiently small, has the first division general attacking whenever the enemy is unprepared (even if he has not received any message confirmation from the second division general); while the second division general attacks even if he has received only one message from the first division general.* Thus co-ordinated attack occurs with probability $(1-\delta)(1-\varepsilon)$. In fact, this can be achieved under any

* To illustrate this claim, consider three action protocols. (1) If the first division general attacks whenever the enemy is unprepared and the second division general always attacks, the expected payoff is $\delta(-M)+(1-\delta)(1) = 1-(M+1)\delta$. (2) If the first division general attacks whenever the enemy is unprepared, and the second division general attacks if he has received at least one message, the expected payoff is $(1-\delta)\varepsilon(-M)+(1-\delta)(1-\varepsilon)(1) = (1-\delta)(1-(M+1)\varepsilon)$. (3) If each general attacks if he has received at least one message, the expected payoff is $(1-\delta)(1-\varepsilon)(1-(M+1)\varepsilon)$. Protocol (2) is better than protocol (3) if $\varepsilon < (1/M+1)$. Protocol (2) is better than protocol (1) if $\varepsilon < (\delta/1-\delta)(M/M+1)$. Thus protocol (2) is better than protocols (1) and (3) for all ε sufficiently small. Similar arguments show that protocol (2) is better than *all* alternative protocols.

$$[(1-\delta)(1-\varepsilon)(1-\varepsilon)]1 + [(1-\delta)(1-\varepsilon)\varepsilon] \times (-M)$$

The analysis of this section showed that if the objective is only to achieve "co-ordination with high probability" and agents are not strategic, then it is enough that the communication system is usually accurate.

go away. A remaining difficulty is that the optimal action protocol turns out to be sensitive to *strategic concerns*. The optimal action protocol described is optimal as long as the generals can be relied on to choose to follow it. Perhaps their battle orders instruct them to follow that protocol and generals always follow their battle orders. But suppose that the first division general knows that the enemy is unprepared, sends a message to the second division general, but receives no confirmation. He then believes with probability $1/(2-\varepsilon)$ that his own message never arrived, and thus that the second division general will not attack. For all ε, this probability is more than $1/2$. Perhaps he would be tempted not to commit his division to the battle in these circumstances. Anticipating this possibility, the second division general may hesitate to attack if he has not received a re-confirmation from the first division general. The unraveling argument may start all over again.

$$\frac{\varepsilon}{\varepsilon+(1-\varepsilon)\varepsilon}=\frac{\varepsilon}{2\varepsilon-\varepsilon^2}=\frac{1}{2-\varepsilon}>\frac{1}{2}$$

To understand this argument formally, we must treat the situation as an "incomplete information game" played between the two generals.* It is a game because each general, in seeking to maximize his expected payoff, must take into account the action of the other general. There is incomplete information because under the

so now we must specify the generals' payoffs. Suppose that each general gets a payoff of 0 if his division does not attack. If his division participates in a successful attack, he gets a payoff of 1; if his division participates in an unsuccessful attack (either because the enemy is prepared or the other division does not attack), he gets a payoff of $-M$. Thus if the enemy is in fact prepared (i.e., the state is $(0, 0)$), the payoffs can be represented by the matrix as in Table II.

Table II. Payoffs if the enemy is prepared.

	Attack	Don't attack
Attack	$-M, -M$	$-M, 0$
Don't attack	$0, -M$	$0, 0$

Table III. Payoffs if the enemy is unprepared.

	Attack	Don't attack
Attack	$1, 1$	$-M, 0$
Don't attack	$0, -M$	$0, 0$

- In the strategic co-ordinated attack problem with the naive communication protocol, both generals *never* attack if the communication system is sufficiently reliable.

The argument is as follows. Clearly the first division general will never attack if he knows the enemy is prepared. Now suppose $\varepsilon < \delta$ and the second division general never receives a message. He believes that with probability $\delta/(\delta + (1 - \delta)\varepsilon) > 1/2$, the enemy is prepared. Whatever he believes the first division general will do if the enemy were unprepared, his optimal action must be not to attack:

not attacking gives a payoff of 0, while attacking gives an expected payoff of at most $(1/2)(-M) + (1/2)(1) = -(M - 1)/2$ (recall that M is very large, and in particular greater than 1).

Now the first division general knows that the second division general will never attack if he does not receive any messages (i.e., in states $(0, 0)$ and $(1, 0)$). Suppose that the first division general knows that the enemy is unprepared (and so sends a message) but never receives a confirmation from the second division general. Thus the first division general believes the true state is either $(1, 0)$ or $(1, 1)$. He believes that with probability

$$\frac{(1-\delta)\varepsilon}{(1-\delta)\varepsilon + (1-\delta)\varepsilon(1-\varepsilon)} = \frac{1}{2-\varepsilon} > \frac{1}{2},$$

the second division general did not receive any message (i.e., the true state is $(1, 0)$) and so will not attack. By the same argument as before, this ensures that the first division general will not attack even if he knows the enemy is unprepared, but has received any confirmation. An unraveling argument ensures

Table V. An equilibrium action protocol under the simple communication protocol.

State	Enemy's preparedness	Probability	First division general's action	Second division general's action
No message	Prepared	δ	Don't attack	Don't attack
Message sent but not received	Unprepared	$(1-\delta)\varepsilon$	Attack	Don't attack
Message sent and received	Unprepared	$(1-\delta)(1-\varepsilon)$	Attack	Attack

The strong conclusion of the previous section, that co-ordinated attack never occurs, is *not* robust to the communication protocol. The generals would indeed be exceptionally foolish to attempt to co-ordinate their attack using the naive communication protocol. Consider the following "simple communication protocol". Suppose that if the enemy is unprepared, the first division general sends one message to the second division general informing him of this state of affairs. The second division general sends *no* confirmation. This communication protocol gives rise to the state space as in Table IV.

- For sufficiently small ε, there exists an equilibrium of the strategic co-ordinated attack problem with the simple communication protocol where co-ordinated attack almost always occurs whenever the enemy is unprepared.

A Review of Some Arguments in Mechnism Design

- Messages
- Multiperiod tie ins
- Costly state verification
- Limited committment

Risk Sharing with Private Information on Crop Output

- Thus, imagine a pure exchange economy with one period; two agents, named 1 and 2; and a K-dimensional vector of goods as endowments.
- The endowment of agent 1, $e^1(\varepsilon)$, is seen by agent 1 alone. That is, shocks are private to agent 1
- Let agent 1's endowment be denoted parameter θ in some set Θ, realized with probability $p(\theta)$. Agent 1 is the stand-in for the villa
- Agent 2's endowment is presumed to be public, for simplicity, some constant K-dimensional vector W. Agent 2 is the stand-in for the central monastery.
- Agents 1 and 2 agree ex ante to some resource allocation rule $f(m)$ specifying a K-dimensional vector of commodity transfers from agent 1 to agent 2 given some message m sent by villa 1 to monastery 2, message m in a set of *a priori* feasible messages, M.
- Under this resource allocation scheme, villa 1 waits to see output vector θ before sending message m. Thus its decision problem is of the form, for every $\theta \in \Theta$, maximize $U^1[\theta - f(m)]$ by choice of $m \in M$

- Suppose there exists a unique maximizing solution to this problem, denoted $m^*(\theta)$. Then, given θ,

$$U^1\{\theta - f[m^*(\theta)]\} \geq U^1[\theta - f(m)] \tag{83}$$

for all possible messages $m \in M$.

- Evaluating the right hand side of (83) at $m^*(\widetilde{\theta})$, the maximizing message agent 1 would have sent if his endowment vector had been $\widetilde{\theta}$ even though it is θ,

$$U^1\{\theta - f[m^*(\theta)]\} \geq U^1\{\theta - f[m^*(\widetilde{\theta})]\} \tag{84}$$

- Now consider an *alternative* scheme in which villa 1 announces a value for its endowment vector directly, some arbitrary value of $\widetilde{\theta}$ in Θ, so that the message space is now the space of output possibilities Θ instead of arbitrary message space M (truth telling is not required).

- Suppose announced $\widetilde{\theta}$ effects transfers $g(\widetilde{\theta}) \equiv f[m^*(\widetilde{\theta})]$, so that the transfer function is the direct function $g(\bullet)$ rather than the composite function $f(\bullet)$.
- Transfer function $g(\bullet)$ define a new mechanism.
- By substitution of the notation of $g(\bullet)$ into (84), at any particular $\theta \in \Theta$, and for all alternative values $\widetilde{\theta} \in \Theta$,

$$U^1[\theta - g(\theta)] \geq U^1[\theta - g(\widetilde{\theta})] \tag{85}$$

- It is apparent from (85) that in the alternative mechanism, with message space Θ and transfer function $g(\bullet)$, villa 1 would "tell the truth," though, again, it is not required to do so.
- Announced values θ would coincide with actual values θ.
- Further, a parameter draw of θ thus would effect transfer $g(\theta) \equiv f[m^*(\theta)]$, so that the outcome under the original scheme would be sustained. Object $g(\theta)$ may be thought of as a parameter-contingent allocation, with θ now playing the role of the actual parameter value.

- **Program 7**: Maximize by choice of the lotteries $\pi(\tau|\theta)$ the objective function

$$\lambda^1 \left(\Sigma_\theta p(\theta) \Sigma_\tau U^1[\theta - \tau] \pi(\tau \mid \theta) \right) + \lambda^2 \left(\Sigma_\theta p(\theta) \Sigma_\tau U^2[W + \tau] \pi(\tau \mid \theta) \right) \tag{93}$$

subject to incentive constraints, for every actual value θ and counterfactual $\widetilde{\theta}$

$$\Sigma_\tau U^1[\theta - \tau] \pi(\tau \mid \theta) \geq \Sigma_\tau U^1[\theta - \tau] \pi(\tau \mid \widetilde{\theta}) \tag{94}$$

- Constraints (94) can again be derived as endogenous
- Program 7 is concave so its solution can be easily characterized. In fact, Program 7 is a linear program, so that solutions can be computed numerically.
- The only binding constraint would have high-θ agents claiming on the margin to be low-θ agents, so we would not need to worry about the feasibility of low-θ agents claiming to be high anyway. With multiple goods, however, there remains the possibility that something can be accomplished with pretransfer displays.

Optimal Multiperiod Tie-ins-2

- **Program 8**: Maximize by choice of lotteries over transfers τ at date 1, $\pi_1(\tau|\theta_1)$, and lotteries over transfers τ at date 2, $\pi_2(\tau|\theta_1,\theta_2)$, the objective function

$$\begin{aligned}
&\lambda^1(\Sigma_{\theta_1} p(\theta_1)\Sigma_\tau U^1[\theta_1-\tau]\pi_1(\tau\mid\theta_1)\\
&+\beta\Sigma_{\theta_1} p(\theta_1)\Sigma_{\theta_2} p(\theta_2\mid\theta_1)\Sigma_\tau U^1[\theta_2-\tau]\pi_2(\tau\mid\theta_1,\theta_2)) \qquad (95)\\
&+\lambda^2(\Sigma_{\theta_1} p(\theta_1)\Sigma_\tau U^2[W_1+\tau]\pi_1(\tau\mid\theta_1)\\
&+\beta\Sigma_{\theta_1} p(\theta_1)\Sigma_{\theta_2} p(\theta_2\mid\theta_1)\Sigma_\tau U^2[W_2+\tau]\pi_2(\tau\mid\theta_1,\theta_2))
\end{aligned}$$

- subject to incentive constraints at date 2, for every $\widetilde{\theta}_1$ announced at date 1, and for every actual θ_2 and announced $\widetilde{\theta}_2$ at date 2

Optimal Multiperiod Tie-ins-3

$$\Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \widetilde{\theta}_1, \theta_2)$$
$$\geq \Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \widetilde{\theta}_1, \widetilde{\theta}_2) \tag{96}$$

and the incentive constraints at date 1, for every actual θ_1 and announced $\widetilde{\theta}_1$,

$$\Sigma_\tau U^1[\theta_1 - \tau]\pi_1(\tau \mid \theta_1) + \beta\Sigma_{\theta_2} p(\theta_2 \mid \theta_1)\Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \theta_1, \theta_2)$$
$$\geq \Sigma_\tau U^1[\theta_1 - \tau]\pi_1(\tau \mid \widetilde{\theta}_1) + \beta\Sigma_{\theta_2} p(\theta_2 \mid \theta_1)\Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \widetilde{\theta}_1, \theta_2) \tag{97}$$

- Constraint (96) ensures that agent 1 will tell the truth at date $t = 2$ no matter what happened or what was announced at date 1.
- Working backward from this, constraint (97) ensures that agent 1 will tell the truth at date $t = 1$.
- Again, "Revelation Principle" arguments ensure that these constraints can be imposed without loss of generality in the search for private information efficient arrangements.

Problem 5:

$$\max \pi[U(y' + F_1(y')) + EU(y_2 + F_2(y'))] + (1-\pi)[U(y'' + F_1(y'')) + EU(y_2 + F_2(y''))]$$

subject to

$$U(y' + F_1(y')) + EU(y_2 + F_2(y')) \geq U(y' + F_1(y'')) + EU(y_2 + F_2(y'')) \tag{10}$$

$$U(y'' + F_1(y'')) + EU(y_2 + F_2(y'')) \geq U(y'' + F_1(y')) + EU(y_2 + F_2(y')) \tag{11}$$

$$\pi[W - F_1(y') + W - F_2(y')] + (1-\pi)[W - F_1(y'') + W - F_2(y'')] \geq 2K. \tag{12}$$

- First two constraints are truth telling constraints, third is agent $b's$ IR constraint

Multiperiod Contracts

Townsend (1982)

- From FOC we can see that optimal borrowing may not be zero
  - When $y_1 = y'$ but π is close to zero, agent a has little wealth at $t = 1$ and expects to have much more wealth at $t = 2$ and will therefore borrow at $t = 1$ (and will conversely lend at $t = 1$ when income in period 1 is high)
- This two period contract allows for beneficial trade between agents $\Rightarrow$ welfare improvement over the single period contract

Theorem

Either (10) or (11) must bind in a solution to problem 5.

Proof: By contradiction. If borrowing and lending, then no incentive constraint is binding, in which case its the full info solution, which is not borrowing lending.

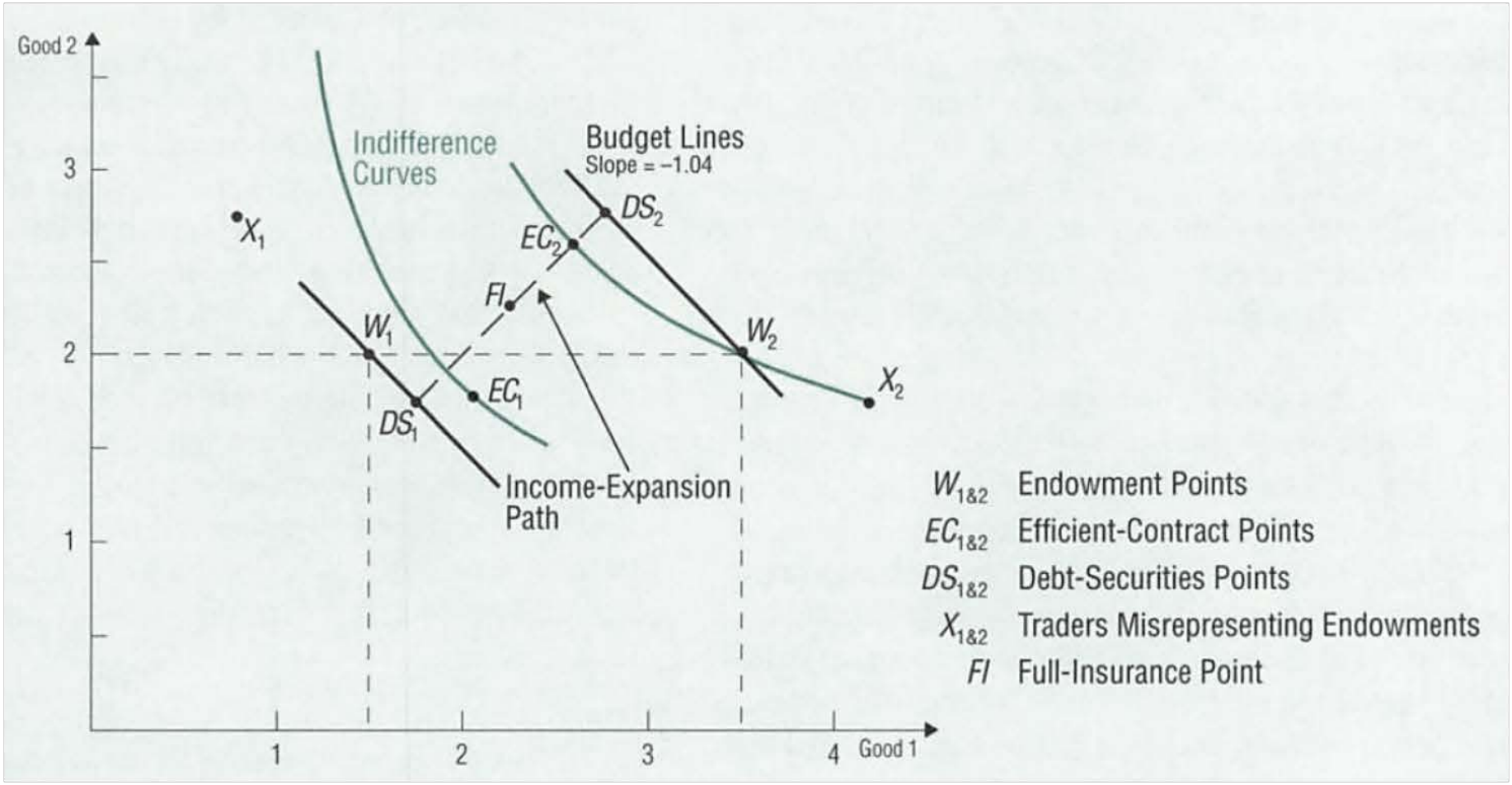
Corollary

There must be history dependence in the second period transfer, i.e. $F_2(y') \neq F_2(y'')$. *This is the "relationship" that captures private information*

Examples of Relationships among Financial Institutions

- It is not immediately evident that long term contracts discussed above are regularly implemented in traditional credit markets
- Deposits and savings accounts do not directly resemble history dependent insurance based contracts
- However, Berlin and Mester (1999) find that banks funded more heavily with core deposits provide more loan-rate smoothing in response to exogenous changes in aggregate credit risk
    - evidence for a novel channel linking bank liabilities to relationship lending

Efficient Contract Allocation



Relationships Among Broker Dealers

"In the past, the common belief is if one dealer wins, the other has to lose....Large dealers are now the liquidity manufacturing plants and small dealers remain vital distribution engines..... Its all about the client and how they can service them properly in order to get business in the form of valuable inquiry (flow). Every client inquiry does not need to be profitable, but over time the aggregated inquiry needs to have a positive expected return- ... Inquiries vary according to the client and what they are paying the dealer for. ...Dealers take risk when they price a client transaction. .... Clients realize this and know that their business must take place in a form that over the long run will fit the dealers model and have positive expected returns. If this isnt the case, their liquidity will ultimately be compromised. Our experience with fixed income clients is that they are extremely thoughtful as to how they reward their dealers and have rich metrics to evaluate those relationships. They cherish and need to have relationships with both the large and small dealer for the benefit of their business. Hence, clients develop a portfolio of dealer relationships that forms over time.

Costly State Verification

- Thus far we have operated under the premise that outputs of the villas were not directly observable, except of course in actual net transfers and perhaps in deliberate, pretransfer displays.
- Suppose that at some cost K in terms of forgone consumption, agent 2, the monastery, could observe or verify all of agent 1's actual output.
- Agent 2 could audit or monitor agent 1.
- Supposing that this cost K might be considerable, we can still ask whether such auditing would take place.
- Retreat to the single-period setup. So let $\pi(d \mid \widetilde{\theta})$ denote the probability of an audit conditioned on announced parameter $\widetilde{\theta}$, either $d = 1$ for audit or $d = 0$ for no audit.
- Also, let $\pi(\tau \mid \widetilde{\theta}, d = 0)$ denote the probability of transfer τ conditioned on announcement $\widetilde{\theta}$ and no audit and $\pi(\tau \mid \widetilde{\theta}, \theta, d = 1)$ denote the probability of transfer τ conditioned on announcement $\widetilde{\theta}$, the fact of an audit, and revelation of actual parameter value θ.

- **Program 9**: Maximize by choice of probabilities

$$\pi(d \mid \widetilde{\theta}), \pi(\tau \mid \widetilde{\theta}, d=0), \pi(\tau \mid \widetilde{\theta}, \theta, d=1)$$

- The objective function

$$\begin{aligned}
&\lambda^1(\Sigma_\theta p(\theta)[\pi(d=0 \mid \theta)\Sigma_\tau \pi(\tau \mid \theta, d=0)U^1[\theta-\tau] \\
&+\pi(d=1 \mid \theta)\Sigma_\tau \pi(\tau \mid \theta, \theta, d=1)U^1[\theta-\tau]]) \\
&+\lambda^2(\Sigma_\theta p(\theta)[\pi(d=0 \mid \theta)\Sigma_\tau \pi(\tau \mid \theta, d=0)U^2[W+\tau] \\
&+\pi(d=1 \mid \theta)\Sigma_\tau \pi(\tau \mid \theta, \theta, d=1)U^2[W+\tau-K]])
\end{aligned} \tag{105}$$

- Subject to incentive constraints, for all $\theta, \widetilde{\theta}$,

$$\begin{aligned}
&\pi(d=0 \mid \theta)\Sigma_\tau \pi(\tau \mid \theta, d=0)U^1[\theta-\tau] \\
&+\pi(d=1 \mid \theta)\Sigma_\tau \pi(\tau \mid \theta, \theta, d=1)U^1[\theta-\tau] \\
&\geq \pi(d=0 \mid \widetilde{\theta})\Sigma_\tau \pi(\tau \mid \widetilde{\theta}, d=0)U^1[\theta-\tau] \\
&+\pi(d=1 \mid \widetilde{\theta})\Sigma_\tau \pi(\tau \mid \widetilde{\theta}, \theta, d=1)U^1[\theta-\tau]
\end{aligned} \tag{106}$$

- The $\pi(\tau \mid \widetilde{\theta}, \theta, d = 1)$ can be set equal to unity at τ values implying extreme values of consumption, zero or subsistence, for agent 1. These probabilities appear only on the right-hand side of the incentive constraints, or, to put it another way, they are never brought into the solution.
- The agent never lies about his parameter values. Still, audits can occur with positive probability. In this way the agent is threatened with off-equilibrium behavior.
- A striking feature of the solution to Program 9, or at least to similar programs, is that the probability of audits is positive even for relatively large values of audit cost K. Even rare, costly audits can help alleviate the incentive problems of nonfixed rentals, that is, of θ-contingent transfers.

Limited commitment literature: overview

- Pure exchange economy, I agents, one good
- Identical utility functions $U(c) = \mathbb{E}\left[\sum_t \beta^t u(c_t)\right]$
  - with $u : \mathbb{R}_+ \to \mathbb{R}$ strictly concave and $\mathcal{C}^1$
- Endowments:
  - Uncertainty is described by a finite-state Markov process $\{z_t\}$, taking values $z \in \{1, \ldots, Z\}$, with transition matrix Π. Let $z^t = (z_0, \ldots, z_t)$
  - Individual endowments: $e_{i,t}(z^t) = \epsilon_i(z_t) > 0$
  - Aggregate endowment: $e_t(z^t) = \sum_i \epsilon_i(z_t)$
  - This endowment process allows for idiosyncratic and aggregate uncertainty, as well as serial correlation in shocks
- Write the utility corresponding to the stochastic consumption process $\{c\}$, starting at time t and history z^t, as

$$U(c)(z^t) = \sum_{s=t}^{\infty} \sum_{z^s \in Z^s} \beta^{t-s} u(c_s(z^s)) \pi(z^s | z^t)$$

Feasible allocations

Definition

An allocation $\{c_i\}_{i=1}^I$:

- is *resource-feasible* if

$$\sum_{i=1}^{I} c_{i,t}\left(z^t\right) = e_t\left(z^t\right) \quad \forall t, z^t \tag{RC}$$

- satisfies the *participation constraints* if

$$U\left(c_i\right)\left(z^t\right) \geq U\left(e_i\right)\left(z^t\right) \quad \forall t, z^t, i \tag{PC}$$

- is *feasible* if it is resource-feasible and satisfies the participation constraints
- is *constrained efficient* if it is feasible, and not Pareto-dominated by another feasible allocation

Smart Contracts - including Multiparty Mechanisms

fourth component

Smart Contracts Implementing Solutions to Mechanism Design Problems

- Contracts are on distributed ledgers
- States of the system (as in balance sheet), controls as actions or messages result in transitions (as in cash flows) –as in economics and engineering
- Messages are put on the ledgers, revelation principle and truth-telling

> Under this resource allocation scheme, villa 1 waits to see output vector θ before sending message m. Thus its decision problem is of the form, for every $\theta \in \Theta$, maximize $U^1[\theta - f(m)]$ by choice of $m \in M$

- Multi-period contracts: Past histories recorded become immutable, a series of incentive constraints

$$\Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \widetilde{\theta}_1, \theta_2) \geq \Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \widetilde{\theta}_1, \widetilde{\theta}_2) \quad (96)$$

and the incentive constraints at date 1, for every actual θ_1 and announced $\widetilde{\theta}_1$,

$$\Sigma_\tau U^1[\theta_1 - \tau]\pi_1(\tau \mid \theta_1) + \beta\Sigma_{\theta_2} p(\theta_2 \mid \theta_1)\Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \theta_1, \theta_2) \geq \Sigma_\tau U^1[\theta_1 - \tau]\pi_1(\tau \mid \widetilde{\theta}_1) + \beta\Sigma_{\theta_2} p(\theta_2 \mid \theta_1)\Sigma_\tau U^1[\theta_2 - \tau]\pi_2(\tau \mid \widetilde{\theta}_1, \theta_2) \quad (97)$$

- Commitment in entering into the agreement and commitment to the way it is carried out it out

Incentives and the meaning of 'Trust'

- Revelation principle: incentive constraints ensure agents are honest (truth telling) and obedient (moral hazard)
  - Per se we do not trust to carry out otherwise
- If there is limited commitment
  - Need collateral, multi period contracts, or reputation
- Unique implementation of mechanisms: Design can prevent collusion
- So what is the CS community worrying about exactly?
- Faulty communications vs. nefarious behavior, a distinction not made
- And what about equilibrium behavior under the protocol? (a literature on bitcoin emerges)

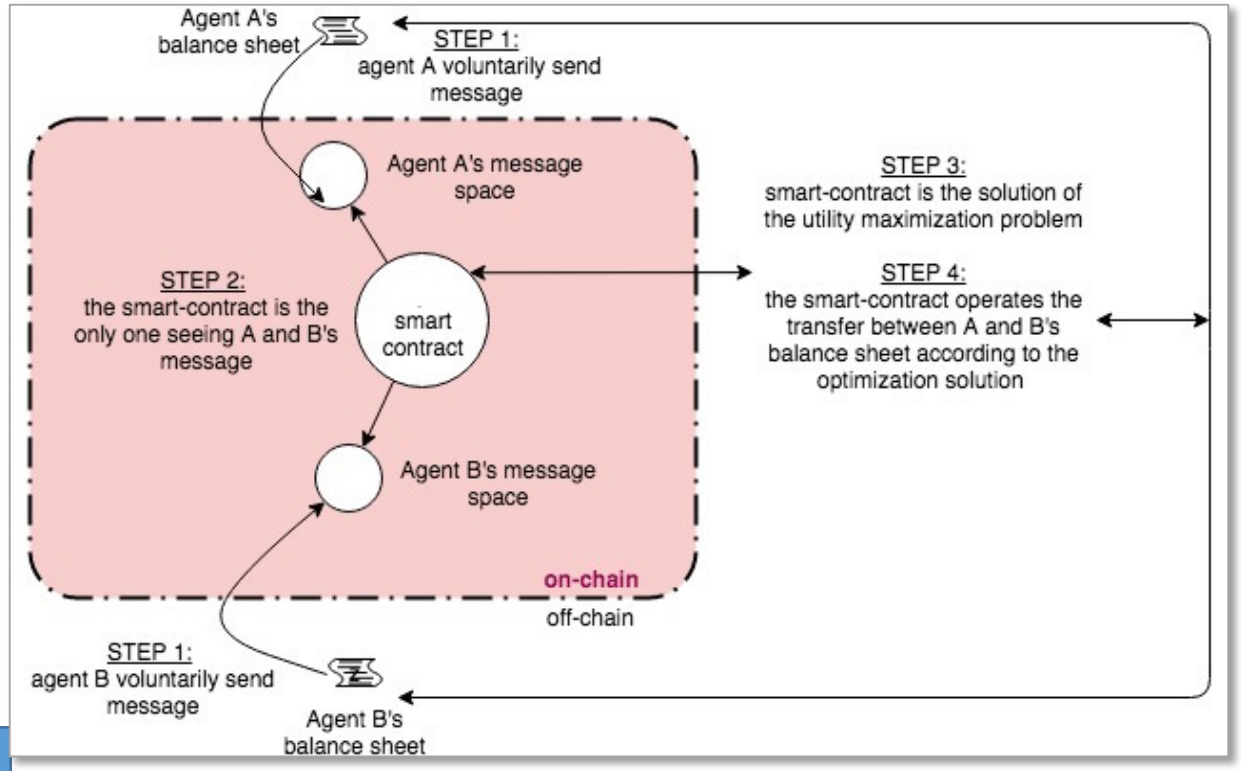
Byzantine Generals Problem: In Computer Science and Economics

- If enemy is prepared or generals do not attack as a group, failure
  - The generals exchange messages with each other
  - If the number of potential traitors (faults) is known, and all other nodes tell the truth, cross-checking a sufficient number of messages is sufficient
    - Requires "3f+1" replicas to be able to tolerate "f" failing nodes
- New design: Second general not allowed to communicate back. First attacks as long as informed enemy is unprepared
- Other designs: Sending of the same message along multiple paths, or repeatedly along the same path , or one informed agent serves as a "leader" relaying messages
  - Coles and Shorrer (2012) , Chwe 1995; De Jaegher and van Rooij 2011).

Hybrids in the Middle Ground: the pieces are there from both sides

- From mechanism design
  - Contracts with *costly state verification* are literally executed with messages where, over some range of states, costly messages are not used
  - A version of the *revelation principle* works with no communication at all and with noisy messages,
    - so one need not abandon mechanism design when facing the reality of imperfect messaging (Prescott 2003)
- From smart contracts (as in Corda)
  - Validity consensus: Unique vs. non-unique consensus, Info-partitioned ledgers
  - Notaries: one, or multiple trusting, or multiple non-trusting notaries
  - Public and/or private nodes
  - Oracles: Broadcast communication vs. selectively private communication

Hybrids: On- and Off-Chain, Quasi-Private



Nicholas Zhang (2019)

No planner, but then Compiling and verify code on-chain is incredible costly.
Solution is do some things off-chain-
Entire documents can be encrypted off-chain and accessed as reliable
Messages, states in contract can be separate from ledgers for transfer of value
Multiparty computation, share partial information, know system is functioning properly
But in practice, mpc technology is still limited, hence quasi private, not going to extremes