Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers

Authors

Alberto Sonnino*

Mustafa Al-Bassam* Shehar Bano* Sarah Meiklejohn* George Danezis*

* University College London

February 2019

The Authors



Alberto Sonnino



Mustafa Al-Bassam



Bano Shehar



Sarah Meiklejohn



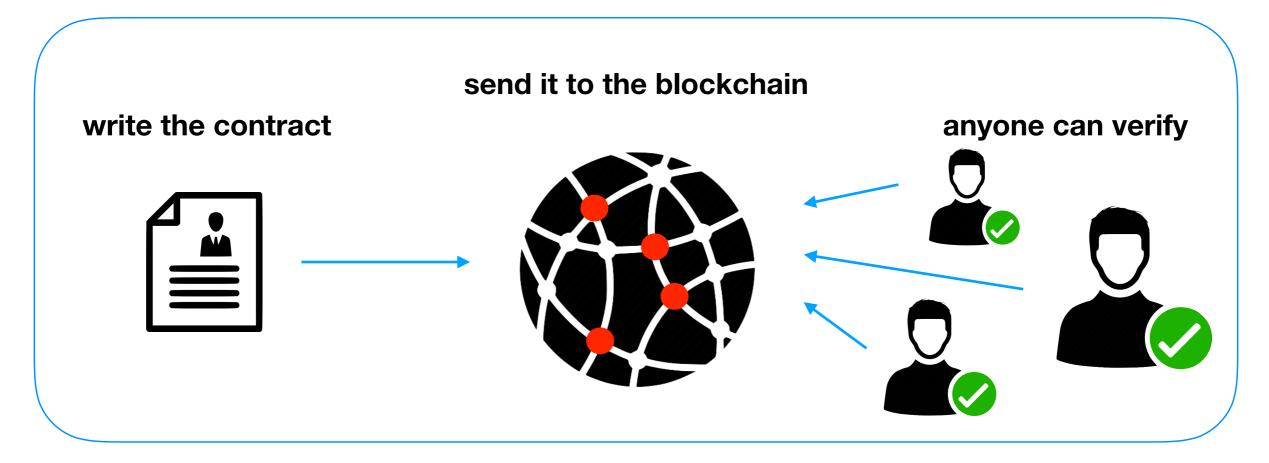
George Danezis

Challenges in blockchains



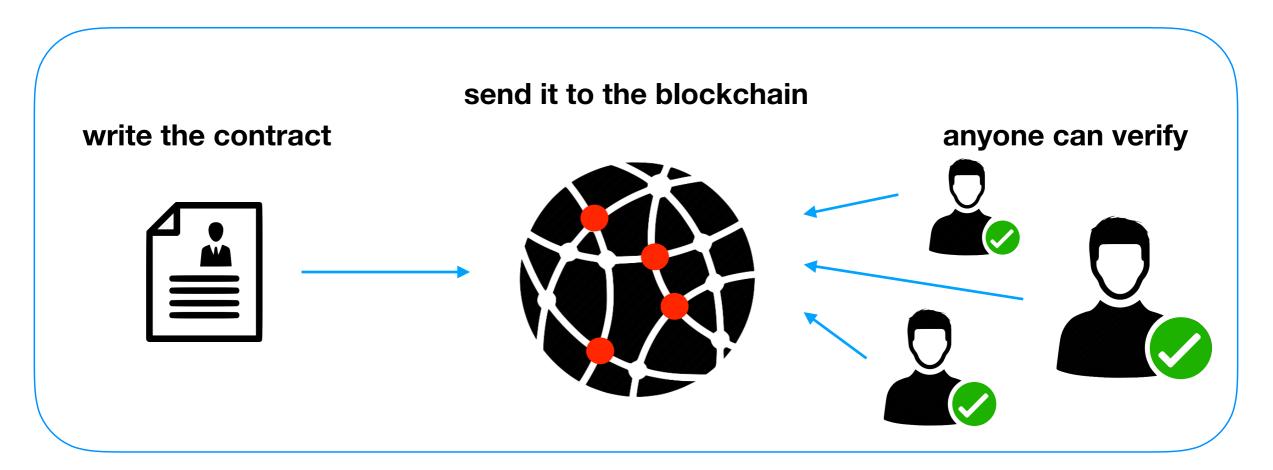
Challenges in blockchains





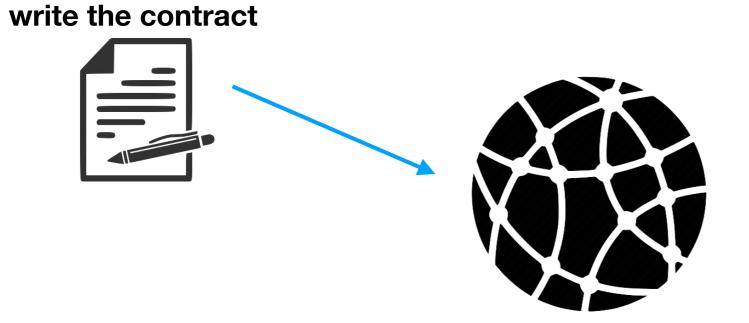
Challenges in blockchains

Can we issue credentials in this setting?



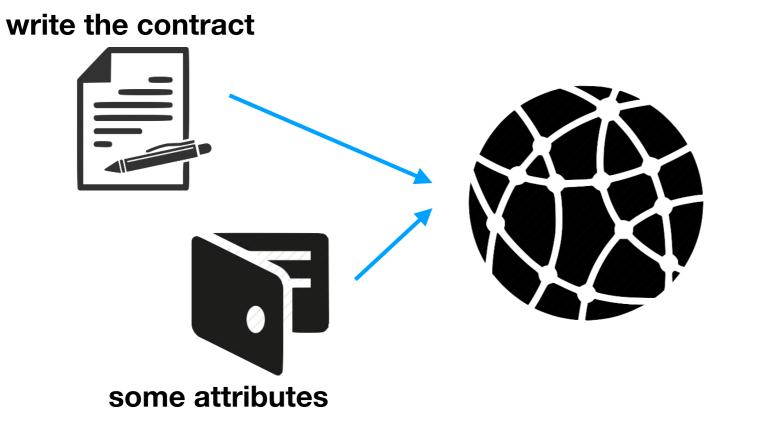
What are we trying to do?

Issuing credentials through smart contracts



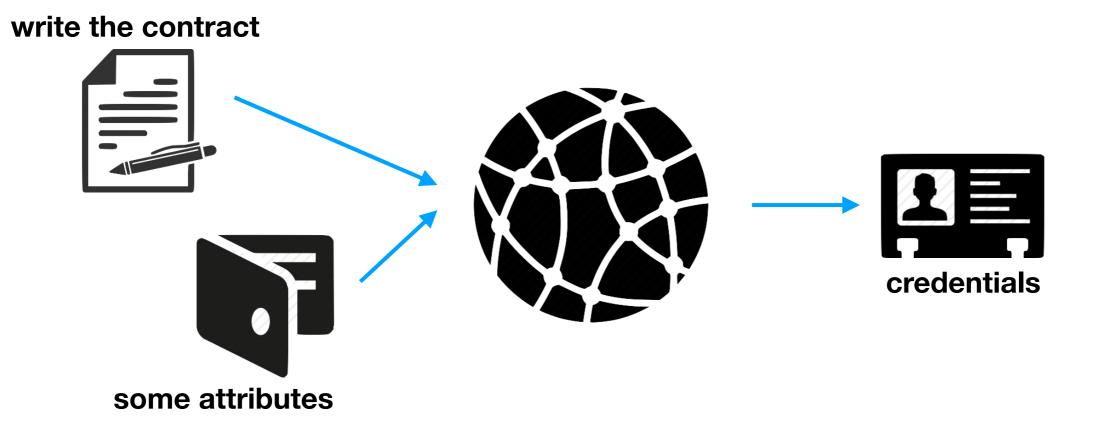
What are we trying to do?

Issuing credentials through smart contracts



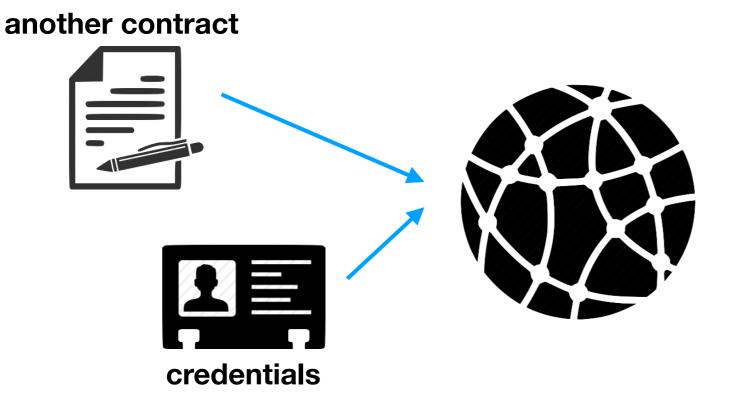
What are we trying to do?

Issuing credentials through smart contracts



What are we trying to do?

Issuing credentials through smart contracts



What are we trying to do?

Why is it hard?



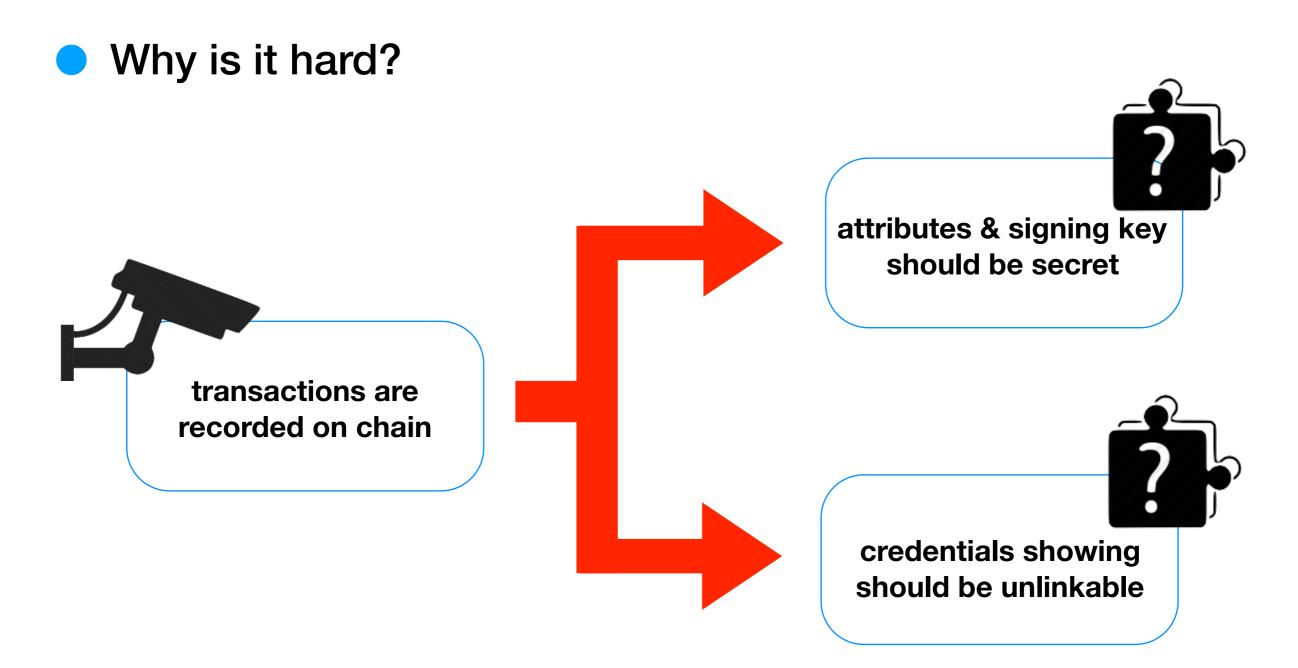
In a decentralised setting

What are we trying to do?

• Why is it hard?

In a decentralised setting

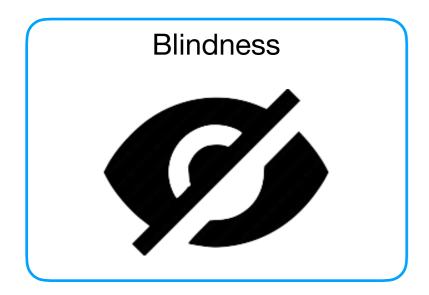
What are we trying to do?



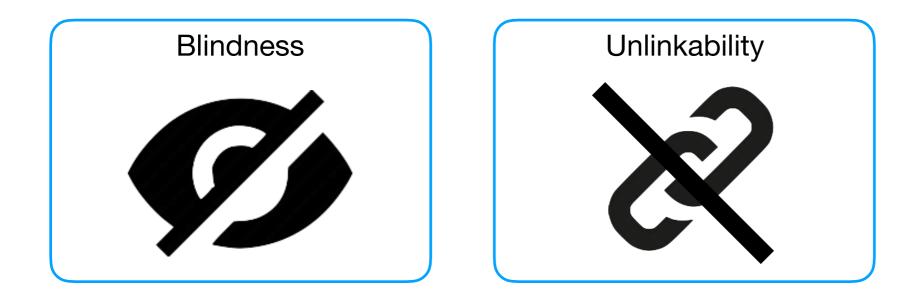
In a decentralised setting

Introduction

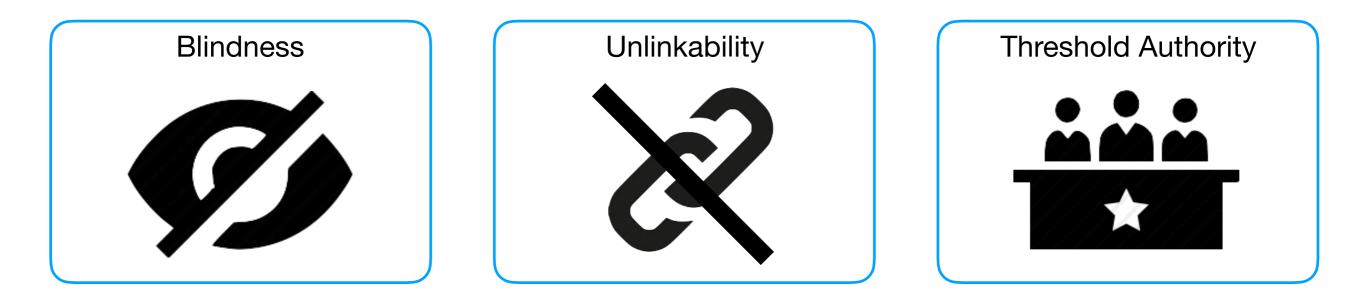
Introduction



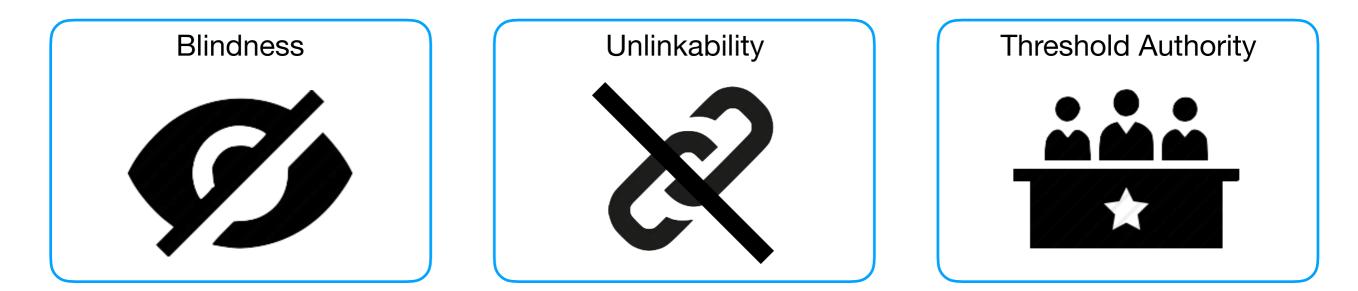
Introduction

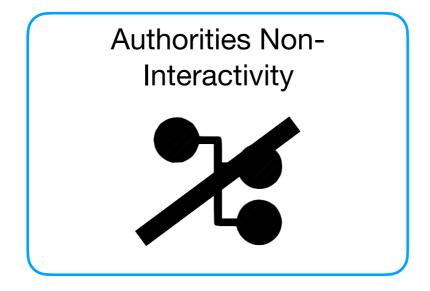


Introduction

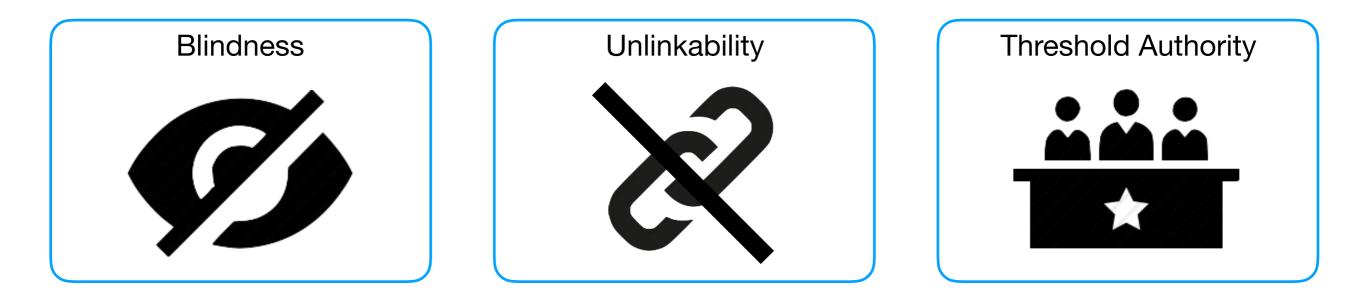


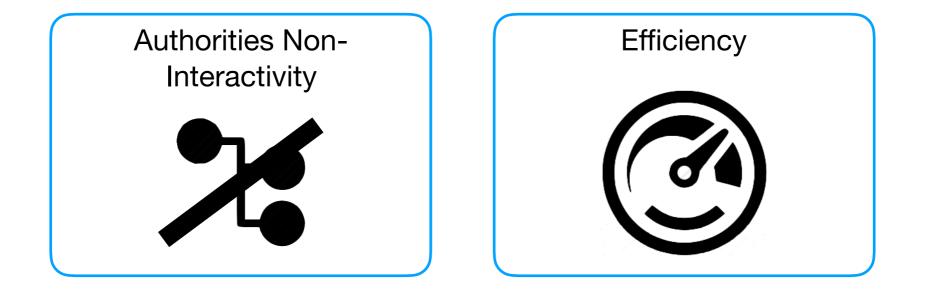
Introduction





Introduction





So we built Coconut



Introduction

• What is Coconut?

Introduction

What is Coconut?

Contribution I

Coconut credentials scheme



Introduction

What is Coconut?

Contribution I

Coconut credentials scheme



Contribution II

Coconut smart contract library & example of applications



A. Primitives evalue $f_{i}\overline{\sigma n} (g_{1}^{\kappa})^{-1}$

Then, Tibeysightatuneir solutions thas dottion simplomented to in python listu Lingart debtailed arypoolkhravites dgetlipbo[bf] standy ibgglith [2]. The buildilifteen phiring neorkaluever and the itoe Neak-Iniga [st.7] curve, using

$$\pi = \mathrm{PK}\{\left(k
ight):
u = \left(g_{1}^{k}
ight)^{UUID} \ \land \ \kappa = lpha eta^{k}\}$$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been

C. Mapping au Alberto: @G can also be C. of CoCoNut w actually built a

A. Pri

The using bilinear pairing works over a Barreto-Naeprio 177 curve, using OpenSSL as the arithmetic backend. We have released the code as an open-source project on GitHub. 2 CCUz Intel Year. This table shows

TABLE II: Co

³https://github.c and 3 time faste aggregation of 1 Table II sho size of each ex presented in fig. of signing author message on wh that in practice therefore set to 3 132 bytes. The

ask a-signature

hiorsaulion labor

Jeta-coi

table ohow

and stahoigr & lot you and the state of the

described the section of the section

uthori tian

poter

Then, They sight their solutions that determined to be appreciated to be the solution of the s

$$\pi = \mathrm{PK}\{\left(k
ight):
u = \left(g_{1}^{k}
ight)^{UUID} \ \land \ \kappa = lpha eta^{k}\}$$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been built from a signed private key k.

C. Mapping authorities to blockchain nodes

Alberto: @C can also be C of CoCoNut w actually built a

A. Pri

The using bilinear pairing works over a Barreto-Naehrio II 71 curve, using OpenSSL as the arithmetic backend. We have released the code as an open-source project on GitHub. 2 (CUz Intel Year This table shows)

TABLE II: Co

³https://github.c and 3 time faste aggregation of 1 Table II sho size of each ex presented in fig. of signing author message on wh that in practice therefore set to 3 132 bytes. The

ask a-signature

signatures labor

Jeta-coi

table ohow

and stachdiar & 107 yearing Try out A

described the sector of the se

uthori tian

poter

Then, They sight their solutions that determined the determined to be the solution of the solution of the listual of the solution of the solut

$$\pi = \mathrm{PK}\{\left(k
ight):
u = \left(g_{1}^{k}
ight)^{UUID} \ \land \ \kappa = lphaeta^{k}\}$$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been built from a signed private key k.

C. Mapping authorities to blockchain nodes

Alberto: @George, Describe how the CoCoNut authorities can also be Chainspace nodes (to make clear the poter of CoCoNut when doorly_related to blockchains. Since we

actually built a

TABLE II: Co

³https://github.c and 3 time faste aggregation of 1 Table II sho size of each ex presented in fig. of signing author message on wh that in practice therefore set to 2 132 bytes. The

ask a-signature

iorsautos labo

Jeta-coi

table ohow

stehoigra lokavanta us use h

avective the section of the section

A. Pri

The using bilinear pairing works over a Barreto-Naeprio 177 curve, using OpenSSL as the arithmetic backend. We have released the code as an open-source project on GitHub. 2 CCUz Intal Yaar. This table shows

Then, They sight their solution is determined by the solution of the solution

$$\pi = \mathrm{PK}\{\left(k
ight):
u = \left(g_{1}^{k}
ight)^{UUID} \ \land \ \kappa = lpha eta^{k}\}$$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been built from a signed private key k.

C. Mapping authorities to blockchain nodes



TABLE II: Co

³https://github.c and 3 time faste aggregation of 1 Table II sho size of each ex presented in fig. of signing author message on wh that in practice therefore set to 2 132 bytes. The

Albert	o: @George, Describe how the CoCoNut authoriting	therefore set to .
	be Chainspace nodes (to make clear the poter	132 bytes. The
of CoCo	Nut when deeply related to blockchains ince we	-ask a-signature
actually	Nut when deeply related to blockchains, ince we built all of the to block the shower and standard built all of the to block equation of the shower and the standard built all of the to block equation of the shower are the source of the so	that the proof at
	The stonature scheme has been traplemented as all and the power the result of the surrouted in the second surrouted in the second se	an on an Octa-coi
		at onisvaole olion
A. F	hilling a marke and Barreto-Ngehrio. 1. / 1 C	gurve, using
Tl	ickend We have releas	onan lear tarressage
usin	5.00112 1 at theor. It	EStable show B
bilin	iring works over a Barreto-Nachrig [17] curve using	entatuentes) (abotit_ a
Ope	iring works over a Barreto-Naehrig 171 curve using the execution of steenfproteetscherser workingeonor as the arithmetic backend. We have released the code Each entry is the result of 10,000 measured on ar	11896219Nedragame
*	en-source project on GitHub	4

Then, They sight their solutions that determined to the prelistu Lingart debtailed ary pool knowledge theory of standy long lith (2). The build life an printing near knowledge to Batteritoe Near Inign [st 7] curve, using

$$\pi = \mathrm{PK}\{\left(k
ight):
u = \left(g_{1}^{k}
ight)^{UUID} \ \land \ \kappa = lpha eta^{k}\}$$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been built from a signed private key k.

C. Mapping authorities to blockchain nodes



TABLE II: Co

³https://github.c and 3 time faste aggregation of 1 Table II sho size of each ex presented in fig. of signing author message on wh that in practice therefore set to 2 132 bytes. The

Alberto: @George, Describe how the CoCoNut authorities 132 bytes. The can also be Chainspace nodes (to make clear the poter ask a-signature of CocoNut when deeply related to blockchains) incentional lange when a particle in the prover and an end of the prover an end of th actually built all Equinactionse de la place du ce des de la place de la Gitatoso table olion icicenterdesanine sectivity section labor A. Primitives eva nd We have release of the corten evalue The signature BOTTE BLOCK I TIES Able show Bo using the two cryponia The mouth (faster of that doer den at 1921) (fortit - (bilinear pairing works brockenscherkonstingentionlagetime Hageime OpenSSL as the arit ured on an Octa-core as an open-source project on GitHub⁻³.2 (CUT Intel Veen This table above

n

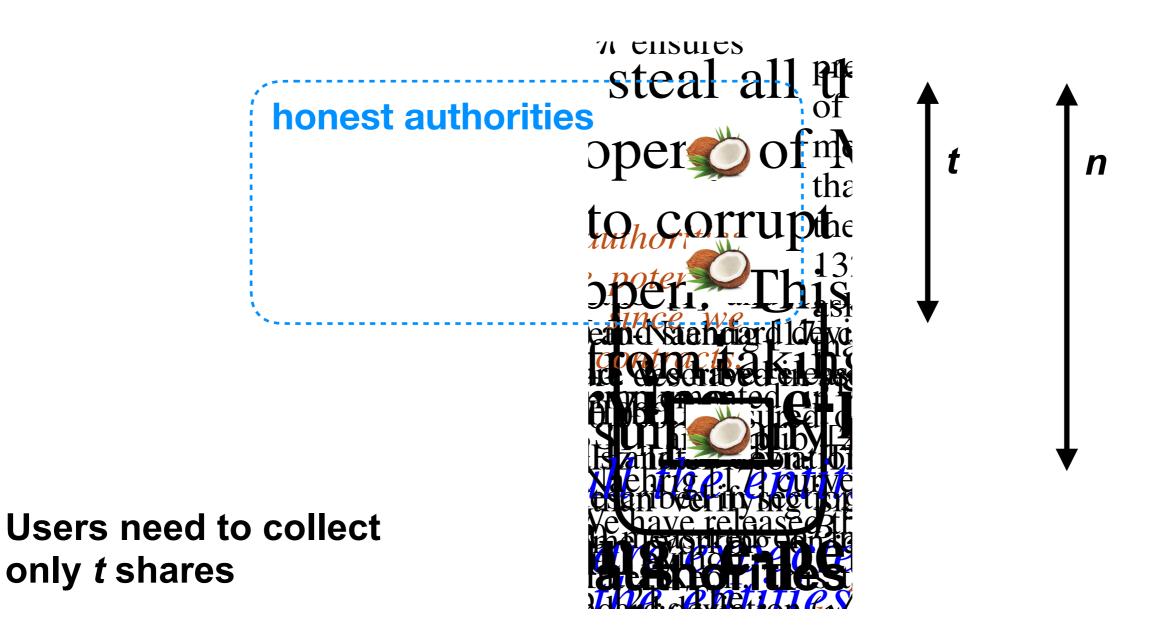
System Overview

Threshold authorities



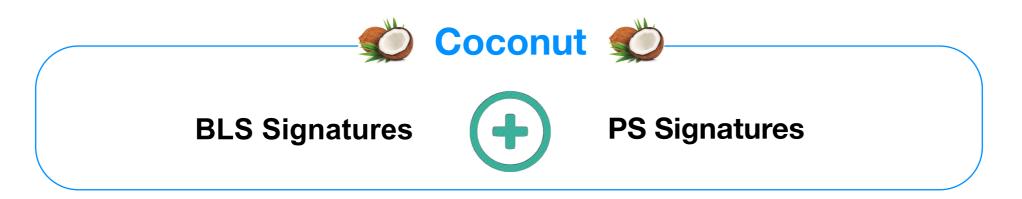
System Overview

Threshold authorities



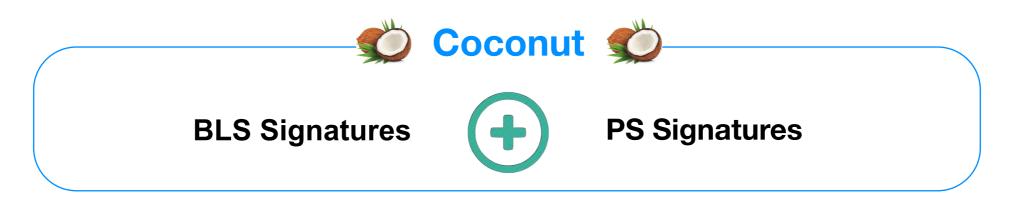
Coconut Credentials Scheme

From where do coconuts come from?



Coconut Credentials Scheme

From where do coconuts come from?



What do they look like?

take an attribute: mcompute: $h \leftarrow H(c_m)$ signature: $\sigma \leftarrow (h, h^{x+my})$ & secret key: (x, y)

	The listu	
	built C. Mapping authorities to blockchain nodes	
Cocc	Alberto: @George, Describe how the CoCoNut authorities can also be Chainspace nodes (to make clear the potential	
Coi	that ν has been built from a signed private key κ . $V = EVALU \epsilon TION$	se ese sig
	C. MappingPauthavitiesvtallehookchain nodes the	ess at i ere
repeat t imes	Albor Are signature sscheme hash been Cimplemetheditins pytho can alsousing Cheinspore corypoldibitaries apetible (1] than dophiba[2]. The of CoCdo him earl pairing phores lover to Baherbe Nachrig (1774 curve, using a that contain contains and the second	f a a a b a b a b a b a b a b a b a b a
	as a Doppedeskupec projecter of B.GatHzblitel Xeon. This table shows	te

Alberto: @George, Describe how the CoCoNut authorities
The UISDID parameter uniquely (identifies the petit of Open function
the open construction in the petition of the petition of the present of the present of the petition of the third party creating the petition and
$$of_1$$
)
authorities issuing the credentials. In order to sign the petition, that f_1 as f_2 and h_1 and $\nu_{erifier}$ respectively hold
the users compute a value ν as follows.

EVALUATION A. Primitives evaluation $(g_1^k)^{\overline{UUID}}$

Then, They signature is solven the option simplemented to a python listu singantebtuild arypoolkbravies dgetlibo [1] shook ibglith [2] V The buildifican phiring means a solution of the second se

$$\pi = \mathrm{PK}\{(k):
u = \mathbf{cop}_{k}^{k} \text{ act info} \kappa = lpha eta^{k}\}$$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been built from a signed private key k.

attributes

C. Mapping authorities to blockchain nodes

Alberto: @George, Describe how the CoCoNut authorities can also be Chainspace nodes (to make clear the potential of CoCoNut when the signing signing some contractor and the significant of significant significant of the si

The second and the experimental second and balls by the second of the experimental second and the experimental second and balls been implemented in py too been were second and balls been implemented in py too been were second and balls been implemented in py too been were second and balls been implemented in py too been were second and balls been implemented in py too been were second and balls been implemented in py too b

A. Primitive lipeaturation works over a Barreto-Naehright verifying as provide signatures in the signature source of the sou Al Al OpenSSL as the arithmetic backena. We have released in section section desktop computer, 3.60 Hz intel Xeon. This table shows as an open-source project on Cittud 10,000 measured on an Octa-core is Albach faster offare vetifying dignatures (about ernatives)

as an open-source project on onthus. Intel Xeon This table shows faster of the result of the second standard deviation (V. Person the standard deviatin (V. Person the standard Dell deskton computer 3 6GHz Intel Xeon This table shows to accurbly it is acclustiffy not many scheme have getually been

Adding ν to L prevent a citizen to vote twice during the campaign (prevent double spending), while the proof π that ν has been built from a signed private key k.

C. Mapping authorities to blockchain nodes

k¶ § that the 318 by Alberto: @George, Describe how the CoCoNut aut can also be Chainspace nodes (to make clear the p of CoCoNut when deeply related to blockchains), si TABLE II: Communication complexity and mansattibnisize art co

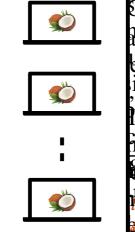
V. EVALUATION ³https://github.com/asonnino/coconut

and 3 time_faster fonitinessevenuetion hidden messages). Also,

aggregation of the signal the attension of the strength affinishented in Table II aboves the two menupoic this are compared to be it and the lib [

size of each man gain my wed in the signature schenge, 17\$ curv presented in OpenSTheasoner of signing authoritiesemsour message on what the shows that in practice meisthe be therefore set to 32 bytes (for 132 bytes. The highest transf

sign



send.awtheavertheased t entsuthe size of the and signature deviation (\mathbf{v} aldeserises in section sec 500 measureturenisan Oc garaten han the pass table amesefremthesignatures SAN AND RANGE STATE ppliction II. d ourse Wingcore te ashie the to de aves a a a a

Application

Privacy-pr

that reatoren built of built of a sogned private key k.

options, scores)

C. Mapping authorities to block than nodes $\nu = (g_1)^{\ell}$ smart Alberto: @George, Describe how the CoCoNut auth The UUUU parameter uniquely identifies the petit \mathcal{G} of the significant best in the size the oscoras oparameter holds, the leitizen's brotesh (initialized) zero tulnly the it as of thas petition, the entires are only not the and NO; and the felds owner and verifier respectively hold the public key of the third party creating the petition and qf_{1} authorities issuing the credentials. In order to sign the petition, the users compute a value ν as follows. V. EVALUATION

A. Primitives evaluation $(g_1^k)^{UUID}$

Then, They signature is scheme the option simple manted to a system listusingarthebtid arypoolknaviesdgetlibobf] showinglithat by The buibilifrean priving neorkal were a Bahreitoe Neathning [st7] curve, using

 $\pi = \mathrm{PK}\{\left(k
ight):
u = \left(g_1^k
ight)^{UUID} \ \land \ \kappa = lpha eta^k\}$

Adding ν to L prevent a citizen to vote twice during the same campaign (prevent double spending), while the proof π ensures that ν has been built from a signed private key k.

C: Mapping authorities to blockchain nodes

Alberto: @George, Describe how the CoCoNut authorities can also be Chainspace nodes (to make clear the potential

using the 5tymery partition of the state of the state of the states of t

bilinear pairing works over a Barreto-Naehrig [17] curve, using OpenSSL as the arithmetic backend. We have released the code

as an openinstituce qualitation GitHub.³. petition Table I. S. Create petition destandard heriation (a) python tor exercise the straight of t creator exercition of wach proceeder and section beside on 21. The that asigningpen-muse foresection configing signatures (about

15 times faster fors the scheme) working on deteriances ages?) of the execution of each procedure described in section section II. Each entry is the result of 10,000-measured on an Oeta-core Dell desktop computer, 3.6GHz Intel X Lecipertable shows that signing is much faster than verifying signatures (about 15 times faster for the scheme working on clear messages,

and 3 time flat Bil foil: the scheman cos bidden timessages). aggregation of keys and signatures are extremely efficient

Table II shows the communication complexity at sizeNufbeach automaingen in Vierveue Hirehersighature scher presented in fig. 1. The complexity is expressed as the h mes age signature wish $\binom{0}{n}$ tain a signature that it entry signature is the hash of the actual message is the signature is the hash of the actual message is t therefore set to 32 bytes (for SHA-2). The size of a signal 1328 hypers re The hild in the strans action size appears when the ask a signature on a hidden message (This comes from t that the proof π_s associated with the message is approximately signature 318 bytes; the proof π_v is only 157 bytes.

TABLE II: Communication complexity and transaction

³https://github.com/asonnino/coconut

and 3 time faster for the scheme on hidden messages). aggrhappens ys and signatures are extremely efficient Table II shows the communication complexity ar size of each exchange involved in the signature scher presented in fig. 1. The complexity is expressed as the n signing authorities (n), and ||m|| represents the size message on which the user wish to obtain a signature that in practice m is the hash of the actual message, therefore set to 32 bytes (for SHA-2). The size of a signal **N2** bytes. The highest transaction size appears when the of Coast asking the provide the provide the stand of the

Is by less the proof of the only 159 by test in only 159 by test i check he time it takes to hear back from t authorities.

Shappens every ith Related Works B

³https://github/cbm/accom/npAcedSON WITH RELATED WORKS

Alberto: discuss crypto related works

Alberto: compare results (speed and size) with altern see why it is cool stuff; not many scheme have actuall

³https://github.com/asonnino/coconut

Performance

• What is out there?



Performance

What is out there?

The Coconut cryptographic library

Python & Timing benchmark



Performance

What is out there?

The Coconut cryptographic library

Python & Timing benchmark





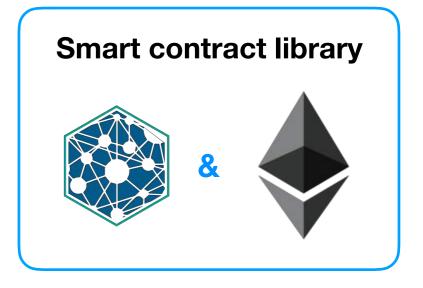
Performance

What is out there?

The Coconut cryptographic library

Python & Timing benchmark





Applications

Coin tumbler E-Petition (CRD proxy distribution)

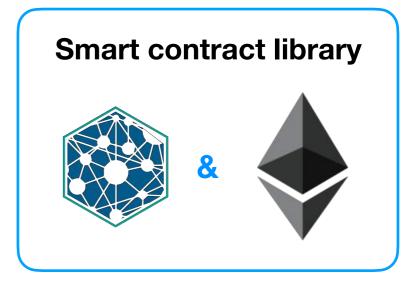
Performance

What is out there?

The Coconut cryptographic library

Python & Timing benchmark





Applications

Coin tumbler E-Petition (CRD proxy distribution)

Everything is released as open source software

https://github.com/asonnino/coconut



Performance

How fast is Coconut?

	Operation	μ [ms]	$\sqrt{\sigma^2}$ [ms]
	PrepareBlindSign	2.633	± 0.003
sign	BlindSign	3.356	± 0.002
	Unblind	0.445	± 0.002
	AggCred	0.454	± 0.000
	ProveCred	1.544	± 0.001
verify	VerifyCred	10.497	± 0.002

signing is fast, verifying takes 10ms

Performance

What is the size of the credentials?

2 Group Elements

No matter how many attributes...

No matter how many authorities...

Performance

How does Coconut scale?

	Number of authorities: n, Signature size: 132 bytesTransactioncomplexitysize [B]		
	Signature on public attribute:		
	• request credential	O(n)	32
	2 issue credential	O(n)	132
	3 verify credential	O(1)	162
	Signature on private attribute:		
issue	• request credential	O(n)	516
	2 issue credential	O(n)	132
verify	O verify credential	O(1)	355

Signing scales linearly, verifying is constant time

Performance

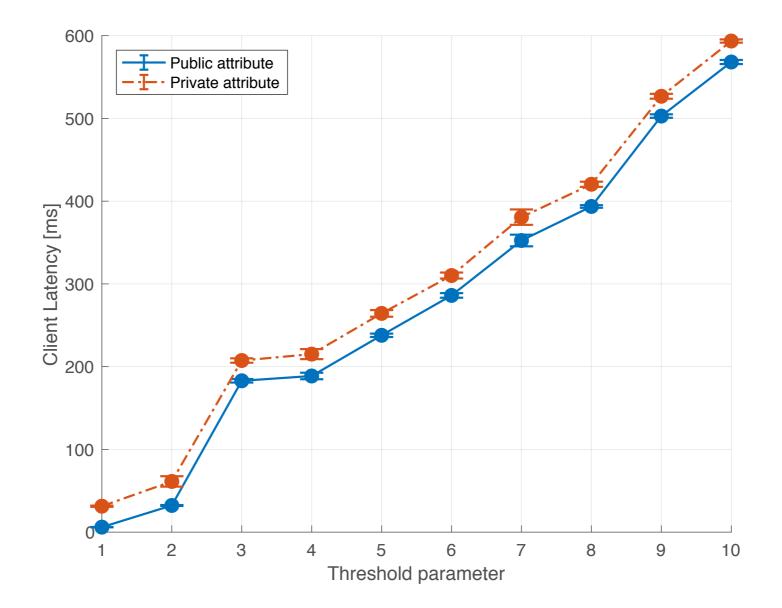
Did you evaluate it in the real world?



pick 10 locations across the world

Performance

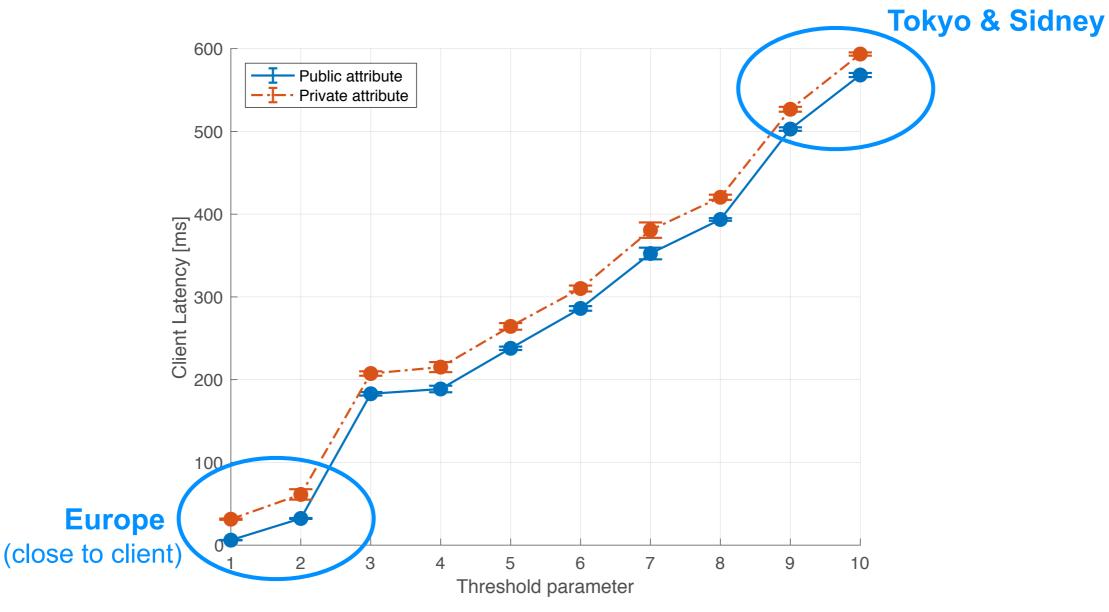
Did you evaluate it in the real world?



client latency VS number of authorities

Performance

Did you evaluate it in the real world?



client latency VS number of authorities

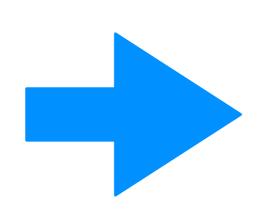
What else is in the paper?

Full cryptographic scheme

Smart contract library evaluation

Coin tumbler, CRD proxy applications

Applications evaluation and benchmarking



Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers

Mustafa Al-Bassam

Alberto Sonnino University College London University College London

Shehar Bano University College London

George Danezis University College London The Alan Turing Institute

Abstract

20 Feb 2018

CR

cs.

arXiv:submit/2158644

We present Coconut, a novel selective disclosure credential scheme supporting distributed threshold issuance, public and private attributes, re-randomization, and multiple unlinkable selective attribute revelations. Coconut can be used by modern blockchains to ensure confidentiality, authenticity and availability even when a subset of credential issuing authorities are malicious or offline. We implement and evaluate a generic Coconut smart contract library for Chainspace and Ethereum; and present three applications related to anonymous payments, electronic petitions, and distribution of proxies for censorship resistance. Coconut uses short and computationally efficient credentials, and our evaluation shows that most Coconut cryptographic primitives take just a few milliseconds on average, with verification taking the longest time (10 milliseconds).

1 Introduction

Selective disclosure credentials [15, 17] allow the issuance of a credential to a user, and the subsequent unlinkable revelation (or 'showing') of some of the attributes it encodes to a verifier for the purposes of authentication, authorization or to implement electronic cash. However, established schemes have shortcomings. Some entrust a single issuer with the credential signature key, allowing a malicious issuer to forge any credential or electronic coin. Other schemes do not provide the necessary re-randomization or blind issuing properties necessary to implement modern selective disclosure credentials. No existing scheme provides all of threshold distributed issuance, private attributes, re-randomization, and unlinkable multi-show selective disclosure.

The lack of full-featured selective disclosure credentials impacts platforms that support 'smart contracts', such as Ethereum [40], Hyperledger [14] and Chainspace [3]. They all share the limitation that ver-

ifiable smart contracts may only perform operations recorded on a public blockchain. Moreover, the security models of these systems generally assume that integrity should hold in the presence of a threshold number of dishonest or faulty nodes (Byzantine fault tolerance); it is desirable for similar assumptions to hold for multiple credential issuers (threshold aggregability).

Issuing credentials through smart contracts would be very desirable: a smart contract could conditionally issue user credentials depending on the state of the blockchain, or attest some claim about a user operating through the contract-such as their identity, attributes, or even the balance of their wallet. This is not possible, with current selective credential schemes that would either entrust a single party as an issuer, or would not provide appropriate re-randomization, blind issuance and selective disclosure canabilities (as in the case of threshold signatures [5]). For example, the Hyperledger system supports CL credentials [15] through a trusted third party issuer, illustrating their usefulness, but also their fragility against the issuer becoming malicious.

Coconut addresses this challenge, and allows a subset of decentralized mutually distrustful authorities to jointly issue credentials, on public or private attributes. Those credentials cannot be forged by users, or any small subset of potentially corrupt authorities. Credentials can be rerandomized before selected attributes being shown to a verifier, protecting privacy even in the case all authorities and verifiers collude. The Coconut scheme is based on a threshold issuance signature scheme, that allows partial claims to be aggregated into a single credential. Mapped to the context of permissioned and semi-permissioned blockchains, Coconut allows collections of authorities in charge of maintaining a blockchain, or a side chain [5] based on a federated peg, to jointly issue selective disclosure credentials

Coconut uses short and computationally efficient credentials, and efficient revelation of selected attributes and verification protocols. Each partial credentials and the

46

Limitations & Future Works

Would you like to contribute?

Limitation I

Adding and removing authorities is complicated. Can we do better than re-running the key generation algorithm?

Limitations & Future Works

Would you like to contribute?

Limitation I

Adding and removing authorities is complicated. Can we do better than re-running the key generation algorithm?

Limitation II

Current key generation algorithms are complex to implement. Can we design a key generation algorithm for blockchains?

Limitations & Future Works

What is the next milestone?

A general framework allowing nodes to execute any kind of threshold cryptography?

Conclusion

What did we talk about?

Contribution I

Coconut credentials scheme



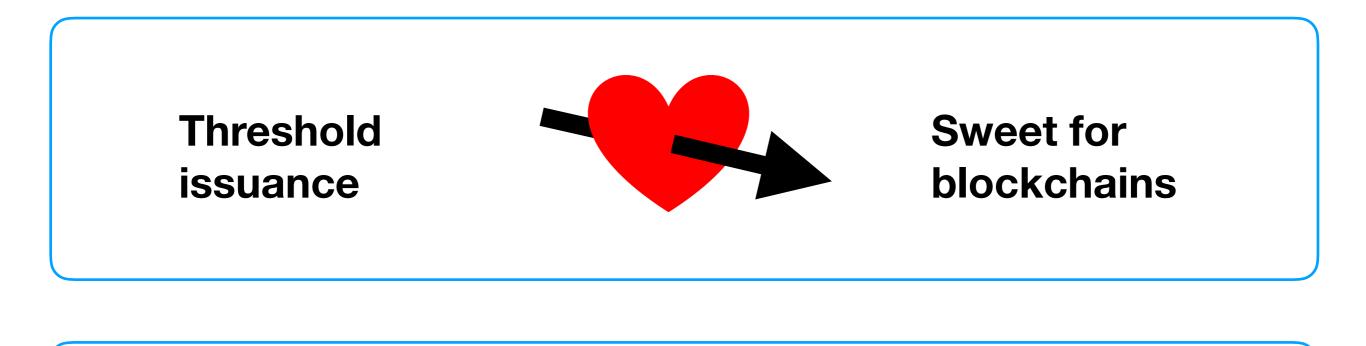
Contribution II

Coconut smart contract library & example of applications

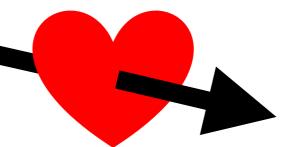


Conclusion

Main take-aways







Multi-use & unlinkability



Thank you for your attention

Alberto Sonnino alberto.sonnino@ucl.ac.uk https://sonnino.com



https://github.com/asonnino/coconut





THE ALAN

TURING INSTITUTE

This work is supported in part by EPSRC Grant EP/M013286/1, the EU H2020 DECODE project (grant agreement number 732546), and The Alan Turing Institute.